Publication date:
February 2023
Author:
Hollie Hennessey
Mike Sullivan-Trainor

Consumer IoT Device Cybersecurity Standards, Policies, and Certification Schemes

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Connectivity Standards Alliance

Contents

Summary	2
Part 1: Consumer IoT security regulations	3
Part 2: Voice of the consumer	30
Conclusion: Time for reliably secure IoT products	36
Appendix	37

Summary

There are three key elements in the world of Internet of Things cyber security. Standards are created in order to harmonize a common set of requirements. Regulations are created in order to incentivize manufacturers to adopt cybersecurity hygiene practices so as to protect societies and increase their cyber-resilience. Labels are created in order 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 Internet of Things (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 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). 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. The devices themselves include the following:

- Consumer electronics (home audio, health/fitness, appliances)
- Lighting and control devices (lighting, plugs/switches, blinds/shades)
- Safety and security devices (cameras, electronic locks, intruder alarms, video doorbells, garage door operators, hazard detectors, smart speakers)
- Climate control (air conditioners, thermostats, radiator valves, 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. With this connectivity, attackers can potentially reach into millions of homes, putting devices in jeopardy for use as botnets, for example, by bad actors in wider attacks.

Paired with this is the generally weak security of IoT devices. IoT devices, especially consumer devices, are often vulnerable for a number of reasons such as hardware issues or vulnerabilities in software. The proliferation of devices poses a real risk, especially when it is combined with a rapidly evolving threat landscape. IoT is a fast-moving market, and Omdia forecasts that by 2026 there will be around 49.5 billion installed devices. With this level of growth, the impact of an incident will likely be exacerbated by the massive attack surface that these devices represent.

The COVID-19 pandemic has driven 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. But with this increased use of technology in people's daily lives, the potential threat vectors available for criminals 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**, in order 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,

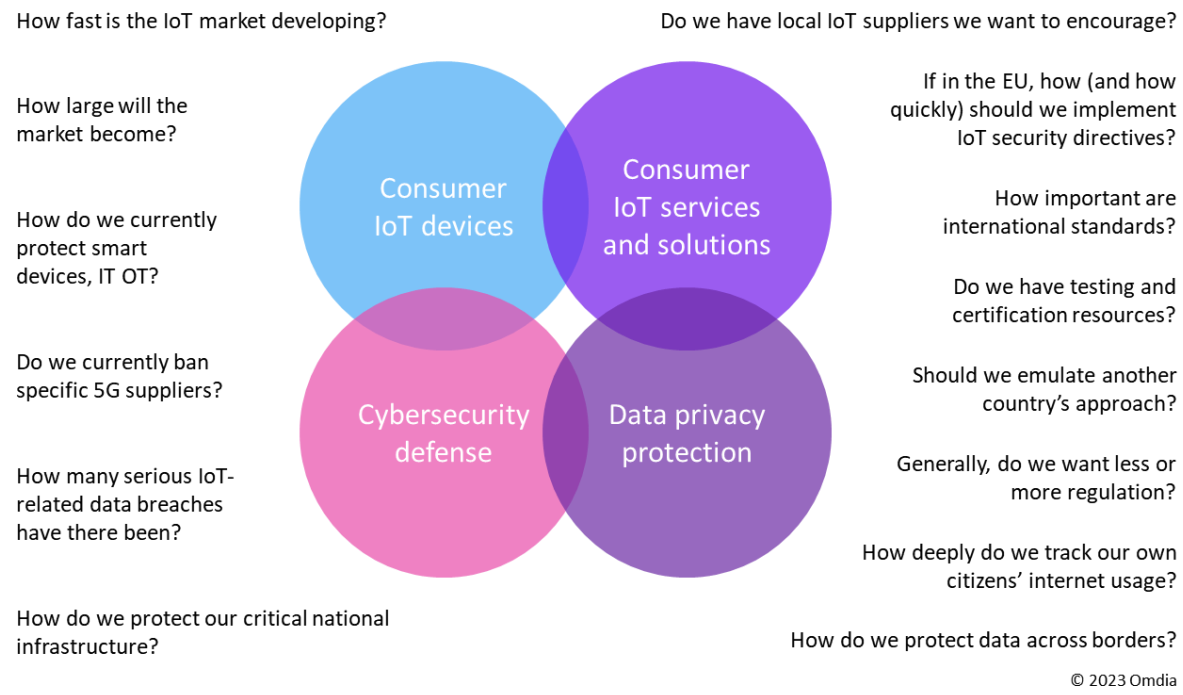
- ETSI published its EN 303 645 standard, "Cybersecurity for Consumer Internet of Things: Baseline Requirements," in June 2020. ETSI is Europe based and has been the fastest of the three main organizations listed here to address IoT security. This is currently the most widely used and referenced standard in this area.

- 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, nongovernmental organization. Although there is currently less adoption, it has published a number of standards including ISO/IEC 27402, "Cybersecurity — IoT security and privacy — Device baseline requirements."

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



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 the president'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.

Most recently, a fact sheet was published in October 2022 by the White House that outlines its plans to move forward with a consumer labeling scheme. Companies, associations, and government partners will be meeting to discuss the development of a cybersecurity label for IoT devices. Routers and home cameras have been identified as the most at risk and are expected to be prioritized as part of this effort.

ETSI: Standards for IoT device cybersecurity

The European Telecommunications Standards Institute (ETSI), a European standards organization, is the recognized standards body dealing with telecommunications, broadcasting, and other electronic communications networks and services. Its role in Europe is to support European regulation and legislation through 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, released in June 2020, was the first globally applicable standard for consumer IoT products. The standard was developed from a standard 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 EN 303 645 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 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 recommendations: the top three are: 1) no default passwords, 2) implement a vulnerability disclosure policy, and 3) keep software updated.

