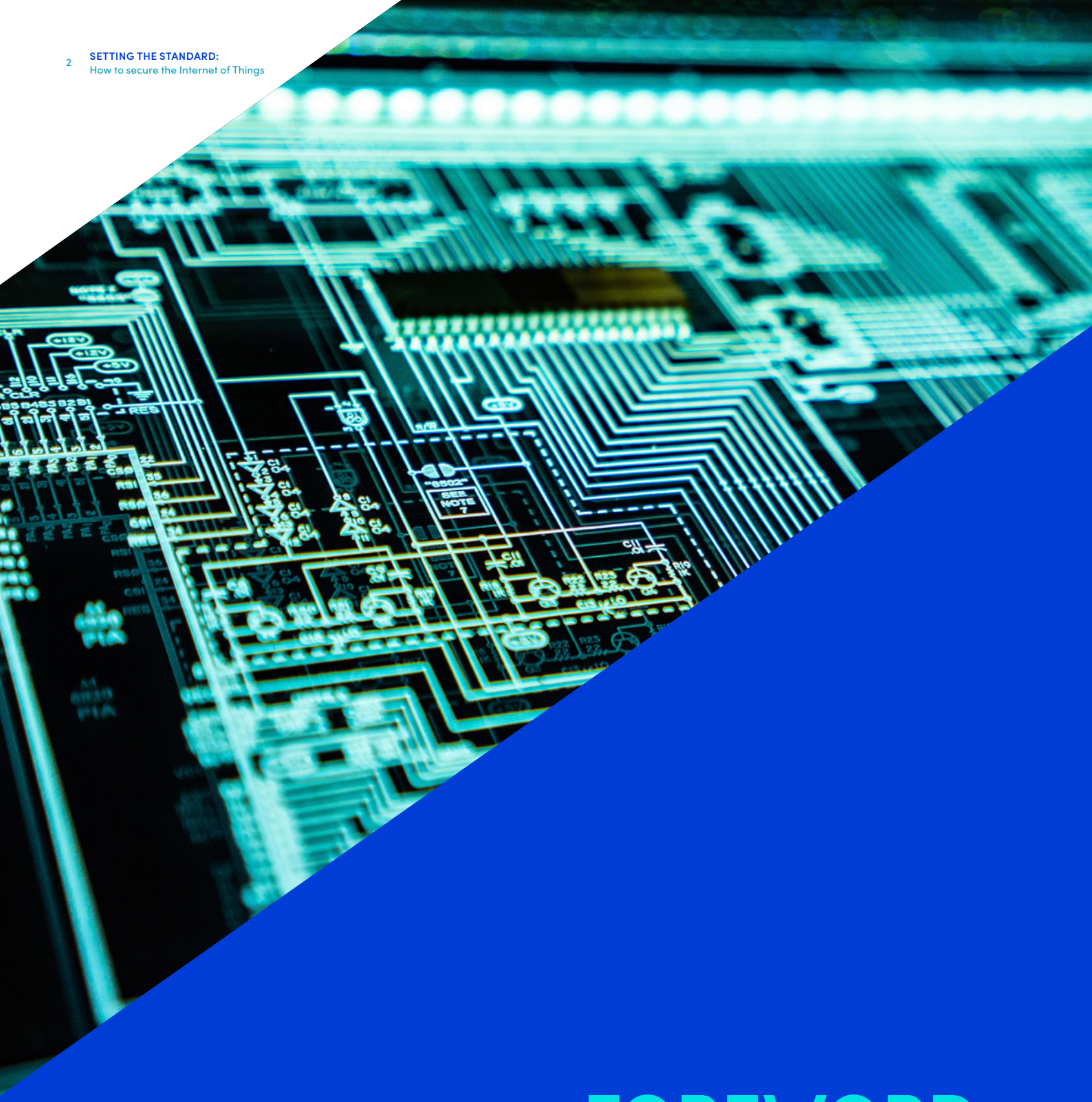
SETTING THE STANDARD

How to secure the Internet of Things

DIGITALEUROPE



FOREWORD

There were 12.4 billion IoT devices estimated to be connected around the world in 2020, a number expected to more than double to 26.4 billion by 2026 alone.[1] This rapid growth generates cybersecurity risks, with potential vulnerabilities that hackers could exploit.

Ensuring the cybersecurity of connected products, and thereby enhancing our digital resilience, has therefore become a top priority for Europe. This is reflected in the Commission's landmark Digital Decade goals, the COVID recovery funds and the new EU budget.

