INTERNET
STANDARDS,
SECURITY AND
SAFETY COALITION
(IS3C)

MAKING THE INTERNET
MORE SECURE AND SAFER

Saving the World from an Insecure Internet of Things

An IS3C research report by

Nicolas Fiumarelli

Chair of IS3C Working Group 1 on Security by Design and co-founder of IoT CyberSec LAC (IoTcsLAC)

and

João Moreno Falcão

Intelliway Technology

Preface

This report presents the findings and recommendations of a research project on security policies and practices relating to the Internet of Things (IoT) that was undertaken in 2022-23 by the UN Internet Governance Forum's dynamic coalition on Internet Standards, Security and Safety (IS3C). The project's aims were i) to gain a better understanding of how governments and regulators worldwide are developing policies that will strengthen the security of the Internet of Things (IoT); and ii) to identify policy approaches and best practices that could form the basis of recommendations that will lead to more consistent implementation of IoT security standards and practices worldwide.

IS3C was launched at the virtual IGF in 2020 as a multistakeholder coalition with the objective of improving Internet security and safety through wider and more effective adoption of security-related Internet standards and ICT best practices in the public and private sectors.

The coalition's work programme brings together key security supply and demand factors to propose optimal policies and practices for deploying key standards. The outcomes are presented as policy recommendations, guidelines and toolkits for policymakers, decision-makers, and capacity-building programmes worldwide.

Information about IS3C's working group programmes, mission statements, work plans, and timelines can be found on IS3C's website at https://is3coalition.org/ and on the UN Internet Governance Forum (IGF) website at https://www.intgovforum.org/en/content/internet-standards-security-and-safety-coalition-is3c .

This report was written by the project leader and Chair of IS3C Working Group 1 Nicolas Fiumarelli, with the assistance of João Moreno Falcão, leading member of the research team. Editing assistance and support was provided by Mark Carvell, IS3C senior policy adviser and Maarten Botterman. The authors also acknowledge the valuable contributions from the members of the research team Oscar Giudice, Sávyo Vinicius de Morais, and Victor de Pan, and the overall management provided by the IS3C's coordinator Wout de Natris. Special thanks is given to Maarten Botterman for editorial advice.

The initial project planning was carried out by Yuri Kargapolov, the first chair of Working Group 1 on Security by Design, and member of the Coordination Council for the Ukrainian Network Information Center (UANIC).

IS3C is grateful to Microsoft for sponsoring this research project and to Rob Spiger and Elizabeth Eigner in Microsoft's team for their active support.

Executive summary

Adopting a comprehensive security by design approach ensures the resilience and integrity of our interconnected world, making it imperative for organisations to prioritise security measures and incorporate them into the core design of their IoT systems.

The Internet Standards, Security and Safety Coalition (IS3C) conducted a study on the policies and practices related to the security of the Internet of Things (IoT) across national and regional levels. The research provides valuable insights into the best practices that can be implemented to enhance IoT security and its findings and recommendations have significant implications for the industry and manufacturing sectors where IoT systems are increasingly being adopted

The research team analysed over national and regional documents relating to IoT security and identified 442 practices in 30 specific IoT security policy and regulatory initiatives, from 18 national and regional administrations[1]. These practices were grouped into four categories.

1. **Data Privacy and Confidentiality** - includes secure data encryption, access control, minimization of exposed attack surfaces, authentication systems, regular security assessments, and compliance with data protection regulations.
2. **Secure updating -** includes updating software and firmware, restricting unauthorised installations and implementing a security updates policy.
3. **User empowerment -** practices that empower users to take an active role in securing their IoT devices through vulnerability disclosures and reports, educational programmes, and consumer awareness initiatives.
4. **Operational resilience -** practices that ensure continuous and secure IoT network and device operation through secure network configurations, logging of security incidents, having disaster recovery plans, having regular security incident monitoring, and securing product disposal or end-of-life strategies.

The research was conducted on the basis of five policy questions relating to: responsibilities of stakeholders; government policies and regulations; user empowerment; compliance with existing standards; security updating; and global adoption of standards. The main conclusions drawn from this research are:

- IoT security is a complex and multifaceted issue that requires a comprehensive approach;
- Many countries (including almost the whole Global South) lack any policy framework for IoT security;
- Many of the national practices identified did not match other countries' policies and there are many differences in taxonomy;

[1] There is an overview in the annex to this report.

- Many of the practices are voluntary guidelines without effective accountability and consequences for non-deployment;
- National administrations rarely require or specify security by design in the hardware and software that they procure. This would drive and increase the deployment of security-related standards;
- The standards that form the public core of the Internet and on which the Internet runs, are not formally recognised as such by governments and are usually absent in policy documents such as those analysed in this research;
- Specifying links between security flaws and device integrity is a strong basis for security updates.

The research team drew up a series of four policy recommendations on the following issues:

1. Accountability frameworks from the design-stage through to use;
2. Strategies for countering unauthenticated vulnerabilities such as denial of service attacks;
3. Stakeholder cooperation on coordinating vulnerability disclosures;
4. Endorsing global implementation of open standards.

The research by IS3C highlighted the critical importance of multistakeholder cooperation between governments, industry, and the wider community of consumer and user stakeholder interests, as being essential to have the global adoption of IoT security standards and practices become the standard practice. The report concludes with a set of proposed next steps for specific stakeholders to undertake in pursuit of this goal that will establish a more secure and safer global IoT environment.

The next steps include launching targeted awareness campaigns for both the public and private sectors. It is vital to provide government policymakers and regulators with a deeper understanding of IoT security, leading to strengthened IoT policy frameworks that integrate robust compliance standards and actionable guidance.

A good example is the importance of embedding cybersecurity standards in procurement decisions and procedures and in educational initiatives. Users are urged to actively participate in securing their IoT devices, e.g. by demanding secure by design devices. Operational resilience can be bolstered through strategies like secure network configurations and disaster recovery plans.

Collaborative endeavours, especially with consumer protection and advocacy organisations, are pivotal to champion IoT security labelling schemes. A deeper dive into IoT security measures and a commitment to engage with standardisation bodies, such as the IETF, are also recommended.

Observing the increasing attention for governments, we believe that much can be learned from global good practice, and we are confident that the first steps we observed today will be followed by better informed interaction, taking into account that IoT is truly deployed globally - and it can help build a world we want.

Part 1: IS3C’s IoT security by design research project

This part provides an overview of the research's objectives, methodology, and initial findings, and sets the stage for a deeper exploration of best practices and recommendations in subsequent sections.

i. Addressing the Challenge of a Secure and Safe Internet of Things

The rapid growth of the Internet of Things (IoT) has become an important social and economic issue for governments and the technology sector. The number of consumer goods and devices connected to the internet continues to increase, and connectivity is now ubiquitous and all but the standard. From coffee machines to cars and refrigerators to cell phones, they are connected while data flows to and from them. IoT is also having a transformational impact in the manufacturing sector through wider use of sensor technologies, for example in remote monitoring and maintenance. The healthcare sector is also widely adopting IoT technologies, e.g. to monitor patients, while in the agricultural sector IoT applications monitor livestock farming and make growing vegetables and plants more efficient. Many of these applications are combined with powerful data analysis capabilities that transform the way we work and live. The projected impact of IoT technologies on national economies is significant. Where an analysis from 2017 predicted there would be almost twenty billion devices connected to the Internet by 2025, with a potential contribution to the global economy of US$11 trillion[2], a more recent one predicts 29.5 billion by 2030 (see fig. 1).

However, the evolution and spread of IoT also raises significant cyber policy challenges that could make it difficult to achieve its potential benefits. News about attacks on Internet-connected devices, fear of surveillance, privacy-related concerns and theft of confidential material and digital money have already caught the public's attention.