The standard also includes a specific section on five data protection provisions for consumer IoT, intended to be supplemental to 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 **Table 3** for more information.

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

Table 1: 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

Source: ETSI

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 ISO, the International Organization for Standardization, which publishes standards in all fields apart from electrical and electronic engineering, which are 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," is currently under development.

ISO/IEC 27402 builds on and supports the security controls documented in the recently published ISO/IEC 27400 "Cybersecurity — IoT security and privacy — Guidelines" (2022). Another notable draft is ISO/IEC 27403 "Cybersecurity — IoT security and privacy — Guidelines for IoT-domotics," aimed at the designers, manufacturers, and security assessors of IoT domotics (home automation).

The SC27 subcommittee is also working on a framework and methodology for implementing and maintaining the trustworthiness of IoT systems and services and doing very early work on the ISO/IEC 27404 labeling scheme for labeling for consumer IoT devices.

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 **Table 2**.

Table 2: 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	▪ 27402 is expected to be published in 2023 ▪ Very high-level set of requirements

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 labelling 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.

Table 3: Summary of IoT device security specifications by geographic region

Region	IoT device security specification	Mandatory/ voluntary	Certification	Labeling	Key standard referenced
Asia					
Australia	Under development	Voluntary	Yes	Yes	ETSI EN 303 645
China	Yes	Mandatory	No	No	None
India	Yes	Voluntary	Yes	Yes	ETSI EN 303 645

Japan	Yes	Voluntary	No	No	NIST, ETSI EN 303 645
Singapore	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
South Korea	Yes	Voluntary	Yes	Yes	ITU X.1352
Thailand	Under development	Voluntary	No	No	None
Vietnam	Yes	Voluntary	No	No	ETSI EN 303 645
Europe					
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

Source: Omdia

Global summary and findings by region and country

Asia

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 is not yet a legal requirement but 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 televisions and refrigerators). The guidelines do not include mobile phones, which are covered by other guidance.

The Behavioral 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 2: Proposed options for Australian IoT device security labeling

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.

In its approach to privacy and cybersecurity regulations, Australia publicly claims to follow the approach taken by the UK.

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.

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.

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.

China not only has potentially the largest internal market for IoT devices but is also the world's largest manufacturing base for them. According to Omdia's IoT Investment Tracker, IoT investments in China topped $9bn over the last three years.

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 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.

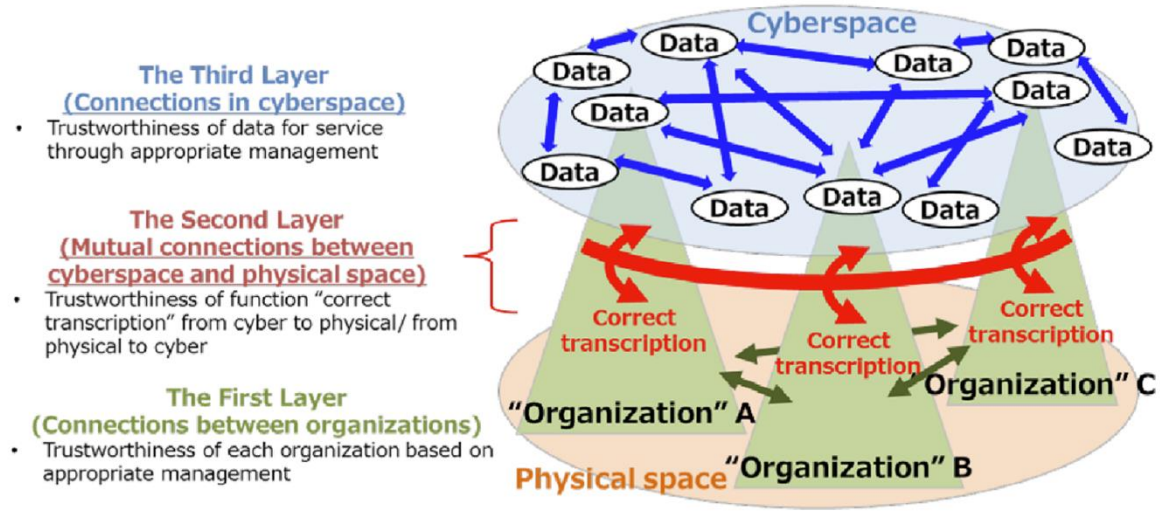
The aim of India's approach is to ensure end-to-end security for connected IoT devices, with a second nested aim of protecting the privacy of the personal data of individuals, especially in the healthcare arena.

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.

Japan

Japan has a very different approach to IoT security, concentrating on enterprise issues of trustworthiness and on the deployment of IoT devices and how they are used rather than on voluntary or mandatory guidelines to manufacturers, service providers, and distributors.