Our approach to product legislation must now evolve to encompass safety of connected devices. This is not an easy task: cybersecurity is a relatively new development, compared with decades' worth of product rules.

Given the speed of technological advancements, setting the wrong framework now could bring unintended consequences in the design and development of connected products years from now.

So far, Europe's product legislation has been particularly successful in its reliance on 'harmonised standards,' that is, those developed by European standards organisations specifically to demonstrate compliance with legal requirements.

Harmonised standards provide reassurance – to manufacturers, authorities and consumers alike – that a product complies with the law, avoiding a lengthy and expensive assessment.

In this study we have asked prominent standardisation experts how cybersecurity requirements can best be integrated into the EU's product rules, and how these can best be supported by harmonised standards:

- **70 per cent** of baseline cybersecurity requirements are common across all connected products. **New, horizontal legislation is therefore most appropriate to tackle this.**
- **94 per cent** of interviewed experts find that sufficient cybersecurity cannot focus solely or primarily on product features, such as passwords. For this reason, **existing product legislation should not be used to address cybersecurity. Or if we must, it should be tightly focused on product-related requirements.**
- It will take **five years** to develop and apply the necessary harmonised standards. **Let us take our time and do this right.**[2]

We hope that this report can contribute to a constructive debate to reach the right decisions for the future of Europe's laws and standards for cybersecurity.

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

[1] *Ericsson Mobility Report*, June 2021
[2] For further recommendations on removing bottlenecks for harmonised standards, see *Joint industry recommendations for effective harmonised standardisation*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/07/DIGITALEUROPE_Joint-Industry-Recommendations-for-effective-Harmonised-Standardisation.pdf

Introduction

This study, based on interviews with 18 standards experts, provides recommendations for how EU product legislation and harmonised standards should work together to ensure the cybersecurity of connected products.

A number of EU initiatives are underway or being explored. Importantly, the EU is looking to leverage its successful legal framework for the placement on the market of products – familiar to most for the CE mark – to also include cybersecurity requirements. Currently, this includes:

- An imminent delegated act under the Radio Equipment Directive (RED), which would activate requirements relating to the protection of data and network resources, and against fraud;[3]
- A proposed Regulation on machinery products, replacing the current Machinery Directive, which would create requirements for protection against corruption;[4]
- A proposed General Product Safety Regulation, replacing the current Directive, whose scope would be extended to cybersecurity risks that have an impact on safety;[5] and
- A future proposal for horizontal cybersecurity rules for all connected products and associated services.[6]

A key feature of the EU legislative framework for the placement on the market of products is its reliance on 'harmonised standards,' providing a presumption of conformity with the legal requirements for manufacturers implementing such standards in their products. It is therefore important to ensure that legal requirements and harmonised standards are developed effectively and coherently.

What are harmonised standards?

A harmonised standard is a standard developed by a recognised European standardisation organisation (CEN, CENELEC or ETSI) following a request from the European Commission. Such request provides the conditions that the standard must respect to meet the legal requirements or other provisions set out in relevant EU product legislation. Subject to verification by the Commission that these conditions have been met, a reference to the standard is subsequently published in the Official Journal of the European Union (OJEU).

Harmonised standards lay down the technical specifications necessary for products to meet the essential legal requirements under relevant EU product legislation. By doing so, harmonised standards are the technical foundation to ensure legal conformity in a uniform way across all the EU, supporting the free movement of goods in the EU single market. Their existence also simplifies the tasks of market surveillance authorities, which ensure the safety of all products across Europe. ▶▶

[3] Arts 3(3)(d)–(f), Directive 2014/53/EU
[4] COM(2021) 202 final
[5] COM(2021) 346 final
[6] JOIN(2020) 18 final

Manufacturing products in accordance with harmonised standards implies that such products are in conformity with the corresponding legal requirements. This allows manufacturers to place their products on the market under a swifter procedure.[7]

The use of harmonised standards is voluntary. However, if a harmonised standard is not available, compliance with legal requirements must be proved using other conformity assessment procedures. In most cases, this will require a conformity assessment by 'notified bodies,' third parties officially designated by national authorities to carry out such tasks.

It has been estimated that third-party assessment can cost up to €40,000 per product,[8] which is challenging especially for smaller manufacturers and for less expensive products.

Overview of findings

70%

Most necessary **baseline cybersecurity requirements** are **common across all connected products.** More targeted cybersecurity requirements for specific types of products would constitute 30 per cent on top of the common baseline.