[2] Internet Society’s IoT Overview - https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

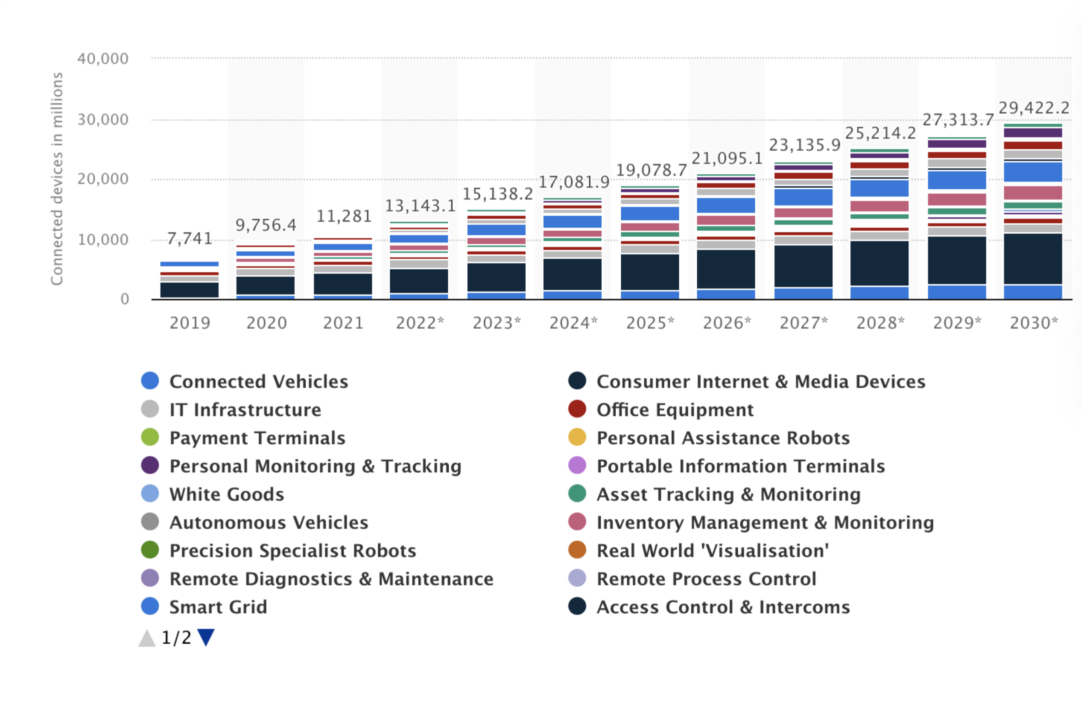

Fig. 1. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by vertical
https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/

ii. The Research Questions

The IS3C stakeholder coalition believes it is essential to address the vulnerabilities associated with IoT technologies and to develop strategies to mitigate risk and harm. A working group dedicated to IoT security and safety (IS3C WG1) was established in 2021 with the aim of developing guidelines and recommendations to promote the adoption of security-related standards and best practices for IoT technologies. The following five research questions were agreed for this project:

1. What are the recommended best practices for setting out the responsibilities of all stakeholders involved in IoT security, including manufacturers, service providers, and users?
2. What policy and regulatory measures can be identified for promoting IoT security by design, specifically with regard to ensuring device resilience against crashes, power shortages, and outages?
3. What policy and regulatory guidelines can be identified to promote user empowerment in IoT security, and what are the recommended best practices for implementing vulnerability disclosure mechanisms?
4. Through what mechanisms are regulators and policymakers enforcing compliance with established IoT security standards and encouraging manufacturers to adopt the recommended best practices?
5. How do policy and regulatory documents relate security updates with warranty policies for IoT devices and services?

As a first step in identifying and mapping current policies, initiatives and practices worldwide relating to IoT security, IS3C's members and the wider IGF community were requested by the WG1's research team to assist in identifying national and regional policy documents and statements that were related to IoT. The research team developed a repository of 30 documents from the following 17 countries and regions: Argentina, Brazil, Canada (2), European Union (2), Egypt, Finland, India, Japan, Kenya, South Korea, Saudi Arabia, Singapore, The Netherlands (5), United Kingdom, United States of America (7), United Arab Emirates, and Uruguay.

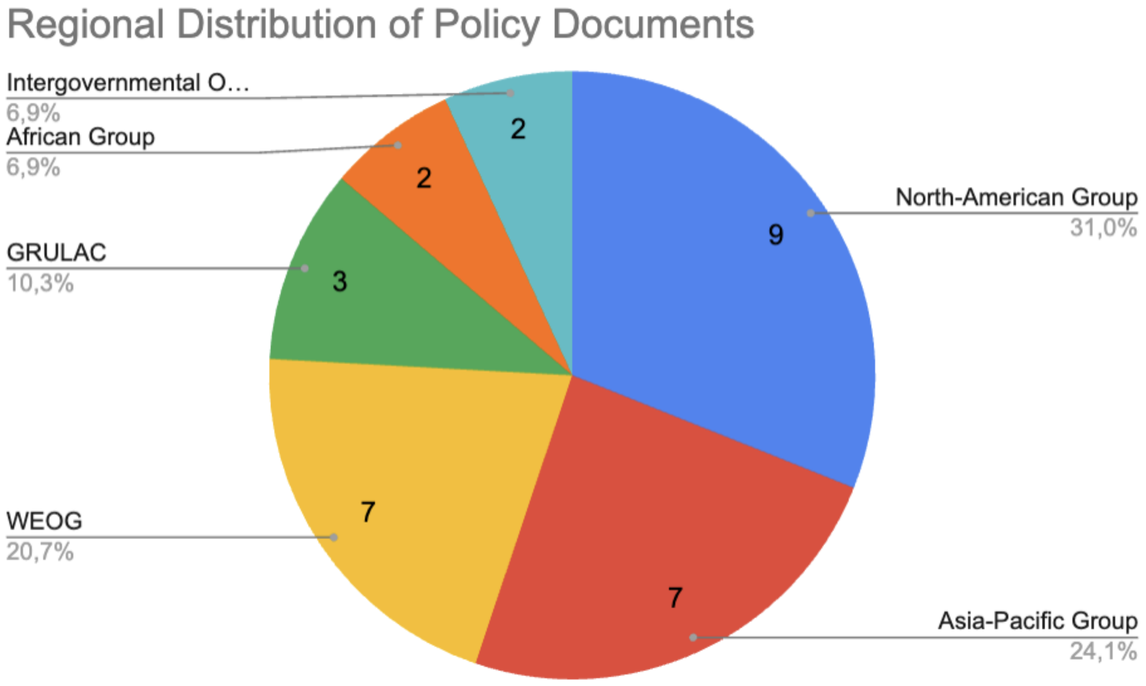

Fig. 2. Regional Distribution of Policy Documents

The research team analysed these documents in order to identify the main provisions of national government policies and regulatory frameworks, regulators' statements, codes of practices, and initiatives related to IoT security, along with legislative and regulatory impact assessments.

The research team found, however, that the number of policy documents related specifically to IoT security was quite limited. In particular, there were significant regional gaps (see fig. 2). For instance, Africa, Latin America, and the Caribbean have very few policies focused on IoT.

Nonetheless, it was noted that there is a growing recognition in all regions of the need to assess the security vulnerabilities of IoT products. On the one hand, it is suggested that this research should be repeated in the future, to include new policy documents and IoT initiatives that are expected to emerge from 2023 onwards to provide valuable insights into the evolving policy landscape on IoT security. On the other hand, this document presents the current best practices in the world and contains recommendations for improvements that can assist policymakers and provides them with an overview and starting point for their future work.

iii. Analysis of IoT Policy Documents

The IoT policy documents that were analysed are listed in Annex 1 and encompass a wide array of topics pertinent to security. While they all underscore the significance of robust security measures, user empowerment and transparency, their methodologies and focal points differed however. The analysis provided a comparative overview highlighting common themes, unique approaches, and best practices. The following summary provides the key points from the comparative overview.

Most of the documents accentuate the necessity of a secure design, routine software updates and the eradication of recognized vulnerabilities. They also emphasised the pivotal role of consumers in IoT security, offering guidelines to facilitate their secure use of IoT devices.

Policy documents such as Brazil's Cybersecurity Requirements for Telecommunications Equipment (#01 in the list at Annex 1) and the US Senate Bill No. 327: Security of Connected Devices (#02) lean towards the technical facets of IoT security, encompassing encryption and secure updating.

However, Canada's Internet of Things (IoT) Checklist for Consumers (#10) and the United Kingdom's Code of Practice for Consumer IoT Security (#30) are more consumer-centric, emphasising education and awareness.

Several documents such as Singapore's Cybersecurity Labelling Scheme (CLS) (#05) and Cybersecurity Labelling Finland Traficom (#06), advocate labelling or certification schemes which enhance the transparency of IoT device security features.

Others such as the United States' NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline (#07) and NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers (#13), provide voluntary guidelines or best practices for manufacturers.

Only a few policy documents set out a direct regulatory approach to IoT security, notably Saudi Arabia's Internet of Things Regulatory Framework (#14) and the United Arab Emirates' Internet of Things Regulatory Policy (#15).

Many of the documents endorse various best practices for IoT security including secure design, frequent software updates, elimination of known vulnerabilities, consumer education, transparency, and collaboration among stakeholders. For example, the United States' NIST 8259 Series (#17) provides wide-ranging guidelines on IoT security, spanning both technical and non-technical dimensions.

