DIGITALEUROPE

24 OCTOBER 2019

Defining the way forward for IoT security and certification schemes

Executive Summary

This document aims to provide guidance on how to address cybersecurity of the Internet of Things (IoT) in the context of the adoption of future cybersecurity schemes under the Cybersecurity Act[1] and other relevant European legislation. Our goal is to advance more effective cyber risk management across the European Digital Single Market.

We specifically recommend EU decision makers and ENISA:

- Promote competitiveness by ensuring IoT security requirements are uniform across and beyond the European Digital Single Market;
- Define any cybersecurity requirements on the basis of international standards;
- Avoid inconsistencies and overlaps between EU regulations – legal consistency must be a key goal of any European Commission initiative dealing with IoT security;
- Beyond a common baseline, adopt a differentiated approach to IoT domains; and
- Consider cybersecurity of the entire life cycle, beyond the device itself.

1 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Setting the scene

The definition of the Internet of Things

There is no common or widely recognised IoT definition in Europe or globally. Existing definitions can vary substantially as to scope and elements that can be included and risk being too broad for the purpose of targeting new technical and process requirements.[2]

In light of this, DIGITALEUROPE believes that a workable scope for an IoT definition should refer to **specific-purpose devices and their associated services that are connectable to network infrastructure, such as the Internet**.[3] Broader definitions could sweep in a wide array of very different products, potentially undercutting the coherence and security benefits of an IoT certification scheme.

Distinguishing between IoT domains

Albeit all IoT products hold the same common ground, we should recognise the different sector-specific application contexts – from consumer/home appliances to industry and automation, automotive, energy, etc. In fact, each sector presents specific and different features, environment of use and risks that would need to be taken into consideration when developing a certification scheme.

At the very least, the differentiation should follow a sectorial risk-based approach**.** In fact, among the various domains there are substantial differences in terms of management environment and risk levels.

DIGITALEUROPE believes that considering different IoT domains would help in building better targeted cybersecurity certification schemes and associated standards.

---

2 See for example the definition contained in ENISA's Baseline Security Recommendations for IoT, available at https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

3 Associated services are defined as 'digital services that are linked to IoT devices, for example mobile applications, cloud computing/storage and third-party Application Programming Interfaces (APIs) to services such as messaging.' ETSI TC Cyber: Technical Specification 'Cyber Security for Consumer Internet of Things,' available at https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

Legislative and standardisation landscape

Legislation

In recent years there have been several initiatives worldwide covering cybersecurity or network information security in general as well as IoT security specifically. This situation poses a risk of a non-aligned and fragmented legislative framework.

In the EU, this includes the following initiatives:

- The Directive on security of network and information systems (NIS Directive), established in 2016, is the first pan-European cybersecurity legislation. This Directive, which focuses on national cybersecurity capabilities, could indirectly cover IoT used in critical infrastructure.
- In the context of the recently adopted European Cybersecurity Act, ENISA is considering the possibility of developing, amongst other schemes, a cybersecurity scheme specifically for the IoT.
- The New Legislative Framework (NLF) sets mandatory product safety requirements that are necessary to put products on the EU market (CE marking). Now that products tend to be connected, the European Commission is looking at how to include cybersecurity requirements in NLF directives and regulations. The first under consideration is the Radio Equipment Directive (RED), which could include cybersecurity requirements through a delegated act on Internet-connected and wearable radio equipment. In addition, the Machinery Directive or the Low Voltage Directive are also considered in this regard.
- Finally, Member States are also adopting their own national legislation on IoT security:
    - Following the adoption of its code of practice on IoT in 2018,[4] the UK is in the process of adopting mandatory requirements for business-to-consumer (B2C) IoT and has launched a consultation on the topic.
    - Germany is also looking at its own IoT security label.

[4] Code of Practice for Consumer IoT Security, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

This legislative landscape exposes industry to a set of patchy and non-aligned laws, which create inconsistent and overlapping requirements and technical standards.