94%

of interviewed experts find that **sufficient cybersecurity cannot focus solely or primarily on product features**, such as passwords. While current EU rules were developed to consider precisely such features, cybersecurity is instead **largely dependent on organisational requirements**, such as cybersecurity management rules (**56 per cent** vs 44 per cent for product requirements).

All interviewed experts agree that **defining baseline cybersecurity requirements for all connected products would be crucial** to improving their overall level of cybersecurity, which is deemed low at present. This would lead to a **good or very good** level of overall cybersecurity for

53%

of experts, with the rest (**47 per cent**) finding it would be **fair.**

46%

Although several cybersecurity standards exist, **almost half of the necessary baseline cybersecurity requirements,** both organisational and product-related, are **not yet adequately covered.** They would need to be further developed before they can be accepted as harmonised standards under current product legislation.

It will take at least

5 YEARS

to develop and apply harmonised standards incorporating the necessary baseline requirements. Half that time would be needed for development, the rest for implementation. Organisational requirements can be developed largely alongside product-based requirements, taking only an additional six months compared to standards focusing only on product features.

[7] More detailed information about harmonised standards can be found in Section 4.1.2 of the European Commission's 2016 Blue Guide on the implementation of EU products rules, available at https://ec.europa.eu/growth/content/%E2%80%98blue-guide%E2%80%99-implementation-eu-product-rules_en

[8] *Commission Staff Working Document Part 1: Evaluation of the Internal Market Legislation for Industrial Products*, available at https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52014SC0023

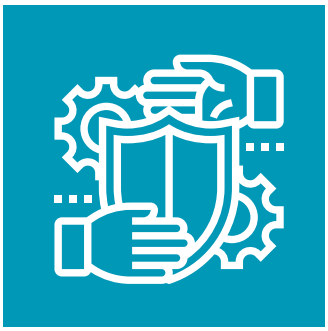
These findings lead to the **following recommendations:**

1

The Commission should prioritise horizontal cybersecurity legislation for connected products.

By more appropriately reflecting the scope of necessary legal requirements, and by allowing standards organisations more time to develop the corresponding technical requirements and methods to verify compliance, a horizontal law can maximise the link between legislation and standards, harmonising cybersecurity across different product categories.

2



Existing product legislation, such as the RED delegated act or the draft General Product Safety Legislation, should not be used to address product cybersecurity.

Because its scope and conformity assessment methods are generally designed to address physical product functions, existing product legislation cannot properly address administrative or organisational aspects, which are more prominent and common to more types of devices.

3

If we do tackle cybersecurity through current product legislation, this should be limited to basic product-related requirements.

Basic product-related requirements that are already supported by existing standards can be adopted as harmonised standards within a shorter timeframe. Such baseline product-related cybersecurity requirements should be repealed once horizontal cybersecurity legislation enters into application.

Study methodology

The data in this report is derived from interviews with 18 cybersecurity experts actively involved in European and international standards organisations. 72 per cent of interviewed experts are active in European standardisation organisations (CEN, CENELEC or ETSI), while the remaining 28 per cent are active in international bodies (ISO/IEC). The full list of interviewees is available on the Acknowledgements page.

Current product rules can only cover device features, but cybersecurity needs more

The overwhelming majority of interviewed experts (**94 per cent**) agree that a sufficient level of cybersecurity for connected products cannot be achieved by focusing solely or primarily on product features.

Examples of product and organisational requirements

- **Product requirement:** If a connected product uses passwords for authentication, such passwords must be unique per device or defined by the user.
- **Organisational requirement:** The manufacturer of a connected product must put in place a vulnerability disclosure policy to enable researchers and others to report security vulnerabilities.

With the minor exception of some devices for which pure product requirements may be sufficient, our experts concur that cybersecurity is not an absolute property that can be measured with certainty under standard product evaluation methods. They stress that product and organisational requirements are not binary – in most cases, both will be needed as they address different issues that are both central to cybersecurity.

By contrast, current EU product rules were developed precisely to consider only performance or functional requirements that can be physically verified in a given product. For example, its physical and mechanical resistance, electrical properties, radioactivity, materials, design or construction.