Figure 3: Japan's three-layer Cyber/Physical Security Framework (CPSF) model including the trustworthiness in each layer



Source: Japan METI IoT Security Safety Framework

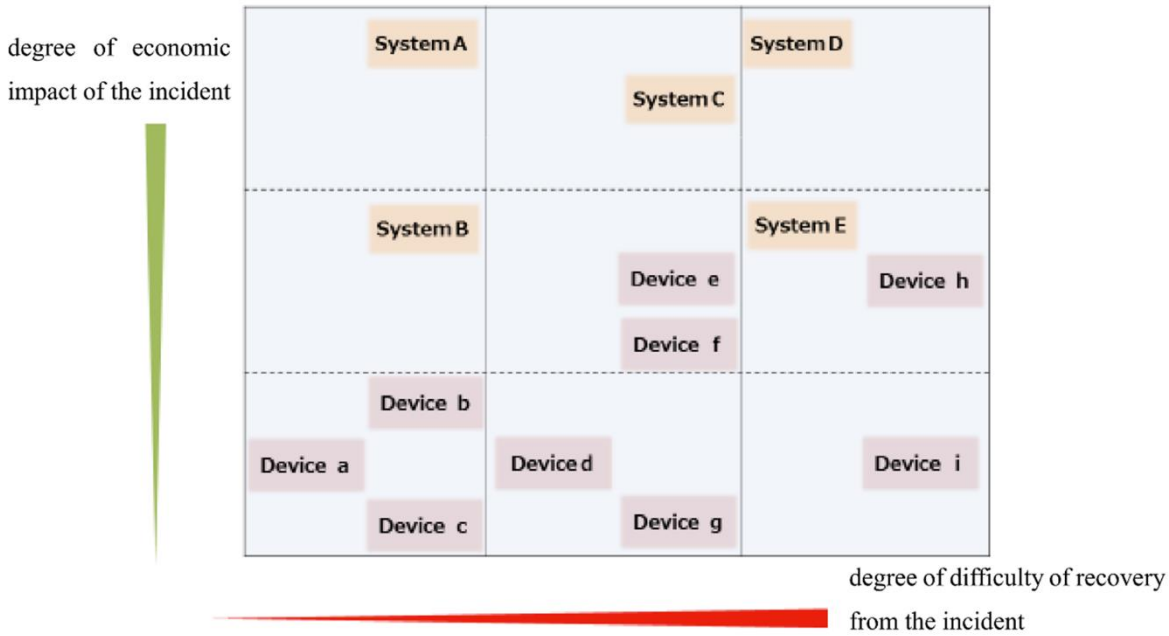
Japan's Ministry of Economy, Trade and Industry (METI) launched its IoT Security Safety Framework (IoT-SSF) in 2020. It is designed to enable players in different industries to use the same approach for reviewing the security and safety in devices and systems and not to establish mandatory rules uniformly applying 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 3**).

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 4: Japan, the categorization of devices and systems connecting physical space and cyberspace



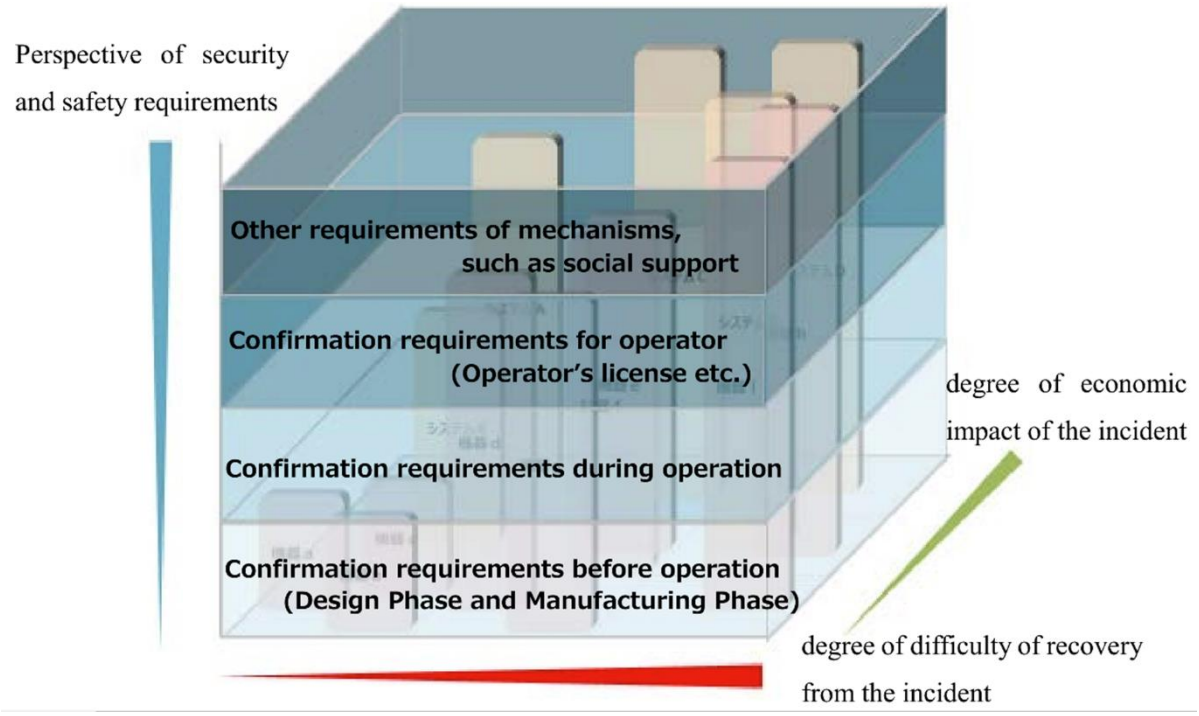
Source: Japan METI IoT Security Safety Framework

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 5: Japan, the perspective of security and safety requirements based on the category



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 as 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.

Singapore

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

Figure 6: Singapore, Cybersecurity Labeling Scheme label

Source: Cyber Security Agency of Singapore

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 Cyber Security Agency of Singapore and the National Cyber Security Centre, Finland signed a memorandum of understanding for mutual recognition of each other's labeling schemes and associated processes.