Standards

Standards are the most effective tool to introduce technical provisions without overly prescriptive requirements that might become outdated as technology evolves. In the area of cybersecurity certification, the role of global standards is key and should be used as a reference for any certification schemes.

A number of cybersecurity standards already exist for specific domains, such as IEC 62443 for industrial applications and ISO 21434 currently under development for the automotive sector. The ISO/IEC 27000 series, which is not linked to a sector, is also relevant for the IoT. Recently, ETSI adopted the first technical specification on Security for Consumer IoT: TS 103 645, which is currently transformed into a European standard under EN303645.[5]

The IEC 62443-4-1 standard describing secure development lifecycle requirements is generic and relevant for the IoT – be it consumer, industrial or other IoT domains – as a common baseline. The standard describes a secure process including security requirement definition, secure design, secure implementation with hardening and coding guidelines, verification and validation procedure, defect management, patch management and product end of life.

In the US, NIST is currently consulting on a Core IoT Cybersecurity Baseline, building on NISTIR 8228, which advises federal agencies on managing IoT devices from a security and privacy perspective.[6]

The work of standardisation bodies (ETSI, IEC/ISO, CEN-CENELEC) is essential for any future cyber requirements by law or certifications scheme under the Cybersecurity Act. We call on ENISA, the Commission and other European decision makers to first assess existing and upcoming standards in order to map the most relevant ones and use them as the basis to define any requirements for IoT cybersecurity. We also call on CEN-CENELEC and ETSI to cooperate on developing European standards and to align activities with those happening in ISO and IEC, especially in JTC1 SC27.

---

[5] ETSI TC Cyber: Technical Specification 'Cyber Security for Consumer Internet of Things.'

[6] NIST Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers, available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf

Our five principles for IoT security

A global and European approach to avoid fragmentation

- One of the main objectives of the Cybersecurity Act is to address the fragmentation of the European cybersecurity certification landscape. As some Member States are moving forward with their own legislation, national approaches to the IoT threaten to undermine the competitive advantage of a European Digital Single Market without yielding meaningful security benefits. In fact, imposing IoT security requirements at the national level will impede the ability of companies operating across the EU to manage risk in a cohesive manner.
- Any **European measure to address IoT cybersecurity,** including any voluntary or mandatory label, regulation or certification, **should aim to avoid multiple and diverging requirements across the EU.**
- At the same time, as cybersecurity and technology know no borders, **the EU should proactively engage for global alignment of IoT cybersecurity.**

Cybersecurity requirements based on international standards

- Risk-based, testable, interoperable and globally aligned standards **are and must remain the basis of any security requirements for IoT or future cybersecurity certification scheme**.

  We encourage regulators to first allow the development of appropriate standards and criteria for IoT security before enforcing or making applicable legislative measures.

  When possible, cybersecurity requirements should be testable – the cost of verification can otherwise stifle market selection and innovation, hurting small and medium businesses in particular. Without clear and practicable testing specifications, cybersecurity requirements will become ambitious objectives but bear no particular effect on the IoT's level of security.
- One technical specification dealing with consumer IoT has been published by ETSI, and similar ones are being developed by other bodies. Given this, there should be no temptation to draft specific security

requirements that would deviate from or add to the existing ones. **ENISA should always refer to standards for cybersecurity requirements**; if not existing, such standards should be developed in parallel to a scheme using an open transparent process.

- **International and global standards must be the preference** for European certification schemes, cybersecurity or cyber hygiene being a global and not a purely European issue. Similarly, for domain-specific applications, existing IEC/ISO/ETSI standards should be used for any certification schemes wherever possible.
- In view of quickly changing cybersecurity threat scenarios, standardisation of processes or management systems has increasing relevance compared to requirements of mere product properties. Relying on a secure development lifecycle process is key to reducing risk, improving trust by making products inherently more secure and better protecting both products and sensitive information. International standards (such as ISO or IEC) are defining these secure practices.