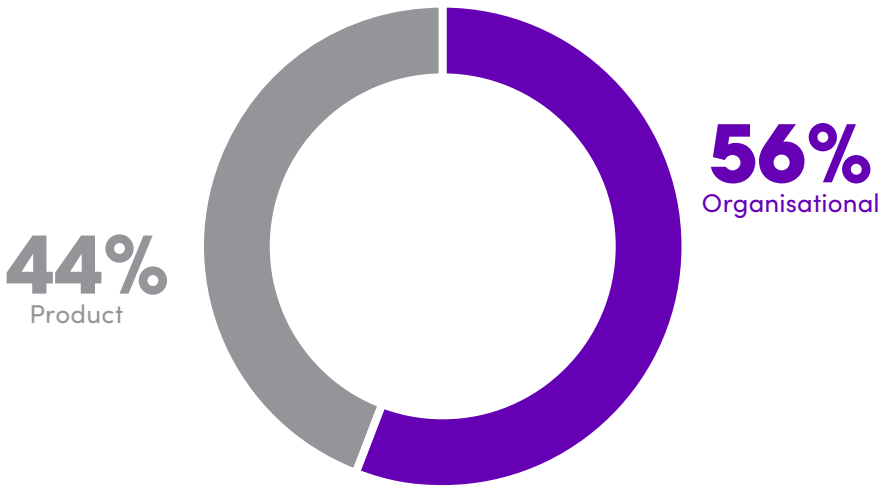
Moreover, such verification occurs at the time a product is placed on the market, while cybersecurity needs to be ensured throughout a product's lifecycle. No product will be secure over time, and organisational requirements are needed to detect and respond to security issues.

94%

of experts find cybersecurity for connected products cannot be achieved with product features alone

ORGANISATIONAL REQUIREMENTS OUTWEIGH TRADITIONAL PRODUCT REQUIREMENTS WHEN IT COMES TO CYBERSECURITY

Share of product vs. organisational requirements estimated to be necessary for the cybersecurity of connected products



According to our experts, physical product features account for **only 44 per cent** of all necessary cybersecurity requirements for connected products. A bigger portion of the requirements (**56 per cent**) should instead focus on **broader administrative, procedural or organisational aspects.**

> *Product requirements are good, but they are only one building block and won't achieve cybersecurity by default.*

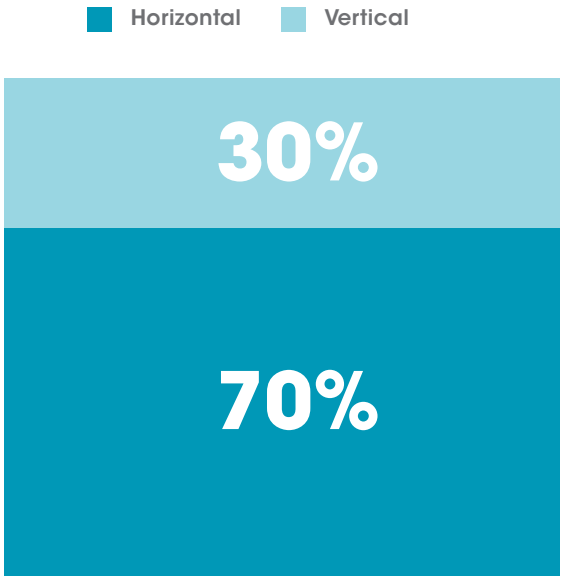
from one of our interviewed experts

Baseline cybersecurity is crucial, and is largely common across all connected products

Our interviewed experts all stress the crucial role that common baseline requirements would play in improving the overall level of cybersecurity for connected products.

MORE THAN TWO-THIRDS OF BASELINE CYBERSECURITY REQUIREMENTS ARE COMMON ACROSS ALL CONNECTED PRODUCTS

Share of horizontal vs. vertical baseline requirements estimated to be necessary for the cybersecurity of connected products



> *Once the industry average improves, we can move to vertical requirements, but a basis of horizontal requirements first is needed.*
>
> from one of our interviewed experts

Interviewed experts found that **70 per cent** of baseline cybersecurity requirements, both product-related and organisational, would be common, or horizontal, across different types of connected products. A few basic threats (related to passwords, for instance) are similar across most connected devices, and defining the related baseline requirements would prevent major risks.

At the same time, there is consensus that beyond this common baseline there will be a need to set out more targeted requirements for specific types of products. Such vertical requirements would constitute **30 per cent** of cybersecurity requirements on top of the common baseline.

Defining the baseline

- Baseline requirements can be defined as a set of requirements that are considered necessary in order to achieve a minimum level of security.