South Korea

South Korea's Internet and Security Agency (KISA) has introduced a Certification IoT of 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 to more than 12 weeks) and different costs for each level of certification.

Figure 7: The three levels of Korean IoT device security certification

Source: South Korea Internet and Security Agency

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 operating system; 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 is carried out by the Korea Institute of Mechanical, Electrical, and Electronic Testing (KTC) and the Korea Information and Communication Technology Association (TTA).

Korea's approach to IoT security is mainly aimed at manufacturers of components and ICT products. Despite its early and advanced approach to IoT certification, the government decided in May 2022 to ease its regulations on the ICT sector as part of a drive toward deregulation. Whether or how this will affect its new IoT security certification regime is uncertain.

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 similar to the EU's GDPR, covering data collection, processing, storage, consent, and protocols. 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, with specifications similar to ETSI 303 645, for manufacturers 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 a number of laws and guidelines.

The European Union

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 developed at a central level before being implemented by each member state. There are a number of EU specifications related to IoT security. Some particular 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 will be mandatory from August 2024. 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 or access of personal data
- Reducing the risk of monetary fraud, focusing on better authentication and control when monetary payments are being 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.

The GDPR Directive

Data created and transmitted 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.

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 upon in May 2022. NIS 2 came into force in the EU on January 16, 2023. It builds on and will replace the existing directive. The EU Agency for Cybersecurity (ENISA) will continue to support the implementation of the NIS Directive, and member states will have 21 months to transpose NIS2 to their national legislative framework. 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.

The Cybersecurity Act

The business services accompanying IoT devices 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. Initially ENISA's certification and labeling schema will be voluntary.

Medical Device Regulation

Medical IoT devices are covered by the EU's Medical Device Regulation (MDR 2017/45), which applies stricter standards for medical devices throughout their lifecycles, including conformity assessments.

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 Cyber Resilience Act

The Cyber Resilience Act is currently in draft form. It 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 digital elements used by both enterprises and consumers, including consumer IoT. The Act states that industry will

- Create conditions focusing on the secure development of products with digital elements, ensuring hardware and software products are placed on the market with fewer vulnerabilities, ensuring a focus on security throughout the entire lifecycle
- Create conditions that allow users to take cybersecurity into account when selecting and using these products
- Ensure manufacturers improve the security of products from design and development through the whole lifecycle
- Ensure a coherent framework to facilitate compliance for producers
- Enhance the transparency of the security properties of these products
- Enable businesses and consumers to use the products securely

Devices are divided into criticality categories: “Class I and Class II Critical” devices, which comprise 10% of products, and a “Default” category, which comprises 90% of products. The default category will be subject to self-assessment rather than third-party involvement.

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 a clear and understandable instructions for use, with security updates for at least five years

Member states have 24 months to implement these new requirements, with the exception of a more limited 12-month grace period concerning manufacturers’ reporting obligations.

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 granted cybersecurity providers “security visas” to signify compliance with certification requirements. The scheme covers three areas:

- Regulatory – meeting French and EU legislation that enforces 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
- Critères Communs (CC) – an international (ISO/IEC 15408) seven-layer test of a product's security based on assessments of the product within its development environment and resistance to a given potential attack

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.

Figure 8: An example German BSI IT security label

Source: German Federal Office for Information Security

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's 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.

Spain

The Spanish government implemented its National Cybersecurity Strategy in 2019, replacing its first 2013 version. It includes a number 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:

- INCIBE-CERT, 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 organizations can take to minimize the risks of suffering associated security incidents.
- CCN-CERT, which is part of Spain's National Intelligence Center, covers government institutions. It has responsibility 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 has as yet no compulsory certification or schemes for IoT device security.

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

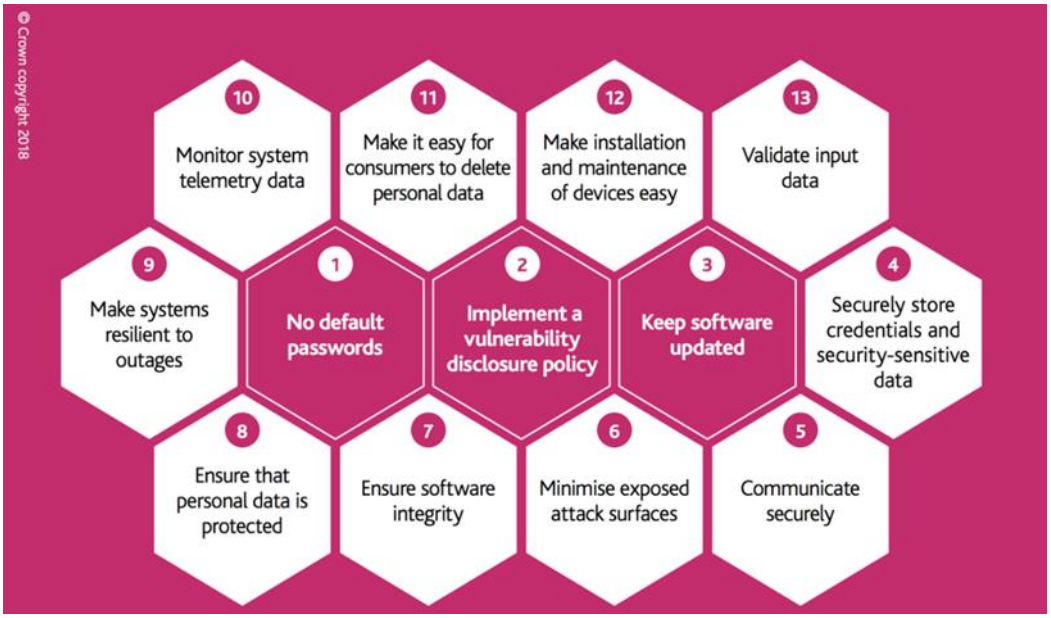
- Ensuring that consumer connectable products, such as smart TVs, internet-connectable cameras, and speakers, are more secure against cyberattacks, protecting individual privacy and security
- Requiring manufacturers, importers, and distributors to comply with new security requirements relating to consumer 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 which 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 requirements will be mandatory for suppliers when regulations come into force. Of the 13 areas that the DCMS indicates suppliers should address in the prior Bill (illustrated below), numbers one through three are considered the most important.