In contrast, some policy documents covered only specific individual practices. For instance, while Brazil's Cybersecurity Requirements for Telecommunications

Equipment (#01) underscores secure design and updates, it does not cover consumer education.

Singapore's Cybersecurity Labelling Scheme (CLS) (#05) and "Cybersecurity Labelling Finland Traficom" (#06) ensure that their labelling requirements promote transparency and encourage the production and acquisition of secure devices.

All the policy documents analysed by the research team provided valuable insights into IoT security. However, their strategies and emphases differ, mirroring the variations in national contexts and priorities. Documents that are both comprehensive and innovative stand out, especially those adopting a multi-stakeholder methodology and pioneering mechanisms like labelling schemes to champion transparency and security.

iv. Review of documents under the four categories of best practices

A diverse set of 442 practices were identified in the analysis of policy and regulatory documents on IoT security[3]. These were organised into four categories with the aim of streamlining the comparison of various national approaches and providing actionable recommendations for policymakers and stakeholders. We noted consistent practices across jurisdictions, such as the necessity for software updates and secure data encryption, but also several inconsistencies such as variations in default password use and vulnerability management. It is worth noting that in addition to technical best practices there were also non-technical ones, including label presentation, consumer education programmes, and vulnerability disclosure policies.

1. Data Privacy and Confidentiality

Data Privacy is a critical aspect of IoT security. To ensure the security and privacy of personal data in the Internet of Things (IoT) devices, different kinds of best practices can be adopted, including strong encryption, mandatory software updates, vulnerability disclosure mechanisms, intuitive personal data deletion, secure user-defined passwords and two-factor authentication, firmware image integrity validation, cooperation for a common labelling scheme, failure boot recovery and outage resilience, and input data validation.

The document analysis by the researchers identified several best practices for privacy protection, including secure data encryption, access control, minimization of exposed attack surfaces, authentication systems, regular security assessments, and compliance with data protection regulations.

The policy documents analysed by the researchers from Brazil (Cybersecurity Requirements for Telecommunications Equipment - #01 in the list at Annex 1), the

[3] The complete list of all 442 best practices can be found in the research main page: https://is3coalition.org/docs-category/research-reports/

United States (Senate Bill No. 327: Security of Connected Devices - #02), and the European Union (Guidelines for Securing the Internet of Things - #22) all highlight the importance of privacy protection in IoT security. These documents are good examples of emphasising the need for secure data encryption, access control, and compliance with data protection regulations[4].

BR #01 · US #02 · CA #03 · IN #04 · SG #05 · FI #06 · US #07 · US #08 · CA #10 · JP #11
KR #12 · US #13 · AE #15 · VN #16 · US #18 · UY #20 · EU #22 · EU #23 · NL #25 · NL #27
UK #30

2. Secure Updating

Secure updating practices are crucial for maintaining the security of IoT devices. These practices include updating software and firmware, restricting unauthorised installations, and implementing a security updates policy.

The documents listed in Annex 1 from Canada (Internet of Things Security - ITSAP.00.012 - #03), Singapore (Cybersecurity Labelling Scheme [CLS] - #05), and the United States (NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline - #07), all emphasise the importance of secure updating practices. They highlight the need for updating software and firmware, restricting unauthorised installations, and implementing a security updates policy.

BR #01 · CA #03 · IN #04 · SG #05 · FI #06 · US #07 · US #08 · CA #10 · JP #11 · KR #12
US #13 · VN #16 · US #18 · UY #20 · EU #22 · EU #23 · NL #25 · NL #26 · NL #27 · NL #28
UK #30

3. User Empowerment

User empowerment practices aim to involve users in the security process. These practices include vulnerability disclosures and reports, educational programs, and consumer awareness initiatives.

[4] The numbered emblems match the numbers in annex 1 containing the overview of analysed documents.

The policy documents from India (Code of Practice for Securing Consumer Internet of Things - #04 in Annex 1), Finland (Cybersecurity Labelling - #06), and Canada (Internet of Things Checklist for Consumers - #10) highlight the importance of user empowerment in IoT security. These documents emphasise in particular the need for vulnerability disclosures and reports, educational programmes and consumer awareness initiatives such as labelling programs.

BR #01 US #02 IN #04 SG #05 FI #06 US #07 US #08 US #09 CA #10
JP #11 VN #16 US #18 UY #20 EU #22 EU #23 NL #25 UK #30

4. Operational Resilience

Operational resilience practices aim to ensure the continuous and secure operation of IoT networks and devices. The policy documents from Japan (IoT Security Safety Framework - #11 in Annex 1), Korea (Information Security Certification Criteria for Information and Communication Network Connection Devices [2021.9] - #12), and Saudi Arabia (Internet of Things Regulatory Framework - #14) all highlight the importance of operational resilience in IoT security. These policies emphasise the need for secure network configurations, logging of security incidents, having disaster recovery plans, and securing product disposal or end-of-life strategies.

BR #01 IN #04 SG #05 US #08 JP #11 KR #12 US #13 SA #14 VN #16
US #18 EU #22 EU #23 UK #30

In Annex 2 the reader can find a summary of the good practices found in the documents in a comprehensive table.

Part 2: Delving into IS3C's Research Questions

In this section, we explore the core research questions posed by IS3C, aiming to shed light on the recommended best practices, policy measures, and regulatory guidelines surrounding IoT security. By dissecting each question, we uncover the collective insights from various policy documents across different regions.

Q1. What are the recommended best practices for setting out the responsibilities of all stakeholders involved in IoT security, including manufacturers, service providers, and users?

US #08 KR #12 UK #30

The policy documents from the United States (#8), and the United Kingdom (#30) propose a collaborative approach to organising and distributing responsibilities among different stakeholders. This approach recognizes that ensuring IoT safety requires the active involvement of multiple parties. Based on these documents, a key recommendation is for policymakers to clearly define the individual responsibilities of each stakeholder in enhancing cybersecurity and safety in the IoT space.

Regarding the focus on specific stakeholder audiences, most of the documents analysed present technical requirements for devices in the form of regulatory specifications. This targeted strategy simplifies document distribution as it caters to a more homogeneous group. Notably, the Korean document (#12) stands out as an initiative addressing technical aspects for IoT developers and producers. This document employs a multilayered approach, providing both simplified and detailed descriptions of requirements. Furthermore, it includes practical examples such as protocol schemes, code snippets, and device illustrations to illustrate secure practices. This approach fosters a direct connection between regulations and engineers, streamlining compliance efforts and expediting the implementation of new requirements.

Q2. What policy and regulatory measures can be identified for promoting IoT security by design, specifically with regard to ensuring device resilience against crashes, power shortages, and outages?

BR #01 SG #05 KR #12 VN #16 UY #20 EU #23 UK #30

The research team found six national and regional policy documents which specifically addressed the need for industry to adopt security-by-design in their research and development against crashes, power shortages, and outages: Singapore (#05), Korea (#12), Vietnam (#16), Uruguay (#20) and the United Kingdom (#30).

The documents show broad consistency in their approaches, with most of them referencing the European Union (#23). The resilience described is a form of 'fault tolerance', a concept in system design that allows a system to continue operating properly even if some of its components fail. The Brazilian document (#01), while not explicitly covering fault tolerance as the other documents do, created a requirement that devices must be able to withstand distributed denial-of-service

(DDoS) attacks and so-called brute force attacks by hackers. These forms of concentrated cyber attacks are important to be addressed since the attacker usually doesn't need to be authenticated to exploit these vulnerabilities. The Korean document (#12) also addresses DDoS Attacks.

The identified policy and regulatory measures for promoting IoT security by design highlight the crucial importance of protecting systems against distributed denial-of-service (DDoS) attacks and brute-force attacks. These malicious activities pose significant threats to the resilience of systems, undermining their core pillars of functionality.

Q3. What policy and regulatory guidelines can be identified to promote user empowerment in IoT security, and what are the recommended best practices for implementing vulnerability disclosure mechanisms?

BR #01 IN #04 SG #05 FI #06 US #08 US #09 CA #10 US #18 UY #20 EU #22 EU #23

The need for implementing a vulnerability disclosure policy that allows security researchers and others to report issues is prominently mentioned across the documents. The theme of acting on disclosed vulnerabilities in a timely manner echoes across the documents. The emphasis on implementing coordinated vulnerability disclosure (CVD)[5] processes and policies underscores the importance of a systematic approach to managing IoT security risks.

These processes are typically adopted by entities involved in the lifecycle of IoT devices, including manufacturers, service providers, and businesses that utilise these devices. The goal of CVD is to ensure a clear and effective process for reporting and addressing vulnerabilities as they are discovered. The approach mentioned across the documents minimises risk by ensuring that all stakeholders have a shared understanding of how to respond when vulnerabilities are identified, thereby enhancing the overall security of IoT ecosystems.