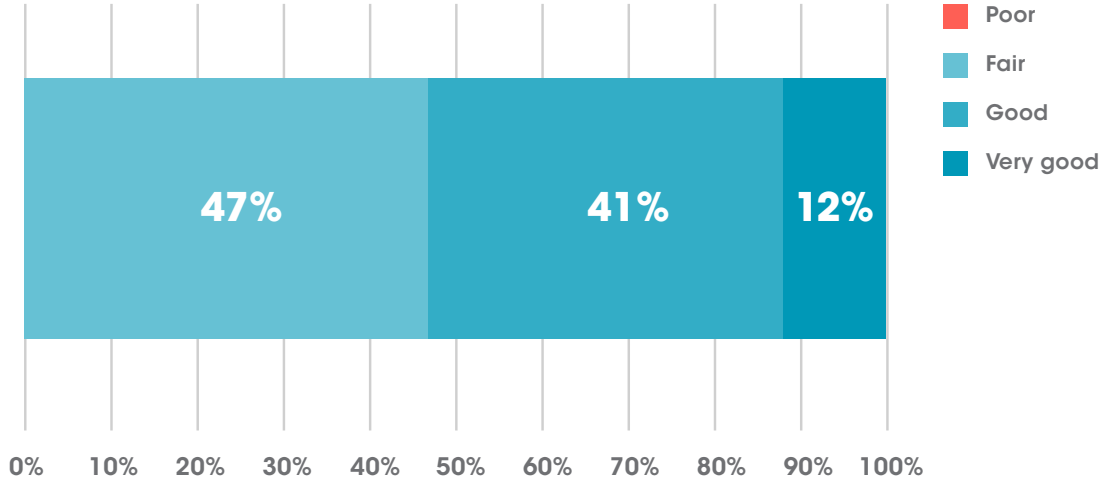
For a majority of experts (**53 per cent**), a common baseline would achieve a **good or very good** level of security, while the remaining **47 per cent** believe a **fair** level can be achieved. This is in contrast with what experts consider to be an overall low level of security at present. None of the experts found that the level of cybersecurity achieved by a common baseline would be poor.

"It's important to reach at least 80% of the threat – not 80% of all requirements, but requirements that cover 80% of the threats."

from one of our interviewed experts

BASELINE REQUIREMENTS WOULD IMPROVE THE LEVEL OF CYBERSECURITY FOR CONNECTED PRODUCTS – FAIRLY OR SIGNIFICANTLY FOR ALL INTERVIEWED EXPERTS

Percentage of interviewed experts by how they would rate the level of cybersecurity achieved by baseline requirements

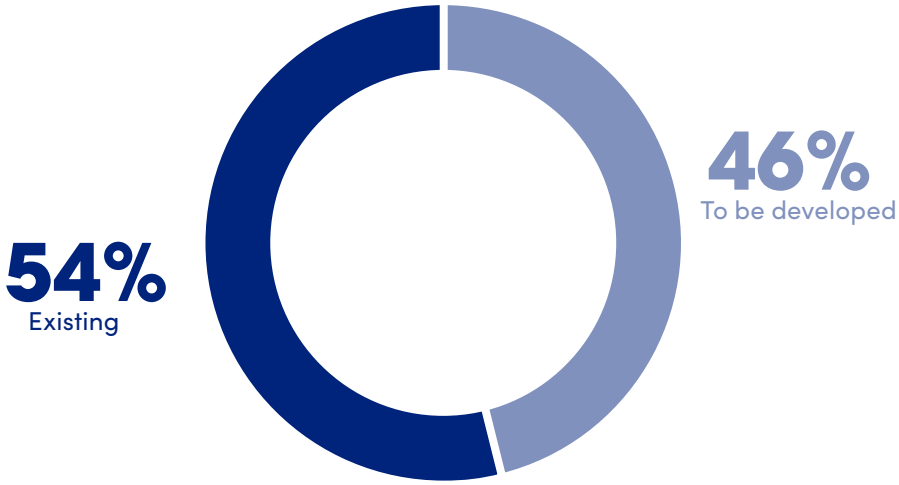


Developing baseline cybersecurity standards under product legislation will take time, except for the most basic ones

Although several cybersecurity standards exist, none today is readily transposable into harmonised standards that would be fit for current product legislation.

ALMOST HALF OF THE NECESSARY BASELINE CYBERSECURITY REQUIREMENTS ARE NOT YET ADEQUATELY COVERED BY EXISTING STANDARDS

Percentage of baseline cybersecurity requirements already covered by existing standards vs needing development before they can be considered for harmonised standards under product legislation



According to interviewed experts, only about half (**54 per cent**) of the technical requirements necessary to achieve a common baseline are already addressed by current standards and ready to be used as harmonised standards for connected products. The remaining half (**46 per cent**) still need to be developed in the standardisation system before they can be considered fit under product legislation and be classified as harmonised standards.

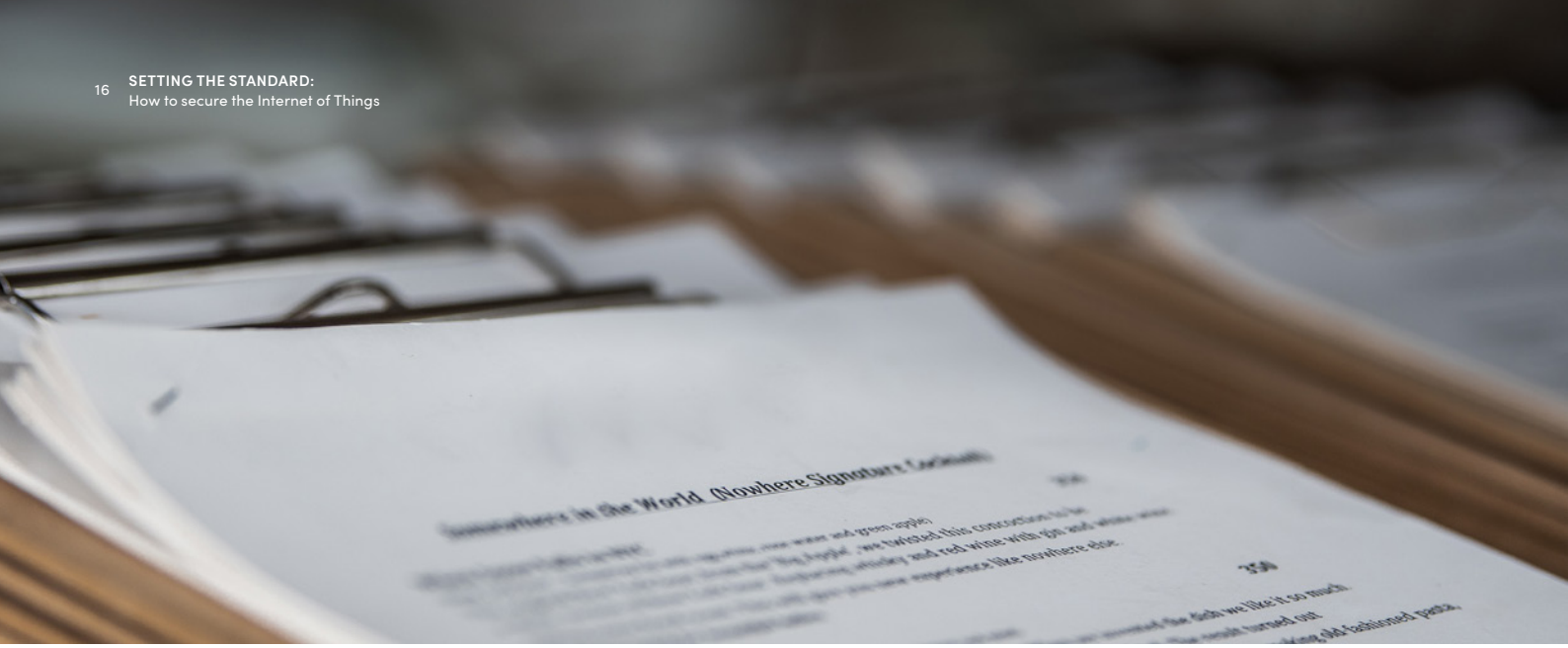
The baseline gap between existing and harmonised standards

- ETSI's Consumer IoT (ETSI EN 303 645) and ISO/IEC's IoT security and privacy (ISO/IEC CD 27402) standards are mentioned by experts as a good basis for the development of harmonised standards for baseline cybersecurity of connected products.

  However, interviewed experts find that they **only cover about half** (54%) of the technical requirements that can be accepted in harmonised standards based on current product legislation.

> *Standards are covering the static part of cybersecurity based on what we know – the reactive/dynamic part that takes future technologies into account is still missing and more work needs to be done.*
>
> from one of our interviewed experts

> *We have good standards, but not one standard that covers everything, and none of them are ready to be used as harmonised standards.*
>
> from one of our interviewed experts



In light of the maturity of existing standards and the development process for harmonised standards, experts on average estimate that it would take **five years** to develop and apply harmonised standards supporting product-related requirements. Half that time (two and a half years) would be required to have the standards developed and published in the Official Journal, with the remaining time required for implementing the standards into products before they can be sold.

This timeline would not change considerably if organisational requirements were also covered. Interviewed experts on average estimate that considering organisational requirements in the standards development process would only take an **additional six months** – three years as opposed to two and a half – with no further impact on product implementation, which would still require two and a half years after that.

> *We need to do it only once. Cost is not the biggest issue, but rather the uncertainty of having to repeat the whole process again.*

from one of our interviewed experts

IT WILL TAKE AT LEAST FIVE YEARS TO DEVELOP AND APPLY BASELINE HARMONISED STANDARDS

Time estimated to be required to develop and apply harmonised standards supporting baseline cybersecurity requirements (in months)

These timelines are subject to variables. Important factors highlighted by experts include:

- **How much the requested harmonised standards would need to deviate from existing standards.** The more existing standards can be reused, the sooner harmonised standards can be finalised. By contrast, the development of harmonised standards would take longer if different or additional requirements were to be mandated.
- **The complexity of the device, the granularity of the requirements and the nature of the change.** For example, experts estimate that hardware changes require more time than software.
- **The extent to which verticals are willing to accept standards from other verticals and other regions.** Some verticals also have a more advanced level of cybersecurity and will not have to start from scratch when it comes to implementation.
- **To what extent companies are involved in the development process.** While bigger manufacturers are usually involved in standards development and can therefore be expected, to some extent, to start considering implementation while standards are being written, smaller manufacturers tend to be less involved and will therefore need more time to adapt. SMEs might just not have the necessary understanding of cybersecurity or budget to hire experts.
- **The extent to which manufacturers have already adopted similar organisational requirements.** A few experts noted that organisational and product-related requirements are separate but parallel processes. In this context, organisational requirements need to be in place first or product-related ones will not be implementable.

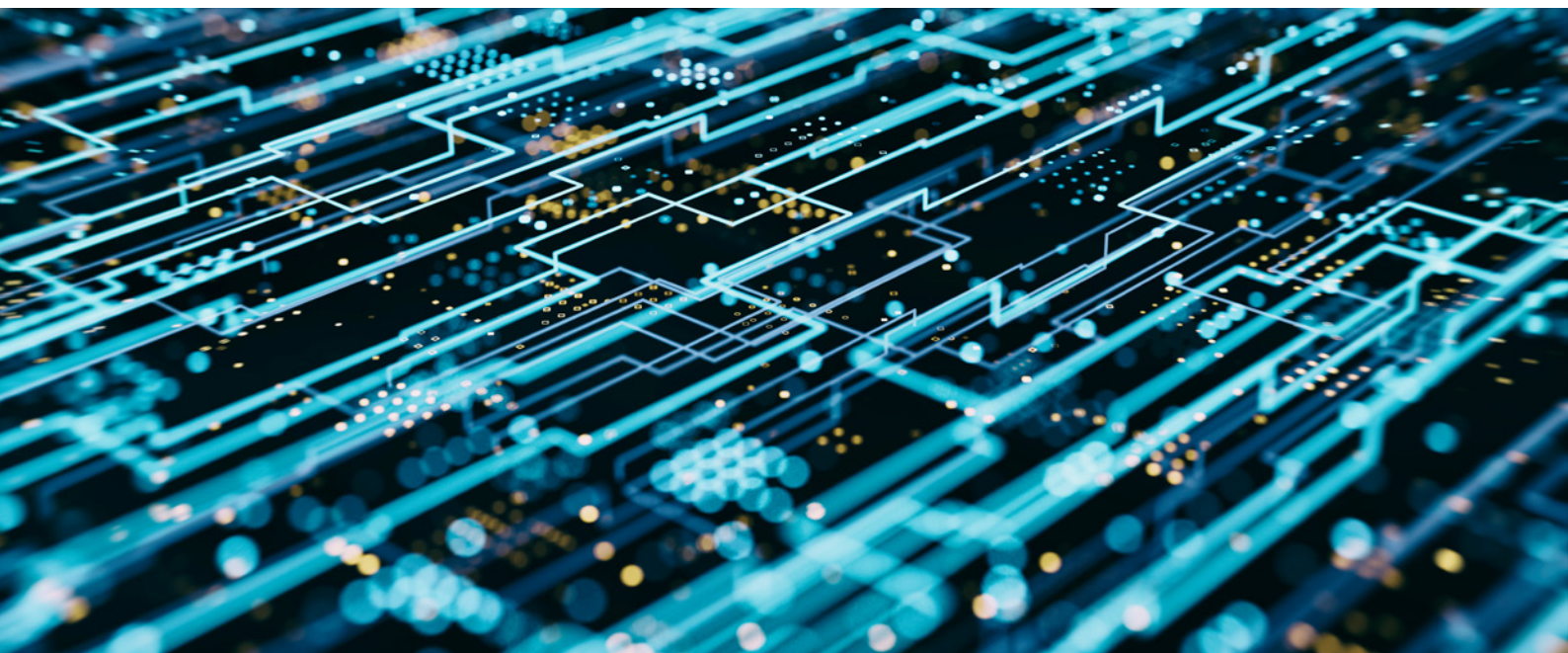
Additional remarks

We need to develop standards for Europe but with global applicability in mind. The EU should see itself not only as a consuming part of the world, but also the selling part of the world.