Figure 9: The UK's DCMS Code of Practice for Consumer IoT Security, 13 areas



Source: UK DCMS

The UK has based its approach on its publication in 2018 of a code of practice that is largely consistent with ETSI's 303 645 13 guidelines. It has not yet introduced a compulsory certification process or labeling scheme.

Americas

Brazil

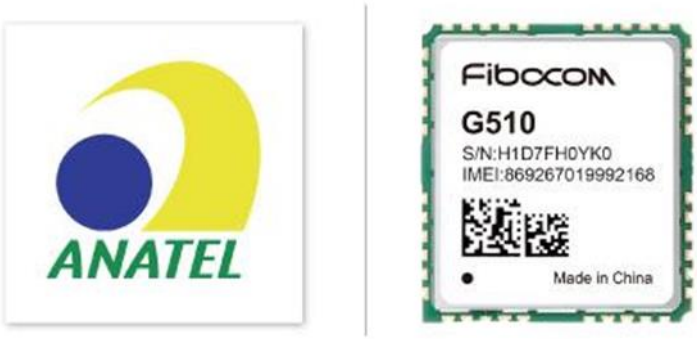
Brazil has recognized the importance of IoT, signing its National Plan of IoT into law in 2021. It also recognized the importance of data privacy in a similar way to the EU's GDPR. The General Law of Personal Data Protection (LGPD) became law in 2020, along with sanctions that would be applied by the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

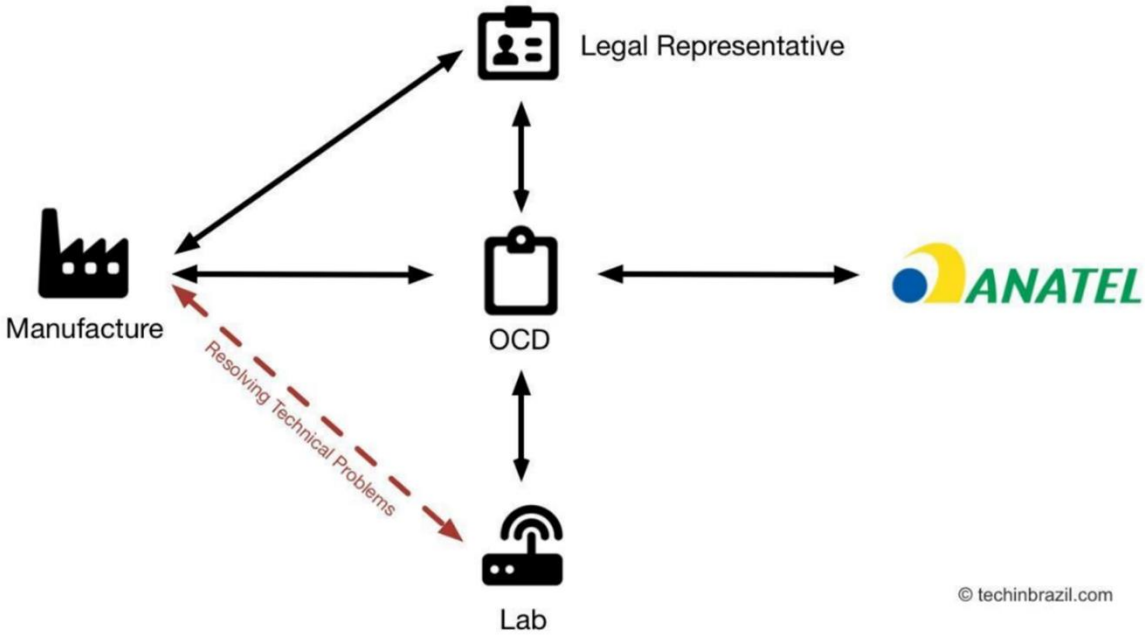
Figure 10: An example Brazilian Anatel certificate of conformity label



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 11: 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 the technology 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 a number of documents including a 2022 paper, "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products," in 2022.

NIST has been active in addressing the need for consumer IoT security. The president's 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.

Meanwhile, 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 is planning to roll out a similar IoT-labeling program with a 2023 launch target.

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

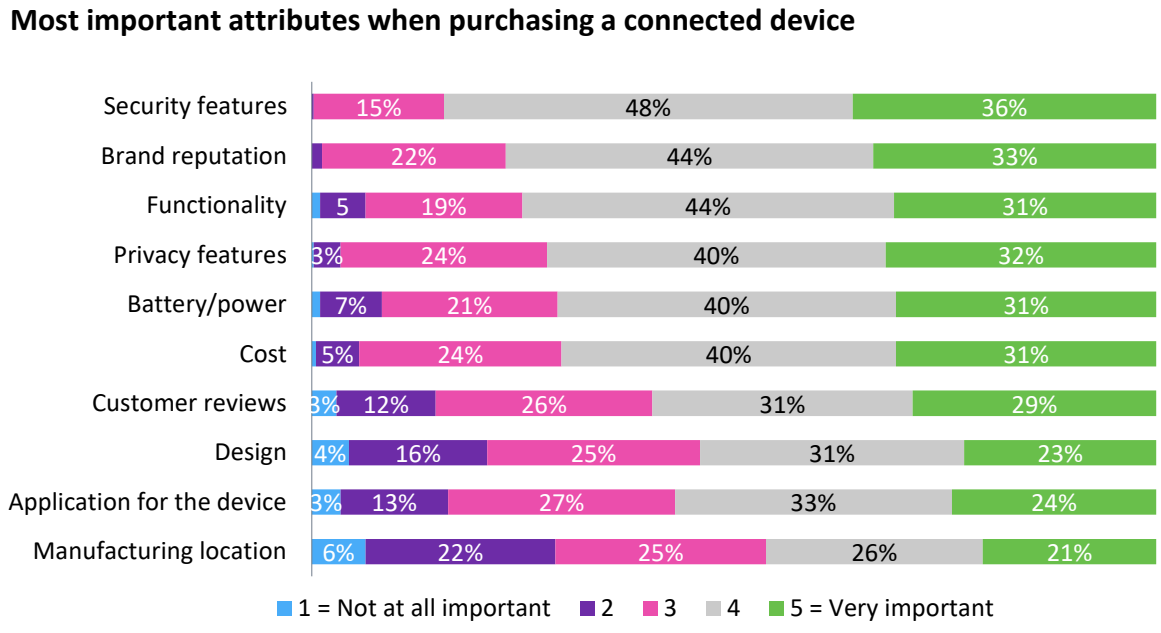
The labels are expected to be “globally recognized” and will be initially targeted to what the White House called the highest-risk devices, such as routers and home cameras. Though it is still under discussion, it is expected that these labels will take the form of a code (such as a barcode or QR code) that users can scan using their smartphone rather than a static paper label. The scanned barcode would then link to information the labeling program would define, such as software updating policies, data encryption approach, and vulnerability remediation.

Part 2: Voice of the consumer

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 12: Security is the most important purchasing attribute

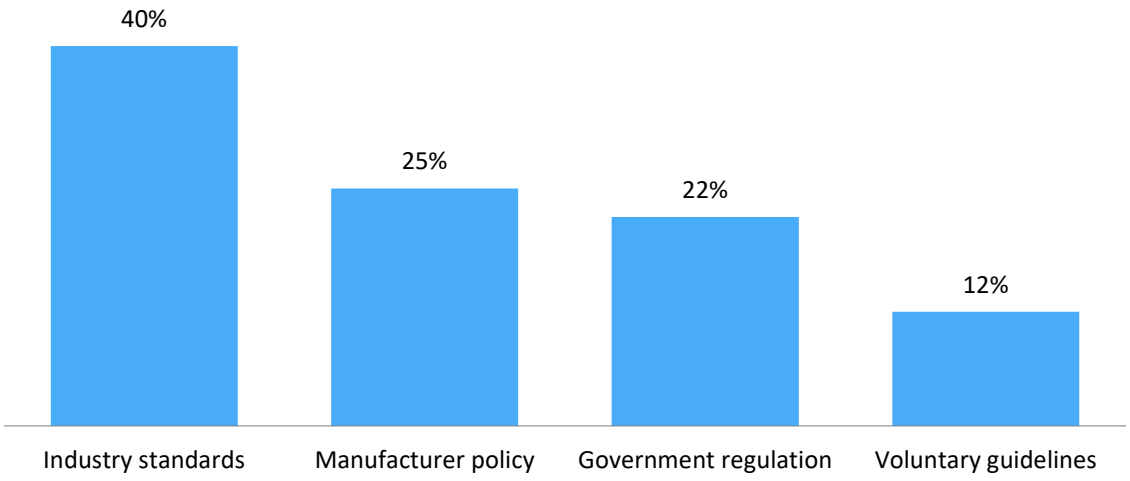


Note: n=409, all regions

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 13: How should security be implemented?



Note: n=409, all regions

© 2023 Omdia

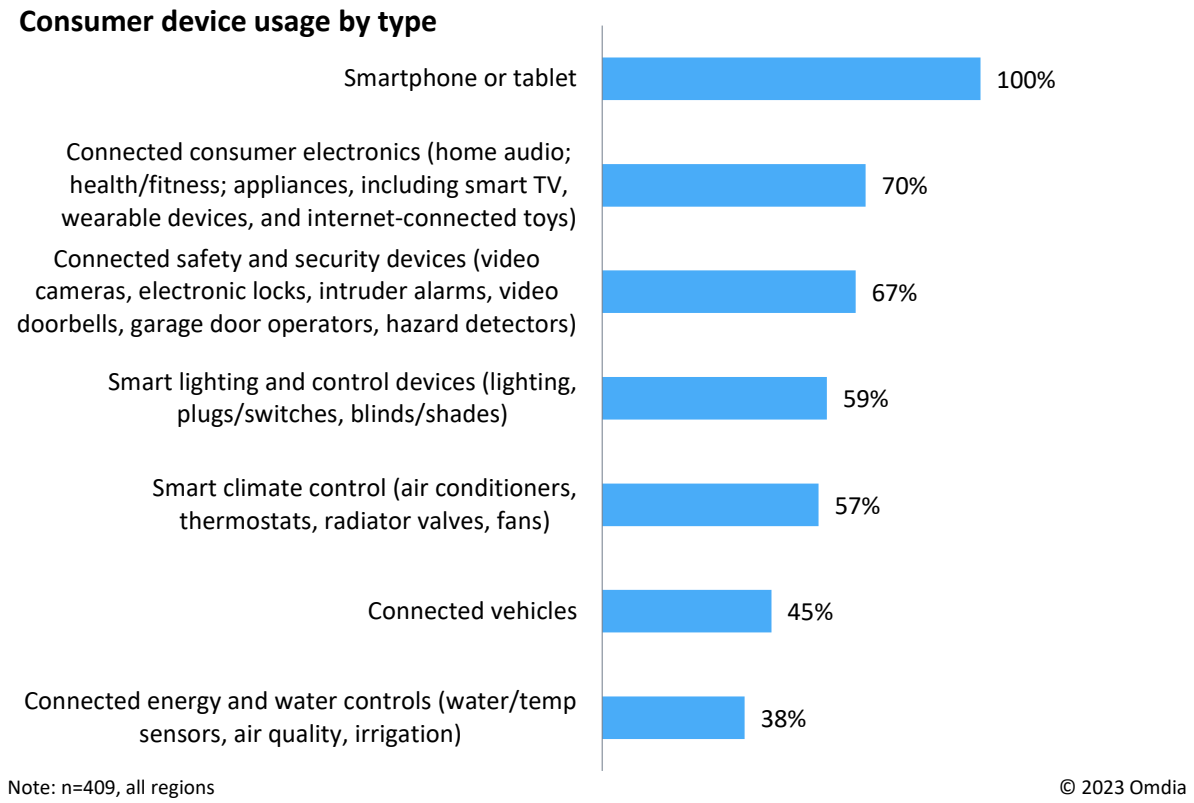
Source: Omdia

Equally interesting is that government regulations were cited next, only 3 percentage points lower than manufacturers, suggesting that even with standards and manufacturer compliance, government, regulators, and policymakers should be considered 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% with between 11 and 20 devices. Although all users reported using mobile phones and tablets, electronics and safety devices are 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.

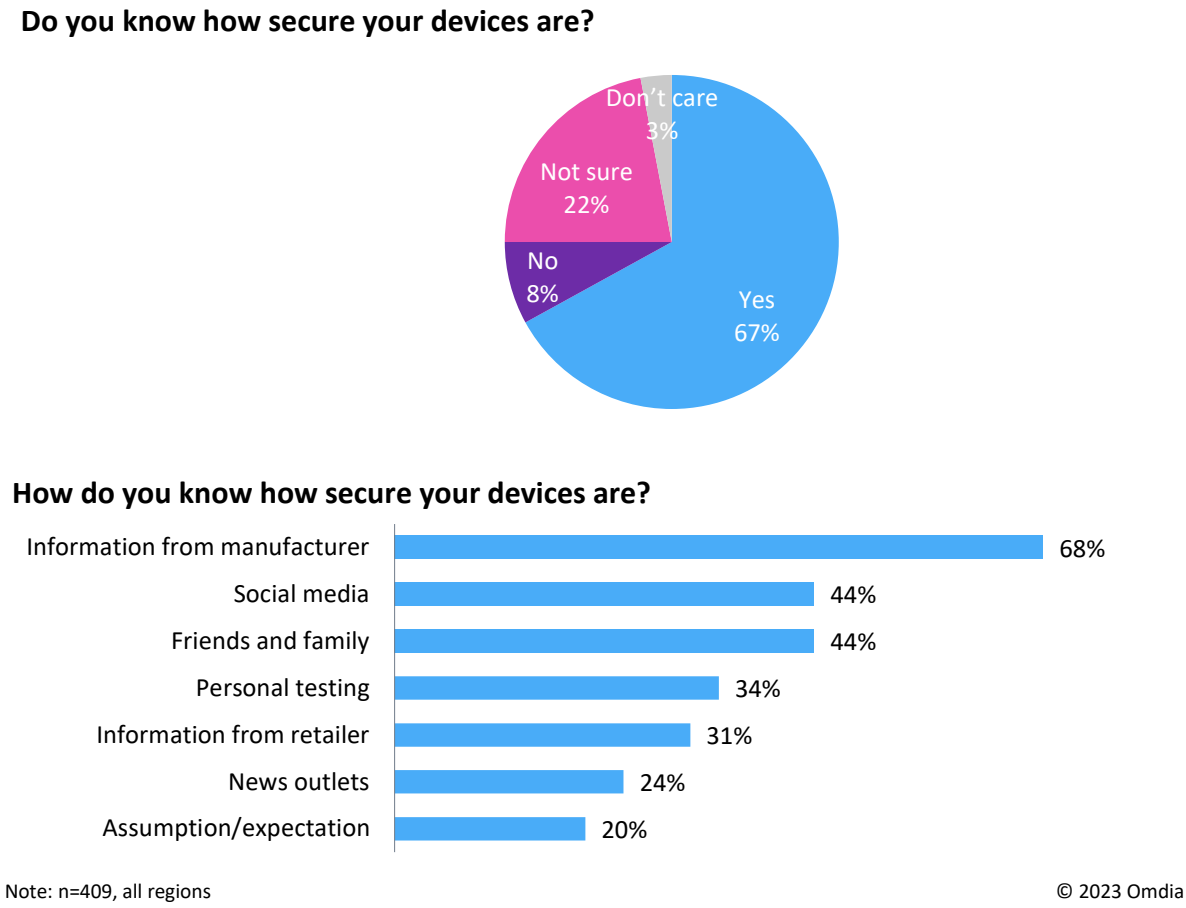
Figure 14: The majority of respondents use comfort, convenience, and safety smart products