The policy documents from India (#4), Singapore (#5), Finland (#6), the United States (#9 and #18), Canada (#10), and the European Union (#23) present an interesting perspective on the contribution of common labelling schemes to online security and safety. The requirements of these schemes, from specifying all product certifications to undergoing an information security inspection by an independent third party, underline the significance of transparency and external validation in enhancing IoT security. The references they make to security standards such as

[5] In a coordinated vulnerability disclosure process, the vulnerabilities are shared with the development team before being published. This way the devices can be safely updated before the vulnerability is publicly known.

ETSI EN 303 645, OWASP IoT TOP 10, OWASP Mobile Application Security Verification Standard (MASVS), EUCS, ISO 27000, and Cloud Security Alliance (CSA), further illustrate the importance of adherence to globally recognized benchmarks.

Documents from the European Union (#8, #22 and #23), and Uruguay (#20) underline the importance of transparency and global cooperation. They stress the importance of stakeholders, particularly suppliers, in providing clear information about the operation of their products. This transparency extends to risk assessments which should account for both internal and third-party risks. The global nature of digitalisation and network security necessitates cooperation on a global scale, including the development of standards for technical interoperability and regulatory coherence.

The documents from the United States (#9 and #18), Uruguay (#20), and the European Union (#22) offer insights into the role of education and awareness campaigns. They emphasise the role of manufacturers in creating awareness of cybersecurity-related information and features of IoT devices. Manufacturers should also be able to identify potential risks and provide comprehensive user guides or manuals to promote safe and secure use of their products.

The importance of incident audits is highlighted in Documents (#1, #20, and #22). These documents recommend allowing security events to be stored in external repositories to avoid data loss. They also underscore the need to perform audits and monitor security events, with an emphasis on minimising trust assumptions where feasible. The idea of sharing knowledge and promoting communication of findings reiterates the importance of transparency, while the call to act in a timely and coordinated manner underscores the importance of swift, collective action in reducing vulnerabilities.

Q4. Through what mechanisms are regulators and policymakers enforcing compliance with established IoT security standards and encouraging manufacturers to adopt the recommended best practices?

US #02 SG #05 FI #06 US #07 US #09 JP #11 US #13 US #17 US #18

Regulators and policymakers employ a variety of mechanisms to enforce compliance with established IoT security standards and encourage manufacturers to adopt the recommended best practices. These mechanisms can be broadly categorised into i. regulatory measures; ii. incentive programmes; iii. education and awareness campaigns ; iv. mandatory vulnerability disclosure policies; and v. labelling schemes. These are described below with examples. It is important to note, however, that the effectiveness of these mechanisms can vary depending on the specific context and regulatory environment. A combination of these approaches is often necessary to promote and deploy IoT security standards effectively.

i. Regulatory Measures

These are legal requirements that manufacturers must meet to sell their products in a particular jurisdiction. For instance, the European Union's General Data Protection Regulation (GDPR) imposes strict requirements on data protection and privacy, and non-compliance can result in hefty fines. Similarly, the California Senate Bill No. 327 (#02) requires manufacturers of connected devices to equip them with reasonable security features.

ii. Incentive Programmes

Policymakers often use incentives to encourage manufacturers to adopt best practices. These incentives can take various forms, such as tax breaks, grants, or preferential treatment in public procurement processes. For example, Singapore’s Cyber Security Agency's Cybersecurity Labelling Scheme (CLS) (#05) aims to incentivise manufacturers to adopt robust security measures by providing them with a cybersecurity label that can enhance their products’ marketability.

These partnerships involve collaboration between government agencies and private sector companies to promote and implement best practices. For instance, the National Institute of Standards and Technology (NIST) in the United States (#07, #09, #13, #17, #18) works closely with industry stakeholders to develop and promote cybersecurity standards.

iii. Education and Awareness Campaigns

Education and awareness campaigns are a key strategy employed by policymakers to inform manufacturers and end-users about the importance of IoT security and the best practices they can adopt. These campaigns can take various forms, including workshops, seminars, and online resources, and are crucial in fostering a culture of security in the IoT ecosystem.

Several of the policy documents analysed emphasise the importance of education and awareness campaigns in promoting IoT security. For instance, the NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline (#07 in the list at Annex 1) from the National Institute of Standards and Technology (NIST) in the United States highlights the role of manufacturers in providing education and supporting materials for establishing roles to support IoT device policies, procedures, and associated documentation.

The "IoT Security Safety Framework" (#11) issued by the Ministry of Economy, Trade and Industry (METI) in Japan, also acknowledges the lack of end users' technical expertise and the need to educate them. This document suggests that education and awareness campaigns are crucial in bridging this knowledge gap.

iv. Mandatory Vulnerability Disclosure Policies

Some jurisdictions require manufacturers to disclose vulnerabilities in their products and provide timely fixes. This encourages manufacturers to prioritise security in their design and development processes.

v. Labelling Schemes

Labelling schemes are an increasingly popular mechanism used by regulators and policymakers to enforce compliance with IoT security standards and encourage manufacturers to adopt best practices. These schemes provide a clear, consumer-friendly indication of a product's security features, helping consumers make informed purchasing decisions and incentivizing manufacturers to improve their security practices.

For example, the Singapore Cyber Security Agency's Cybersecurity Labelling Scheme (CLS) (#05 in the list at Annex 1) is an excellent example of this approach. The CLS is designed to inform consumers about the level of security in smart devices, helping them make informed choices and fostering a market environment where manufacturers are incentivized to enhance the security of their products. The scheme rates devices on a scale, with higher levels indicating more robust security features.

The Cybersecurity Labelling Finland (#06) is an example of a similar labelling scheme which aims to increase transparency about the security features of IoT devices and encourage manufacturers to prioritise security in their design and development processes.

The "Recommended Criteria for Cybersecurity Labelling of Consumer Internet of Things (IoT) Products" (#18) by the National Institute of Standards and Technology (NIST) in the United States provides guidelines for developing and implementing such labelling schemes. It emphasises the importance of clear, understandable labels that accurately represent a product's security features.

Q5. How do policy and regulatory documents relate security updates with warranty policies for IoT devices and services?

SG #05 FI #06 US #08 CA #10 KR #12 EU #23 NL #25 NL #28 UK #30

The ETSI regulation (#23) requires the producer to provide security updates for as long as the device warranty. This is an important specification since security flaws must be interpreted as a violation of the integrity of the device. The regulation is incorporated in Finland's IoT security labelling system (#06) as a mandatory requirement. It is also recommended in Singapore's Cybersecurity Labelling Scheme (CLS) (#05). It is worth noting, however, that IoT cybersecurity labelling schemes are not mandatory in any country.

The labelling scheme document (#12) from Korea is intended to create a warranty link with device updates by requiring the producer to provide technical support to fix update failures during the warranty time. However, this requirement is only enforced for the highest label tier intended for medium to large IoT appliances.

Most of the policy documents analysed by the researchers treat security updates as a new category of support to clients. This means that it is not treated as a defect as such. In the document from the Netherlands (#28), a producer is advised to give security updates proportionally to the cost of the device, without specifying a minimum period. In another document from the Netherlands (#25) states that the producer must create an end-of-life policy describing the minimum time during which they provide updates. and that they are working to make security updates mandatory. A requirement for an end-of-life policy also appears in documents from the United States (#8) and the United Kingdom (#30).

The regulation effort focuses on defining the security requirements of the software update system rather than enforcing the update response time for new vulnerabilities or specifying for how long updates will be provided. The only document asking for consumers to take into account security updates support is the Canadian Checklist for Consumers (#10).

EU members are obliged to implement the EU regulation (#23) which requires producers to provide security updates throughout the device's warranty period. Policies like this being practised in Finland and recommended in Singapore, position security flaws as violations of device integrity. However, in most jurisdictions the uptake of such requirements under cybersecurity labelling schemes remains voluntary, and there is scope therefore for introducing compulsory policy enactment.

Korea's approach (#12) is where producers are mandated to provide technical support for update failures during the warranty period, albeit only for higher-tier devices. In a more flexible approach, the policy in the Netherlands suggests that security updates should be proportional to device cost, and urges producers to devise an end-of-life policy that specifies minimum periods for updating support.

A similar approach is also reflected in the policies of the United States and the United Kingdom. Policymakers must focus on defining software update system security requirements, while also contemplating enforceable regulations on update response times and support duration for new vulnerabilities. The Canadian policy emphasises the importance of consumer awareness regarding security updates support, and suggests a potential role for consumer education.

Part 3: Conclusions Derived from the Research Findings

Drawing from the extensive analysis of policy documents and regulatory frameworks, this section encapsulates the key conclusions derived from IS3C's research.

1. Emphasis on Collaborative Efforts

The findings emphasise the pivotal role of collaboration in fortifying IoT security. Documents from key regions, notably the United States and the United Kingdom, champion the idea of involving multiple stakeholders. This accentuates the importance of clearly defining roles and responsibilities for all entities, from manufacturers to end-users.

2. Tailored Policy Documents

A significant number of policy documents are designed to address specific stakeholder groups, making their distribution and implementation more streamlined. The Korean policy document, in particular, offers a holistic approach, seamlessly connecting regulatory directives with hands-on applications for engineers and developers.

3. Resilience and Security by Design

There's a unified drive towards embedding security intrinsically in IoT devices. The focus is on engineering devices that are resilient to challenges like crashes, power shortages, and outages. The recurring themes in the documents are 'fault tolerance' and safeguarding against cyber threats, especially DDoS attacks.

4. User Empowerment and Vulnerability Management

A substantial part of the documents underscores the significance of vulnerability disclosure policies and the imperative for a structured approach to managing IoT security threats. The spotlight on education, transparency, and international collaboration amplifies user empowerment and bolsters overall IoT security.

5. Mechanisms for Compliance and Best Practices

To champion adherence to IoT security standards, regulators and policymakers leverage a combination of tools, including regulatory directives, incentive-driven programs, and labelling initiatives. However, the efficacy of these tools can differ based on regional and contextual nuances.

6. Warranty and Security Updates

One discernible trend is the association between device warranty durations and the commitment to security updates. While regions like the EU have advanced in this domain, there's an inconsistent global uptake.

7. Global Standardisation Imperative

While there's an abundance of best practices and guidelines available, a notable gap persists in aligning with universally accepted security standards, such as those proposed by the Internet Engineering Task Force (IETF). This underscores the urgency for a unified approach in addressing IoT security on a global scale.

Part 4: IS3C's specific policy recommendations on IoT security

The following policy recommendations drawn from the IS3C research project focus in particular on i. accountability; ii. unauthenticated vulnerability; iii. coordinated vulnerability disclosure; iv. open standards; v. integration of security updates and warranty policies. The IS3C coalition believes that their implementation provides a roadmap for strengthening the security and safety of the Internet of Things environment.

i. Accountability

Q1

As highlighted in the first question there is a need to clearly define who is responsible for cybersecurity and safety in the IoT realm. This is crucial for a strong defence against potential threats. When the roles of developers, manufacturers, service providers, and users are defined, a framework of accountability is created in which everyone knows what they are responsible for, which promotes teamwork and cooperation, leading to security. This clarity extends from designing IoT devices to their everyday use, creating a strong foundation that protects both the technology and the people who use it.

The protocol schemes, code snippets, and device illustrations cited in the Korean policy document that was analysed by the research team (#12 in the list at Annex 1) sets out a valuable and pragmatic approach that directly caters to developers who are an essential stakeholder in IoT security because of their pivotal role in shaping the security landscape of IoT devices. In this context, the need to bridge the gap between regulatory language and developer comprehension is paramount.

Developers possess the technical expertise to introduce detailed security measures but translating regulatory jargon into actionable steps can be challenging. When regulatory documents present practical examples such as protocol schemes, code snippets, and device illustrations, developers can seamlessly integrate security measures into their work. This approach not only empowers developers but also fosters a collaborative environment where their expertise is harnessed to create resilient IoT ecosystems.

Furthermore, the inclusion of developer-friendly content in regulatory documents serves as a testament to the inclusive nature of IoT security efforts. Developers are not merely implementers but also contributors to the larger discourse on security enhancement. Their insights, innovations, and cooperation are instrumental in driving effective security practices across the IoT landscape.

In essence, moving regulatory language closer to developers is not just a pragmatic move; it is a strategic recognition of their significance as stakeholders in securing IoT. This approach not only facilitates compliance but also amplifies the collective efforts towards strengthening the IoT ecosystem, ultimately benefiting manufacturers, service providers, users, and society at large.

ii. Unauthenticated vulnerabilities

Q2

A critical facet of IoT security is identifying vulnerabilities that necessitate precise and targeted countermeasures. Denial-of-Service (DDoS) attacks and brute-force attacks, both emblematic of the subtle yet potent threats in the digital landscape, warrant special attention due to their inherent nature. Unlike many other cyber threats, these attacks do not rely on authentication for exploitation, making them particularly insidious.

DDoS attacks, with their intent to overwhelm and incapacitate systems by flooding them with a deluge of traffic, exploit the very architecture that enables seamless connectivity. These attacks, often orchestrated from a multitude of compromised devices, can bring down entire networks, disrupt services, and wreak havoc on digital infrastructure. Their non-discriminatory nature renders authentication irrelevant; instead, they target vulnerabilities within the infrastructure itself.

On the other hand, brute-force attacks adopt a more direct approach. By systematically attempting all possible combinations of credentials, these attacks bypass authentication barriers and exploit weak points in an IoT ecosystem. Their relentless pursuit of access, irrespective of authentication, highlights the urgency of bolstering defences against them.

Addressing these threats requires a focused regulatory strategy aimed at embedding countermeasures for brute-force and DDoS attacks directly into IoT devices. Given the constraints of these devices in handling intricate security systems, a targeted approach is essential.

Regulatory frameworks should orient tailored defence mechanisms within the capabilities of IoT devices. This could involve deploying traffic analysis to detect anomalies against DDoS attacks or enforcing robust authentication protocols to counter brute-force attempts. By concentrating regulatory efforts on incorporating specific protections against these threats within the devices themselves, we recognize the unique challenges they pose. This approach ensures that even the simplest IoT devices stand resilient against unauthenticated attacks, cementing the bedrock of IoT security.

iii. Coordinated vulnerability disclosure (CVD*)*

Q3

The research highlighted the importance of a Coordinated Vulnerability Disclosure (CVD) strategy. Embedded within the heart of CVD is a philosophy of cooperation, uniting researchers, manufacturers, service providers, and users in a collective security endeavour. A CVD strategy provides a framework that connects security researchers, who conscientiously report their findings to manufacturers and relevant stakeholders. It creates a cooperative interplay of verification, collaboration, and communication between all stakeholders related to the detection, fixing, and updating of vulnerable devices.

In the world of IoT where devices seamlessly integrate into daily life, a single vulnerability can ripple into far-reaching consequences. CVD serves as the conductor of collective defence, orchestrating the harmonious convergence of stakeholder strengths. This symphony of collaboration forms a shield against potential exploits, enhancing the resilience of the ecosystem and fortifying users against harm.

Policymakers are urged to endorse CVD strategies through regulatory frameworks. Policymakers can advocate standardised guidelines that create a culture of responsibility, transparency, and collaboration. By incentivising manufacturers to adopt CVD programmes, rewarding proactive vulnerability detection and rapid remediation, policymakers can increase IoT security in a safer digital landscape.

iv. Open standards

Q4

Open standards serve as the cornerstone of a secure and interconnected digital landscape, exemplifying a proactive approach towards strengthening the resilience and security of IoT devices. IS3C's research demonstrated that the deployment of open standards, such as those by organisations like the Internet Engineering Task Force (IETF), are important to enhance the security of IoT devices.

Open standards are rooted in principles of transparency, collaboration, and inclusivity. These standards ensure that devices and systems adhere to universally accepted frameworks, minimising the proliferation of proprietary solutions that can inadvertently introduce vulnerabilities. The collaborative nature of open standards encourages a diverse array of perspectives, fostering innovation and pre-emptively addressing potential security pitfalls.

The adoption of open standards underpins a crucial aspect of IoT security – interoperability. Devices built on standardised protocols can seamlessly communicate and function together, forming an intricate yet cohesive IoT-ecosystem. This interoperability not only enhances user experience but also bolsters security. Devices adhering to recognized open standards are inherently designed to follow established security practices, reducing the likelihood of weak links within the system.

One of the hallmark features of open standards is the rigorous peer review process they undergo. The industry-led standards development organisations such as the IETF, subject proposed protocols and architectures to comprehensive scrutiny by experts from various domains. This intensive review process acts as a crucible for identifying vulnerabilities, weaknesses, and potential risks. Such open critique ensures that protocols are stress-tested, refined, and designed to withstand potential security threats.