from one of our interviewed experts

Interviewed experts shared a few further observations that should be kept in mind by policy makers in developing the right legal framework:

- Many experts discussed the right balance between prescriptive rules, which ensure testability but might stifle innovation, and outcome-focused rules that are technology neutral and less prescriptive. Many concluded that **overly prescriptive requirements should be avoided in favour of framework rules,** so that ample latitude is allowed for standards bodies to find the best approach from a technical perspective.
- The discussion about cybersecurity and product legislation seems to assume that cybersecurity is a static threat, while in reality it is a moving target. Vulnerabilities evolve fast and often unexpectedly, and **crystalised requirements stemming from what we know today will similarly get outdated very fast.**
- At present, there is **less of a need to develop completely new requirements from scratch than there is to adjust existing tools to new use cases.** Existing standards already provide the right toolbox, and legislation should adapt to reflect these tools.
- The importance of international alignment has been mentioned by many interviewed experts. Not only have cybersecurity standards emerged largely through global efforts, but the **scalability of EU harmonised standards is essential for European companies developing their products for global markets.** Adopting harmonised standards that are not aligned with global standards will force companies to redesign their product compliance for other markets, wasting considerable resources.



Acknowledgments

This report is based on interviews with 18 cybersecurity experts actively involved in European and international standards organisations.

Jeppe Pilgaard Bjerre, Expert at ISO / IEC JTC 1 / SC 41 'Internet of Things,' member of the Danish Standards S840 committee 'Internet of Things' / Product Compliance Specialist, Force Technology

Ian Brooker, Expert at IEC, IEEE, CENELEC, ETSI and CEPT / Senior Manager, Regulatory Engineering, Johnson Controls

Brian Copsey, Chair of ETSI ERM TG 17 Broadcast & ancillary comms equipment / Director at Copsey-Comms

Amit Bar On Elazari, Expert at ISO/IEC / Director, Global Cybersecurity Policy, Intel Corp.

Stephan Fertig, Technical Regulation, Standardization, Research & Development Manager, Panasonic

Walter Fumy, Chair of ETSI JTC 13

Daniel Gonzalez, Expert at CEN/CENELEC / Standardization Officer, Schneider Electric

Ben Knox, Convenor of CEN-CENELEC JTC 13/WG 6 / Director Product Security, Philips

Alex Leadbeater, Chair of ETSI TC Cyber / Head Global Obligations Futures and Standards, BT

Markus Dominik Mueck, Vice-Chairman at the Board of ETSI / Principal Engineer, Intel Corp.

Kirsty P., UK Department for Digital, Culture, Media & Sport, UK Parliament

Davide Pratone, Vice-Chair ETSI TC CYBER / Director of Consumer Business Group European Standardization & Industry Development, Huawei

Gaus Rajnovic, Cybersecurity Manager, Panasonic

Judith Rossebo, Convener of CENELEC TC65X / Specialist, ABB AS

Enrico Scarrone, Chair of ETSI SMARTM2M Committee / TIM

Peter Stephens, Head of Secure by Design, UK Department for Digital, Culture, Media & Sport

Andreas Wolf, Chair of ISO/IEC Joint Committee IT Security Techniques

Kai Wollenweber, Expert at ISO/IEC / Digital Industries, Strategy & Technology Cybersecurity, Siemens AG

DIGITALEUROPE represents the voice of digitally transforming industries in Europe. We stand for a regulatory environment that enables businesses to grow and citizens to prosper from the use of digital technologies.

We wish Europe to develop, attract and sustain the world's best digital talents and technology companies.

DIGITALEUROPE's members include over 35,000 companies in Europe represented by 86 Corporate Members and 39 National Trade Associations.

www.digitaleurope.org

@DIGITALEUROPE

For more information please contact:
Chris Ruff, Director of Communications & Political Outreach
chris.ruff@digitaleurope.org
+32 485 55 22 54

DIGITALEUROPE
Rue de la Science, 14
B-1040 Brussels
Info@digitaleurope.org
+32 2 609 53 10

DIGITALEUROPE