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

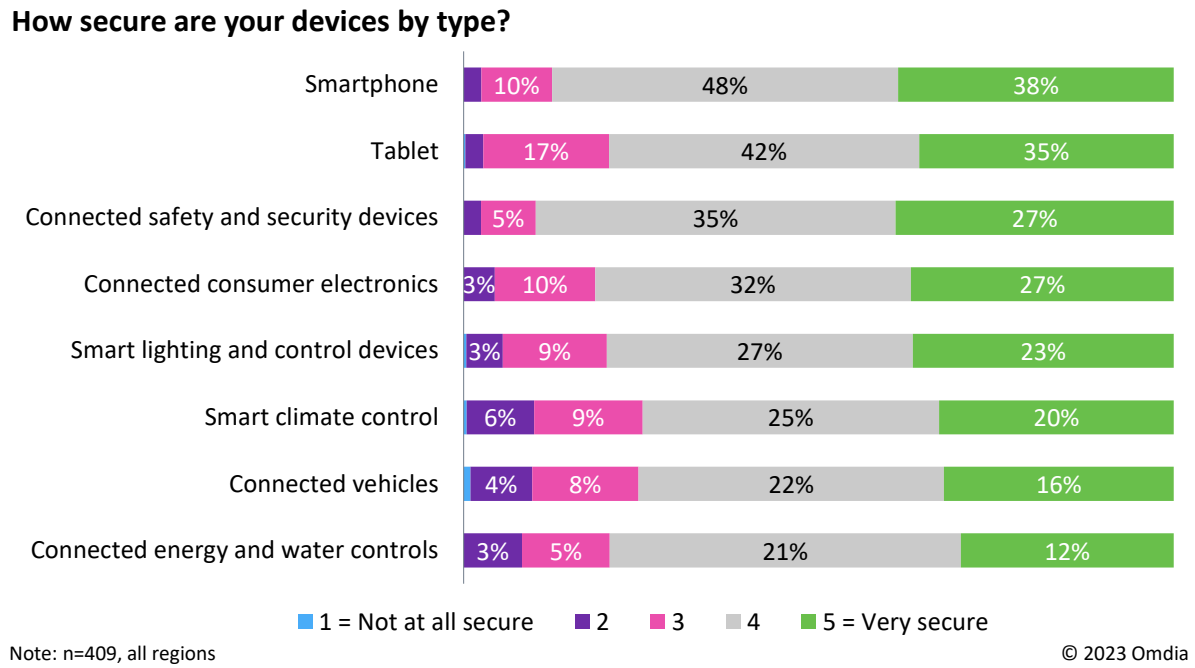


Note: n=409, all regions

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 16: Perceptions of security vary by device type



Note: n=409, all regions

Source: Omdia

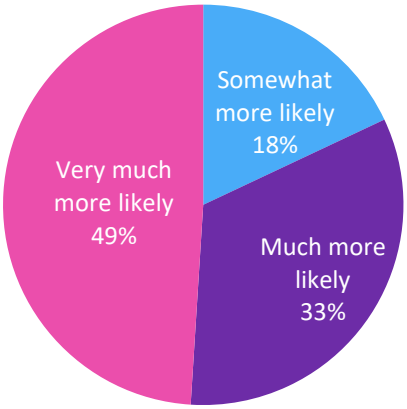
When security concerns were asked about, data protection was the top-rated concern: more than 70% of respondents rated it a major concern or a concern. Data protection included personal data not being protected and related issues such as not having secure backups to protect the data and the inability 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 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 seem 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 17: Likelihood of purchasing device with a privacy/security label

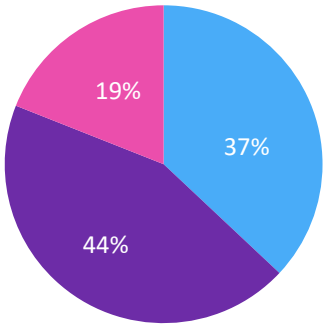


Note: n=409, all regions

Source: Omdia

In alignment with having more connected and digitally savvy consumers, the majority were also in favor of having dynamic and up-to-date information on a product's privacy and security always available. Eighty-one percent preferred a label with either a reference URL linked to a manufacturer's web site or a QR code allowing them to get the latest data on any product.

Figure 18: What kind of label do you prefer?



- Label with QR code that can be scanned to access privacy and security information
- Label with reference URL to website where privacy and security information can be obtained
- Static label with symbols, texts, or checkboxes that explain the privacy and security practices

Note: n=409, all regions

Source: Omdia

Conclusion: Time for reliably secure IoT products

Interviews with more than 400 consumers in 12 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, those 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 15 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 the majority of countries researched are planning to adopt the guidelines.

Additionally, key national initiatives should also 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 in order 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

ETSI, “Consumer IoT security,” www.etsi.org/technologies/consumer-iot-security

ETSI, “ETSI EN 303 645 V2.1.1 (2020-06),”
www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

ETSI, “ETSI TS 103 701 V1.1.1 (2021-08),”
www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

ISO/IEC, “ISO/IEC

DIS 27402 Cybersecurity — IoT security and privacy — Device baseline requirements,” www.iso.org/standard/80136.html

NIST, “Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software,” www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0

NIST, “NISTIR 8425: Profile of the IoT Core Baseline for Consumer IoT Products,”
https://csrc.nist.gov/publications/detail/nistir/8425/draft

Authors

Hollie Hennessey
Senior Analyst, IoT Cybersecurity
customersuccess@omdia.com

Mike Sullivan-Trainor
Director, Consulting Cybersecurity
customersuccess@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.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 Tech, 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