A coherent framework for IoT cybersecurity

- As mentioned, some aspects of cybersecurity have been considered under individual product regulations under the NLF, while the Cybersecurity Act has entered into force and new schemes will soon be developed by ENISA. In such a situation, we see a clear **risk of overlaps and inconsistencies among European legislation.**

  This would produce legal uncertainty, with significant impact in case of concurrent mandatory requirements and certification schemes. This would threaten European companies' ability to compete across the Digital Single Market as well as globally, forcing them to misallocate scarce resources.
- **Legal consistency must be a key goal of any new European Commission initiative** dealing with IoT security. This requires careful analysis of the objectives of the existing frameworks before any new or revised instruments are put forward.
- Certification schemes developed under the Cybersecurity Act should stay voluntary and be sufficient to address the current policy goals on IoT security.
- Were cybersecurity requirements nevertheless to be introduced under the NLF, they should only address **minimum essential requirements**

(mostly safety-related[7]) common to vertical directives and aligned with international cybersecurity standards that should be available before the entry into force of the legislation.

Having the same essential requirements would mitigate the risk of different if not contradicting measures for products that fall under more than one directive.

- As regards the RED, it is essential to avoid addressing cybersecurity requirements in a delegated act. A delegated act would be limited by its own structure to cover only a subset of provisions.[8] Consequently, it would not be possible to ensure the necessary consistency with other existing or upcoming legislative requirements.

Differentiated approach to IoT security per domain

- A sectorial distinction should be made in the **cybersecurity requirements**. The recently adopted ETSI technical specification has recognised this need for a differentiated approach, with a technical specification dedicated to consumer IoT.
- Common cybersecurity requirements that are aligned with international standards could fit sector-specific IoT. However, beyond **a common baseline**, **a segmentation between consumer IoT and other IoT sectors or domains is required**.
- Cybersecurity requirements should **always be based on a risk-based approach and according to the intended use.** The higher the risk, the more stringent the requirements.

Moving beyond security of devices

- Cybersecurity should also take into account life cycle of the device, not just product requirements – a balance needs to be sought between process, system and product security.

---

7 NLF legislation aims to ensure product safety, health, environment and consumer protection.

8 A delegated act under the RED allows requirements only under Art. 3(3). Essentially, this means that cybersecurity requirements would have to stay within the limits of personal data protection and privacy (Art 3(3)(e)) and/or fraud (Art 3(3)(f)).

- **A secure development lifecycle (SDL) process** has the purpose of developing and maintaining secure products to make them more resilient:
  - SDL allows a comprehensive approach from a product's development throughout its lifecycle with incident and vulnerability management.
  - Well-recognised international and European standards on SDL already exist, e.g. for secure development lifecycle IEC 62443 4-1 and/or ISO/IEC 27034 or vulnerability disclosure and handling (ISO/IEC 29147 and 30111).
  - By introducing standardised security and compliance considerations throughout all phases of the development process, developers can help reduce the likelihood of vulnerabilities in products and services and avoid repeating the same security mistakes. Security updates should also be considered in a holistic approach.
  - In addition, the manufacturer can add specific technical cybersecurity requirements based on existing standards.
- It is also crucial to look at the security of the system itself, where security of the product is only part of the security journey. By considering the system view, it is possible to go beyond device design by managing compensating controls (secure process at the commission phase, complementary secure tool and services, etc.). The role of the network is also crucial here – devices, networks and systems need to work in tandem:
  - Specifically, there are things that manufacturers can develop into the device or achieve through services or processes, which enable the network to more effectively handle security at scale.
  - The network has the added advantage of being well-placed to secure IoT devices with no or limited embedded security capabilities as a result of design limitations, such as processing capabilities or battery life, or due to manufacturers' inexperience or unwillingness to do so, often due to cost considerations. This includes the vast number of legacy devices that are already on the market.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK