OECD*publishing*

ENHANCING THE DIGITAL SECURITY OF PRODUCTS

A POLICY DISCUSSION

OECD DIGITAL ECONOMY PAPERS
February 2021 **No. 306**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report was prepared by the OECD Working Party on Security in the Digital Economy (SDE) following discussions held at the inaugural event of the OECD Global Forum on Digital Security for Prosperity (GFDSP) in 2018 (OECD, 2019[1]). It builds upon a separate report on "understanding the digital security of products", which provides a more in-depth analysis (OECD, 2021[2]).

This report has been developed in parallel and should be read in conjunction with the OECD report on "encouraging vulnerability treatment: an overview for policy makers" and the associated background report (OECD, 2021[3]; OECD, 2021[4]). Both work streams on digital security of products and vulnerability treatment were meant to inform the review of the OECD *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* (OECD, 2015[5]).

This report was approved and declassified by the OECD Committee on Digital Economy Policy on 30 November 2020. It was drafted by Ghislain de Salins, under the supervision of Laurent Bernat, and with support from Matthew Nuding and Marion Barberis of the OECD Secretariat. Delegates to the OECD SDE also provided input and valuable feedback, as well as delegates to the OECD Working Party on Consumer Product Safety (CPS).

The Secretariat was supported by an international and informal advisory group comprising 94 experts from government, business, the technical community and civil society who sent written input, and met face-to-face in February and virtually in July 2020, under the auspices of the OECD GFDSP. The Secretariat wishes to thank all these experts for their valuable feedback on earlier drafts, and in particular, Christopher Boyer, Kaja Ciglic, Amanda Craig, Amit Elazari, Sudhir Ethiraj, Stefan Frei, Anastasiya Kazakova, Amélie Koran, Jacques Kruse Brandao, Ariel Levite, Riccardo Masucci, Frederico Oliveira Da Silva, Stephen Pattison, Axel Petri, Raphael Reischuk, Stefan Saatmann, Rayna Stamboliyska and Tarah Wheeler.

Note to Delegations:

This document is also available on O.N.E. under the reference code:

DSTI/CDEP/SDE(2020)11/FINAL

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Acronyms

AIC:	Availability, Integrity and Confidentiality
CDEP:	Committee on Digital Economy Policy (OECD)
CERT:	Computer Emergency Response Team
COE:	Council of Europe
COTS:	Commercial off-the-shelf
DCMS:	Department for Digital, Culture, Media and Sport (UK)
DDoS:	Distributed Denial-of-Service
DHS:	Department of Homeland Security (USA)
ETSI:	European Telecommunications Standards Institute
EOL:	End-of-life
EOU:	End-of-use
GDPR:	General Data Protection Regulation
ICS:	Industrial Control Systems
IETF:	Internet Engineering Task Force
IoT:	Internet of Things
ISO:	International Organisation for Standardization
MFA:	Multi-Factor Authentication
NATO:	North Atlantic Treaty Organisation
NIST:	National Institute for Standards and Technology (USA)
NTIA:	National Telecommunications and Information Administration (USA)
OECD:	Organisation for Economic Co-operation and Development
OEM:	Original Equipment Manufacturer
OS:	Operating System.
SDE:	Working Party on Security in the Digital Economy (OECD)
SDG:	Sustainable Development Goal
UN:	United Nations
VDP:	Vulnerability Disclosure Policy

Table of contents

FIGURES

Executive Summary

Our economies and societies are increasingly reliant upon "smart products", i.e. products that contain code and can connect. They include "pure" software, "traditional" IT devices as well as Internet of Things (IoT) products. As highlighted in the in-depth analysis report (OECD, 2021[2]), smart products frequently have an insufficient level of digital security, resulting from gaps that can emerge at different stages of their lifecycle and steps of their value chain.

Digital security gaps are often caused by economic factors

Digital security gaps in smart products are often imputable to economic factors. They include **insufficient market incentives** for economic agents, fueled by **information asymmetries and externalities**; an **unclear allocation of responsibility** amongst actors; and **a lack of cooperation** across sectors, stakeholder groups, government agencies and at the international level.

As a result, there is a lack of adherence to voluntary guidelines and standards for security-by-design and security-by-default, and the treatment of newly discovered vulnerabilities is often suboptimal. In many cases, smart products continue to be used even though they are no longer supported with security updates from supply-side actors. This **end-of-life (EOL) gap** – the gap between the end of security support and the end of use – needs to be addressed. With billions of IoT products reaching their EOL in the coming decade, the possibility of an "Internet of forgotten things" is a looming policy challenge.

Six high-level principles to enhance the digital security of products

To address these challenges, the report outlines **six high-level principles** that can guide the action of policy makers and stakeholders more broadly to enhance the digital security of products:

- **Increasing transparency and information sharing**, in order to address information asymmetries, including for the traceability of smart product's components**.**
- **Raising awareness and empowering stakeholders**, in particular end-users and security researchers, as they have a key role to play in managing digital security risk.
- **Ensuring responsibility and duty of care** for supply-side actors, to tackle externalities and realign market incentives. The principle of duty of care can be broken down into five sub-principles: **security-by-design**, **security-by-default**, dynamic management of digital security, digital security of the organisation and responsible EOL policies, which can address issues related to the length of support and the product's repairability.
- **Increasing co-operation** between stakeholders, government agencies and at the international level to enhance the digital security of products.
- **Promoting innovation and competition**, to unleash the positive potential of market forces.

- **Addressing digital security with proportionality, through a risk-based approach,** to take into account complexity. Digital security requirements that may be necessary or effective for one market or product category may not be appropriate for another.

A policy toolkit: "smart policies for smart products"

Smart products require smart policies for digital security. Policy makers could usefully approach digital security policy as software engineers approach product development: through an iterative and end-user centric process. Light-touch, voluntary mechanisms could be implemented as a first step. If those are not successful, or if the industry and consumers – the "end-users" of policies – are not receptive, then the use of more stringent regulatory instruments, such as *ex ante* requirements and *ex post* mechanisms, could be further explored. Equally, software engineers can also learn from policy makers. Balancing the interests of various stakeholder groups, considering the impact of their decisions on others and taking into account the longer term should become an inherent part of the development cycle of smart products.

The dichotomy of government intervention v. "laissez-faire" is increasingly considered as too simplistic to capture the broad spectrum of policy options available to enhance the digital security of products**.** In the United States, a report recently recognised that "the status quo is not getting the job done". Policy makers can leverage many tools, from awareness-raising campaigns and multi-stakeholder partnerships to labelling schemes and regulatory requirements. Importantly, these tools are not mutually exclusive, and there is no panacea or one-size-fits-all solution. **A strategy to enhance the digital security of products will likely require a mix of policy tools to be most effective**.

The policy toolkit outlined in this report aims to enable governments to foster the adoption of the high-level principles, focusing on the "how" rather than on the "what". The toolkit discusses emerging policy trends, illustrated with selected examples from OECD countries. The format of the toolkit acknowledges that each government may rely on the policy tools that are the most consistent with its country's culture, history and style of government. It discusses the following policy tools:

- **Raising awareness of mainstream users and developing digital security skills** in order to grow the expert workforce of advanced users, is the starting point of public policies to enhance the digital security of products. However, while important, awareness-raising campaigns alone would not be sufficient to address the economic challenges identified in this report.
- **Beyond their role as regulators, governments are also economic agents. As such, they can leverage their purchasing power and lead by example** to influence the behavior of other stakeholders. Through public procurement policies, they can incentivise supply-side actors to certify the digital security of smart products. Governments should also apply to themselves the principles they often call others to follow – for instance, regarding the timely patching of vulnerabilities.
- **Technical standards and voluntary frameworks are also paramount**. Developed by the government or the multi-stakeholder community, they provide supply-side actors with clear guidance, which can be adapted to each specific market or product category. However, on markets where externalities and information asymmetries are significant, the uptake of voluntary guidance is likely to be limited.
- **Labels** could incentivise supply-side actors to adhere to standards and frameworks, and contribute to reduce information asymmetries. As of November 2020, Finland, Germany and Japan have launched, or are considering launching labelling digital security schemes for specific product categories such as consumer IoT or routers. However, consumer fatigue and lack of uptake by the industry need to be considered as potential drawbacks of labelling initiatives.
- ***Ex post* mechanisms also have a great potential, but their effectiveness needs to be further assessed**. While code is everywhere, smart products are relatively new and do not necessarily fit

in the legal categories of the 20th century. The application of liability laws, insurance and guarantees to smart products is challenging, and will likely require a review of existing frameworks to adapt them to the dynamics and complex value chains of the digital economy.