In the light of the crucial role played by open standards, policymakers are advised to consider leveraging forums like the IETF to facilitate widespread adoption of secure protocols and architectures. These platforms provide an avenue for governments, industry, and other stakeholders to engage in inclusive and informed discussions. Policymakers should actively participate within these fora, fostering an environment where secure standards are not only conceived but also recognised and widely deployed on a global scale.

By incorporating open standards into policy frameworks, governments can pave the way for safer IoT ecosystems. The adoption of well-vetted and globally accepted standards instil confidence in consumers and stakeholders alike, positioning the IoT landscape on a trajectory toward enhanced security, resilience, and interconnectivity. The spirit of collaboration championed by open standards serves as an indomitable force in safeguarding IoT devices.

v. Integration of security updates and warranty policies

Q5

In the realm of IoT device security, a compelling proposition emerges – the integration of security updates with warranty policies. This strategic union has the potential to reform the IoT landscape by ensuring that IoT devices retain their functionality and security over time.

Security updates stand as the cornerstone of IoT device defence, acting as the shield against potential vulnerabilities and emerging threats. By forging a direct connection between these updates and warranty policies, manufacturers establish a commitment not only to delivering innovative devices but also to sustaining their security throughout their operational lifespan.

The rationale underlying this recommendation lies in the recognition that an unpatched, insecure device can deviate from its intended purpose, rendering it ill-suited for its original use. Such devices not only expose users to potential risks but also compromise the efficacy of the technology they rely upon.

The synergy between security updates and warranty policies compels manufacturers to prioritise consistent and timely updates. This alignment ensures that devices remain secure against evolving threats, providing users with an ongoing assurance of reliability and security.

Policymakers are urged to champion this approach, advocating for the integration of security updates into warranty frameworks. By endorsing this linkage, policymakers reinforce the vital connection between security and utility, encouraging a proactive stance against potential security vulnerabilities.

In summary, the recommendation to connect security updates with warranty policies offers a pragmatic avenue for sustaining the security of IoT devices. Embracing this proposition empowers both manufacturers and policymakers to create a robust ecosystem where IoT devices not only meet but exceed users' expectations, functioning securely and seamlessly throughout their lifecycle.

Part 5: Recommended IoT Security Practices

Having made an extensive comparative analysis of legal documents concerning IoT security, the IS3C research team identified the following best practices under the four main categories identified in the research which the IS3C stakeholder coalition recommends are adopted more widely in line with the various responsibilities of all stakeholders in the IoT ecosystem. This includes not only government policy makers but also other crucial parties like manufacturers who are responsible for designing and updating secure devices, and consumers who play a role in practising secure usage and maintenance of their devices.

The list includes best practices that the IS3C researchers agreed to be essential and critical in establishing greater IoT security, or are considered to be innovative in promoting significant advances in IoT security. However, this is not intended to be an exclusive list but to serve as guidance for governments and industry when taking decisions to strengthen IoT security in a rapidly evolving area of digital technology.

i. Data Privacy and confidentiality

To protect sensitive data, including personal information, adequate encryption methods **should** be used for both the transmission and storage of data. The confidentiality of data transiting between devices and services **must** be protected using appropriate cryptography. Additionally, IoT devices **should** be restricted to a separate network, keeping them isolated from other devices such as personal or guest computers and phones.

ii. Secure updating

Manufacturers **should** build in and provide the ability to initiate software updates in devices, either automatically or by actively informing the end-user. The integrity of the firmware **must** also be validated, with secure boot and firmware signing as a measure against tampering. Updates **should only** be performed through authorised entities.

iii. User empowerment

Companies providing Internet-connected devices and services **should** have a mandatory vulnerability disclosure mechanism in place, with a public point of contact for security researchers and users to report problems such as unauthorised access. A recognised coordinated vulnerability disclosure policy **should** be in place.[6]

iv. Operational resilience

Users **should** have the ability to easily delete their personal data from the device. The system **should** recover automatically in case of crashes or power shortages, and the secure boot process **should** warn the user if it fails. IoT services **should** remain operational during outages and recover cleanly in case of power restoration.

Part 6: Synthesis and Final Observations

The importance of IoT security in procurement and policy implementation cannot be overstated, especially in a time where the Internet of Things is becoming a global common good. The IS3C stakeholder coalition recognises this and emphasises that a secure and robust IoT ecosystem can be achieved not by legislation alone, but through public and private demand and adherence to robust security standards.

IS3C's working group (IS3C WG1) focuses on IoT security by design and its research has identified significant gaps in national policies and regulations regarding IoT security standards and best practices, many of which lack explicit reference to rigorous compliance standards and detailed implementation guidance. To address these gaps, there is a pressing need to strengthen the incorporation of robust compliance standards and specific implementation guidance within policy frameworks. By doing so the effectiveness and practicality of IoT security practices, including the following, will create a more secure and safer IoT environment.

i. Privacy Protection

It is crucial to adopt best practices for secure data encryption, access control, minimization of exposed attack surfaces, authentication systems, regular security

[6] By coordinated we mean that the device vendor and software provider **should** provide software updates before releasing a description about the vulnerability. With this approach users can be protected before malicious actors start to take advantage of the vulnerability description. Users will also be able to secure their devices immediately after reading the news.

assessments, and compliance with data protection regulations. These practices provide the backbone for privacy protection in the IoT landscape.

ii. Secure Updating Practices

Updating software and firmware, restricting unauthorised installations, and implementing a security updates policy will strengthen the overall IoT infrastructure, with greater security and resilience. This involves measures such as data encryption, access control, and secure authentication protocols.

iii. User Empowerment

Empowering users is a proactive step towards a secure IoT ecosystem. Users should be encouraged to take active steps in securing their IoT devices. Initiatives can range from vulnerability disclosures and reports to educational programmes and consumer awareness initiatives.

iv. Operational Resilience

Operational sustainability practices, including the implementation of monitoring and response mechanisms (e.g. a responsible disclosure policy[7]) can effectively detect and address security breaches in a timely manner. Continuous and secure IoT network and device operation can be ensured through secure network configurations, logging of security incidents, disaster recovery plans, regular security incident monitoring, and securing product disposal or end-of-life strategies. By prioritising Operational Sustainability, organisations can establish a strong foundation for their long-term success while also strengthening their defences against security threats. Through the adoption of effective monitoring and response mechanisms, organisations can identify and swiftly respond to security vulnerabilities. This underscores the importance of integrating security considerations seamlessly in the architecture of IoT systems from their very inception.

IS3C's research points to significant potential for enhancing IoT security when these best practices are adopted by governments and private sector organisations. Demand for secure IoT services, products, and devices can create a ripple effect leading to a more secure and resilient IoT ecosystem. Importantly, such practices can close potential avenues for attacks and misuse.

Although reactive security measures are a common fallback in government and industry, IS3C strongly advocates a more proactive policy approach where preventive measures take precedence in the IoT landscape, thereby setting new standards for cybersecurity. IS3C’s mission accordingly includes providing policy advice, guidelines, and toolkits to assist stakeholders in advancing towards a more secure IoT ecosystem.

[7] The Dutch government announced a central reporting desk for ethical hackers to report vulnerabilities. https://www.ncsc.nl/actueel/nieuws/2023/oktober/3/overheid-intensiveert-samenwerking-op-waarschuwingen-voor-cyberdreigingen (Dutch, accessed 4 October 2023)

The research has highlighted the existence of beneficial guidelines but the level of adoption of these in regions varies considerably. For example, IoT security labelling schemes have to date not been widely implemented across the world. Lack of effective promotion and monitoring adoption of such schemes and practices can also be a significant cause of gaps in implementation that reduces their effectiveness. Cooperation with national and regional consumer protection and advocacy organisations is therefore recommended in support of such schemes.

Next Steps

The research findings provide a foundation for further initiatives to enhance IoT security. More cooperation between governments, industries, and other stakeholders is essential to drive global adoption of standardised IoT security measures. In particular, it is crucial to prioritise efforts to promote comprehensive adoption and implementation of cybersecurity standards through awareness raising, procurement best practice (e.g. by making them an integral part when procuring IoT products) and inclusion in educational and vocational training curricula.

The IS3C stakeholder coalition accordingly recommends the following specific next steps for concrete action to achieve a more secure and safer IoT environment.

i. Awareness campaigns

Launching awareness campaigns targeting both the public and private sectors is crucial. These campaigns should focus on the importance of IoT security, the potential risks associated with insecure IoT devices, and the benefits of adopting robust security standards. They should also highlight the role of procurement in enhancing IoT security, emphasising that secure IoT services and products should be a prerequisite, not an afterthought.

ii. *Training of government policymakers and regulators*

Policymakers play a pivotal role in shaping the IoT landscape. Therefore, it is essential to provide them with comprehensive training on IoT security. This training should cover the basics of IoT, the importance of security in this context, and the role of procurement in promoting secure IoT practices. Policymakers should also be educated about the potential risks associated with insecure IoT devices and the benefits of adopting robust security standards.

iii. *Strengthening IoT policy frameworks*

Policymakers should work towards strengthening policy frameworks to incorporate robust compliance standards and specific implementation guidance. This will enhance the effectiveness and practicality of IoT security practices, fostering safer and more secure online environments.

iv. *Promoting security standards*

Efforts should be prioritised to promote comprehensive cybersecurity standards. These standards should be made an integral part of procuring IoT products, demanding they are built in by design in order to qualify for a contract. Additionally, these best practices should be taught in educational and vocational training curricula.

v. *User empowerment*

Users should be encouraged to take an active role in securing their IoT devices. This can be achieved through initiatives such as vulnerability disclosures and reports, educational programs, and consumer awareness initiatives.

vi. *Enhancing operational resilience*

Secure network configurations, logging of security incidents, having disaster recovery plans, regular security incident monitoring, and securing product disposal or end-of-life strategies should be implemented to ensure continuous and secure IoT network and device operation.

vii. *Collaboration with consumer protection and advocacy organisations*

To promote the adoption of IoT security labelling schemes, it is recommended to work together with consumer protection and advocacy organisations. This collaboration can help in effective promotion and monitoring of the adoption of such schemes and practices.

viii. *Further research*

More research is needed to deepen our understanding of IoT security measures and develop strategies for better enforcement, to assess the adoption of these protocols and standards and to identify new challenges or opportunities that arise in the field of IoT security. This ongoing effort is crucial to create a more secure global IoT environment and to ensure that best practices are not merely recommendations, but officially recognized and, if needed, enforceable standards across jurisdictions.

ix. *Engagement with standardisation bodies*

Public and private stakeholders should engage with the standards development organisations such as the Internet Engineering Task Force (IETF) in order to understand the latest advances in IoT security protocols and incorporate them into their IoT security and safety strategies.

Finally, no matter how well intended these recommendations are, they come to naught when individuals in decision-taking positions choose to buy, most likely cheaper, insecure by design ICTs. The whole security chain, for their own and other organisations, falls apart because of these kinds of decisions. Motivating our leaders to buy secure by design is an important task for all involved in promoting ICT security. Observing the increasing attention for governments, we believe that much can be learned from global good practice, and we are confident that the first steps we observed today will be followed by better informed interaction, taking into account that IoT is truly deployed globally - and it can help build a world we want.

Acknowledgements

The authors express their gratitude to Yuri Kargapolov for his invaluable contribution in launching this project. Yuri set the overall direction as the first Chair of Working Group 1 on security by design and initiated the outreach for members of the research team on IoT before the war in his home country Ukraine obliged him to step down. Our thoughts are with him and his family, friends and colleagues, and the IS3C coalition hopes to be able to welcome him back as an active member as soon as possible.

The research desk work and analysis was undertaken by João Moreno Falcão, Oscar Giudice, Sávyo Vinicius de Morais, and Victor de Pan whose commitment to the project was much appreciated as is also the editorial work for this report by Mark Carvell and Wout De Natris. Lastly, our sincere gratitude extends to Maarten Botterman, whose invaluable insights and expertise greatly enriched the final stage of our report.

The research project on IoT was sponsored by Microsoft. Without it IS3C would not have been able to conduct this research project. Special thanks go to Rob Spiger and Elizabeth Eigner for their active support.

Annex 1. Source Documents for the Research

Doc	Name	Issuer	Country or Union	Region	Researcher Assigned	Language
BR #01	Cybersecurity Requirements for Telecommunications Equipment	Brazilian Telecommunications Regulatory Agency - ANATEL	Brazil	GRULAC	Oscar Giudice	Portuguese
US #02	Senate Bill No. 327: Security of Connected Devices	State of California	United States	North-American Group	João Moreno Falcão	English
CA #03	Internet of Things (IoT) Security - ITSAP.00.012	Government of Canada	Canada	North-American Group	Oscar Giudice	English
IN #04	Code of Practice for Securing Consumer Internet of Things (IoT)	Telecommunication Engineering Center	India	Asia-Pacific Group	João Moreno Falcão	English
SG #05	Cybersecurity Labelling Scheme (CLS)	Singapore Cyber Security Agency	Singapore	Asia-Pacific Group	João Moreno Falcão	English
FI #06	Cybersecurity Labelling Finland	Traficom	Finland	WEOG	Oscar Giudice	English
US #07	NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline	National Institute of Standards and Technology (NIST)	United States	North-American Group	Oscar Giudice	English
US #08	Strategic Principles for Securing the Internet of Things	U.S. Department of Homeland Security	United States	North-American Group	Oscar Giudice	English
US #09	NISTIR 8259B - IoT Non-Technical Supporting Capability Core Baseline	National Institute of Standards and Technology (NIST)	United States	North-American Group	Oscar Giudice	English

CA #10	Internet of Things (IoT) Checklist for Consumers	Government of Canada	Canada	North-American Group	Oscar Giudice	English
JP #11	IoT Security Safety Framework	Ministry of Economy, Trade and Industry (METI)	Japan	Asia-Pacific Group	João Moreno Falcão	English
KR #12	Information Security Certification Criteria for Information and Communication Network Connection Devices (2021.9)	Korea Internet & Security Agency (KISA)	Republic of Korea	Asia-Pacific Group	João Moreno Falcão	Korean
US #13	NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers	National Institute of Standards and Technology (NIST)	United States	North-American Group	Oscar Giudice	English
SA #14	Internet of Things Regulatory Framework	Communication and Information Technology Commission	Saudi Arabia	Asia-Pacific Group	João Moreno Falcão	English
AE #15	Internet of Things Regulatory Policy	Telecommunications Regulatory Authority	United Arab Emirates	Asia-Pacific Group	João Moreno Falcão	English
VN #16	List of Baseline Cyber Security Requirements for Consumer IoT	Authority of Information Security (AIS)	Vietnam	Asia-Pacific Group	João Moreno Falcão	Vietnamese
US #17	NIST 8259 Series	National Institute of Standards and Technology (NIST)	United States	North-American Group	Oscar Giudice	English
US #18	Recommended Criteria for Cybersecurity Labelling of Consumer Internet of Things (IoT) Products	National Institute of Standards and Technology (NIST)	United States	North-American Group	Sávyo Morais	English
EG #19	IoT Framework in the Arab Republic of Egypt	National Telecom Regulatory Authority	Egypt	African Group	Sávyo Morais	English
UY #20	Document of proposals on IoT security in Uruguay, result of a multi stakeholder	Agencia de Gobierno Electrónico y Sociedad de la	Uruguay	GRULAC	Sávyo Morais	Spanish

	consultation process	Información y del Conocimiento				
AR #21	Public consultation on the Internet of Things	Ministerio de Modernización	Argentina	GRULAC	Sávyo Morais	Spanish
EU #22	Guidelines for Securing the Internet of Things	European Union Agency for Cybersecurity (ENISA)	European Union	Intergovernmental Organization	Sávyo Morais	English
EU #23	EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements	European Telecommunications Standards Institute (ETSI)	European Union	Intergovernmental Organization	Sávyo Morais	English
KE #24	Guidelines on the use of Internet of Things (IoT) Devices	Communications Authority of Kenya	Kenya	African Group	Sávyo Morais	English
NL #25	Roadmap IoT	Min Economic Affairs/The Netherlands	The Netherlands	WEOG	Victor de Pan	Dutch
NL #26	Roadmap IoT 2020 follow up	Min of Economic Affairs and Climate/The Netherlands	The Netherlands	WEOG	Victor de Pan	Dutch
NL #27	Essential requirements for securing IoT consumer devices	Agentschap Telecom	The Netherlands	WEOG	Victor de Pan	English
NL #28	Proposed legislation on IoT security firmware/software updates	Dutch Parliament	The Netherlands	WEOG	Victor de Pan	Dutch
NL #29	CSA certification	Agentschap Telecom	The Netherlands	WEOG	Victor de Pan	Dutch
UK #30	Code of Practice for Consumer IoT Security	Department for Digital, Culture, Media & Sport	United Kingdom	WEOG	João Moreno Falcão	English

Annex 2. Summary of the good practices found in the documents

Category	Name of Best Practice	Description	Found in Documents
Data privacy and Confidentiality	Ensure that personal data is secure (Focus on strong encryption)	Enable the use of adequate encryption methods for the transmission of sensitive data, including personal information. b) Enable the use of adequate encryption methods for the storage of sensitive data, including personal information. c) The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography appropriate to the properties of the technology and usage. d) Including Restrictions of personal IoT devices to a separate bring-your-own-device (BYOD) network (e.g. guest Wi-Fi)	#1, #2, #3, #4, #5, #6, #7, #8, #10, #11, #12, #15, #20, #23, #25, #27, #30
Secure Updating	Mandatory Software Updates	Manufacturers should be able to initiate software updates in devices. Either through automatic updates or by actively informing the end user.	#1, #3, #4, #5, #6, #7, #8, #10, #11, #12, #13, #16, #18, #20, #22, #23, #26, #27, #28, #30

Category	Name of Best Practice	Description	Found in Documents
User empowerment	Have a Mandatory Vulnerability Disclosure Mechanism	1. Implement a vulnerability disclosure policy. All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner. 2. Have in place Coordinated Vulnerability Disclosure processes based on internationally recognized best practices and recommendations. 3. Develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities	#1, #2, #5, #6, #7, #8, #11, #18, #22, #23, #25, #30
Operational resilience	Personal Data Deletion	Allow the user to delete their personal data from the device in the easy and best authenticated way.	#1, #4, #5, #12, #16, #23, #30
Data privacy and Confidentiality	No Universal default passwords + Strong User-defined Password + 2FA	Use a Two-factor authentication mechanism if possible or Passphrase instead of Passwords. In the case of passphrase, passwords and keys it is mandatory for the user to generate those. No default or factory secrets are allowed anymore.	#1, #3, #4, #5, #6, #8, #13, #16, #18, #20, #22, #23, #25, #30
Secure Updating	Integrity Validation of firmware Image	1)Secure boot and firmware signing are security measures that provide a degree of protection against tampering. These integrity measures must be used during device manufacturing and during maintenance. These cryptographic operations must be done in conjunction with tamper resistant hardware in the framework of the chain of trust. These two measures can be integrated into existing Service-Level Agreements with third-party suppliers. 2) Perform software/firmware integrity verification during system startup, being able to alert the user in cases of compromised integrity.	#1, #3, #5, #6, #7, #8, #13, #18, #20, #22, #23, #25, #26, #27, #28, #30

Category	Name of Best Practice	Description	Found in Documents
User empowerment	Cooperation for having Common Labelling Scheme	Specify all certifications as requirements the product fulfils. When applying for a Cybersecurity Label, a company must fill in a statement of compliance form that contains information on the features of the product or service. An independent third party then undertakes an information security inspection on the product or service that the application concerns. The results are compared against the Cybersecurity Label requirements. Once the information and features provided are deemed sufficient, the Certification Authority can grant the Cybersecurity Label.	#4, #5, #6, #9, #10, #18, #23
Operational resilience	Failure Boot Recovery & Outage Resilience	1. If the system crashes by unexpected external factors such as power shortages or communication failure, the device must be able to recover automatically. 2. If the secure boot process fails, the system must warn the user and execute countermeasures, such as restart of the failed component or disabling network connection. 3. Resilience should be built into consumer IoT devices and services, taking into account the possibility of outages of data networks and power (also on recovering). 4. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.	#1, #4, #5, #8, #12, #16, #22, #23, #30
Data privacy and Confidentiality	Validate input data	Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.	#5, #6, #15, #16, #23, #30

Category	Name of Best Practice	Description	Found in Documents
Secure Updating	Update via authorised entities only	1) The IoT device's software can be updated by authorised entities only using a secure and configurable mechanism. 2) Only authorised code must run in the device. This means that the user cannot install software without the vendor acceptance. This protection is meant to prevent malware from being installed through password cracking or any kind of non-authorized access. 3) Owners and operators of the devices and systems are involved or the ownership rights and/or management rights of the devices and systems remain on the supplier side, etc in order to seek reliable implementation.	#7, #11, #18
Operational resilience	Provide End-of Life and Support Channels to the End User	1. If the update fails during warranty period support must be provided. 2 Have a clear signal on How long the manufacturer intends to support the device. To have a clear process for end-of-life. How can customers report suspected problems with cybersecurity implications, such as software vulnerabilities, to the manufacturer and to have clear How can customers maintain securability even after official support for the device has ended (e.g., when a manufacturer or third-party organisation with a role in cybersecurity shuts down entirely or ends support of the device). 3. The IoT product developer broadcasts and distributes information relevant to cybersecurity. To alert the public and customers of the IoT product about cybersecurity relevant information and events throughout the support lifecycle, and to alert appropriate ecosystem entities about cybersecurity relevant information.	#1, #11, #13, #18

Category	Name of Best Practice	Description	Found in Documents
Data privacy and Confidentiality	Minimise Exposed Attack Surfaces and Network (Hardening)	1. The device should only provide ports and links necessary for normal and intended functionality. 2. All devices and services should operate on the ‘principle of least privilege’; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. 3. Software should run with appropriate privileges, taking account of both security and functionality. 4. All unused network and logical interfaces shall be disabled. In the initialised state, the network interfaces of the device shall minimise the unauthenticated disclosure of security-relevant information.	#5, #6, #12, #16, #23, #30
User empowerment	Transparency and Global cooperation	1. Stakeholders, especially suppliers, should be transparent, offering clear and detailed information about the operations and normal behaviour of the supplied products; and communicating all the relevant information to the next step of the chain. 2. Conduct end-to-end risk assessments that account for both internal and third party vendor risks, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded. 4. Global cooperation, given that digitalization and network security involve and might affect everyone. It is essential to develop global standards that facilitate technical interoperability and regulatory coherence, providing clear rules, predictability and transparency.	#8, #20 ,#22, #23

Category	Name of Best Practice	Description	Found in Documents
Secure Updating	No Update Transparency	1. For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user. 2. Legacy IoT devices based on unmaintained software are a threat to the integrity of the supply chain. Extended support and a timely delivery of security patches should be factored into the design and planning of an IoT product—this includes proper dimensioning of resources (e.g. memory) to support future updates.	#22 and #23
Data privacy and Confidentiality	Network Security	1. Consider security measures on the network side. 2. Control Network Traffic (Unauthorised network traffic must be blocked) 3. Restricting personal IoT devices to a separate bring-your-own-device (BYOD) network (e.g. guest Wi-Fi) 4. Isolating IoT networks to restrict access with systems managing sensitive data.	#11, #12, #3.
User empowerment	Education and Awareness Campaign	1. The ability for the manufacturer and/or supporting entity to create awareness of and educate customers and others in the IoT device ecosystem about cybersecurity related information, considerations, features, etc. of the IoT device. 2. Development of capabilities and specific awareness-building on the topic. Understanding the importance of addressing certain aspects in order to be able to evaluate the security in their IoT systems and/or devices. 3. The manufacturers need to [develop the] Ability to identify and understand current or potential risks. 4. manufacturers should be required to include a comprehensive user guide or manual, which provides instructions on the safe and secure use of its products.	#9, #18, #20, #22

Category	Name of Best Practice	Description	Found in Documents
Operation resilience and user empowerment	System telemetry data and considerations on the processing of personal data	1. If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies. 2. If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality. 3. If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.	#4, #5, #16, #23, #30
Operational resilience	Guidance on Security Checks	1. The manufacturer should provide users with guidance on how to securely set up their device. 2. The manufacturer should provide users with guidance on how to check whether their device is securely set up. 3. Make installation and maintenance of devices easy. Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device. 4. Specify where the security guidance is available in the local language.	#5, #6, #8, #23, #26, #28, #30

Category	Name of Best Practice	Description	Found in Documents
Operational resilience	Device Unique Identification	1. The IoT device can be uniquely identified logically and physically. 2. The IoT product is uniquely identifiable and inventories all of the IoT product’s components. The IoT product can be uniquely identified by the customer and other authorised entities. The IoT product uniquely identifies each IoT product component and maintains an up-to-date inventory of connected product components. 3. The ability to uniquely identify every IoT device is crucial and has deep repercussions related to visibility and accountability in the supply chain. Identity management systems should be integrated into the supply chain to provide these unique identifiers. 4. Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software. 5. Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.	#5, #7, #18, #22, #23
User empowerment	Incident Audit	1. Allow security events to be stored in external repositories and avoid the loss of events. 2. Not all stakeholders have the resources to perform security audits or analysis, so the majority perform trust assumptions at some point. It is desirable to minimise these assumptions when feasible, while maintaining privacy assurances for the end user. 3. Perform audits and monitor security events. Share knowledge and promote communication of the findings. 4. Act in a timely manner and in coordination, as this helps to reduce vulnerabilities.	#1, #20, #22