- **Finally, there is also a growing interest in some OECD countries to develop more stringent regulations to enhance the digital security of products**. From technical requirements to high-level principles, such *ex ante* regulations could be very effective at realigning market incentives and ensuring the duty of care of supply-side actors. However, *ex ante* requirements carry a risk of disproportionate use. An ill-prepared law could quickly become obsolete or unenforceable. The report examines the opportunities and challenges associated with *ex ante* requirements, and provides some key insights, for instance regarding the need for technological neutrality, proportionality and international cooperation.

More international co-operation is key

It is essential that policy makers take a **holistic approach** to the digital security of products. There is now a window of opportunity for governments to design smart policies for smart products, to be proactive rather than reactive, and to shape the policy environment for the digital security of products with foresight.

In that regard**, international co-operation stands out as a key success factor**. For policy makers, it is key to **learn from other countries' successes and challenges**, and to leverage policies that have already proved successful elsewhere. Some cutting-edge policies developed nationally have formed the basis of emerging international norms: a code of practice developed by the government in the UK paved the way for ETSI's technical specification for consumer IoT security.

International co-operation is also instrumental to enable interoperability between national approaches, avoid norm proliferation and limit inconsistencies across jurisdictions, which could significantly inhibit the development of the digital economy.

1 Structure and scope

The objective of this policy report is to raise awareness and inform the development of international guidance on the digital security of products, in particular through:

- Identifying key challenges and priority areas that need to be addressed by policy makers and stakeholders more broadly ;
- Developing high-level principles that can serve as guidance to enhance the digital security of products ;
- Exploring the broad range of policy tools, including emerging best practices, which could be used to address the key challenges and foster the adoption of the principles.

This report is structured in four chapters:

- This chapter describes the structure of this report and recalls the scope of this work stream.
- Chapter 2 summarises the key challenges and priority areas that have emerged from the in-depth analysis report (OECD, 2021[2]).
- Chapter 3 develops high-level principles that could serve as references for stakeholders in order to enhance the digital security of products.
- Chapter 4 proposes a policy toolkit exploring the broad range of options available to policy makers to address the key challenges and foster the adoption of the high-level principles.

While chapters 2 and 3 focus on "what" needs to be fixed or promoted, chapter 4 discusses "how" policy makers can take action.

Annex A provides a detailed version of the high-level principles. Annex B provides a detailed version of the policy toolkit. Annex C discusses the merits and limits of the analogy between car safety in the 20th century and the digital security of IoT in the 21st century.

As OECD's mandate is limited to economic and social prosperity, this report focuses on the economic factors (e.g. market incentives) and actors (e.g. producers, users) that are responsible for the digital security of products, and on policy principles and instruments to address the gaps identified in the in-depth analysis report (OECD, 2021[2]). This report does not address directly issues related to national and international security, intelligence and criminal law enforcement. Similarly, this report intends to approach the digital security of products at a policy level, rather than at a technical level (which is the focus of other organisations such as ISO).

The scope for products is large, as it includes all goods and services that contain code and can connect. The term "product" therefore refers to this definition of "smart products", unless specified otherwise.

The terms used in this report have been defined and discussed in the in-depth analysis report (OECD, 2021[2]). A Glossary at the end of this report, provides a summary of the key definitions that are essential to understand the following chapters.

2 Key challenges and priority areas

This chapter presents the key challenges and potential priority areas to enhance the digital security of products. The first section explores the challenges that have been identified as key across the three case studies developed in the in-depth analysis report (OECD, 2021[2]). For a more detailed discussion of these challenges, readers can refer to the in-depth analysis report. The second section discusses a few priority areas that could be addressed by policy makers.

2.1. Key challenges

2.1.1. Complexity

From a high-level perspective, the complexity of smart products, which spans many levels, is at the core of the key challenges described in this chapter:

- The code contained in smart products is often complex, and increasingly so as products become more sophisticated.[1]
- The interactions smart products have with one another are complex. Many products are interdependent and part of complex ecosystems (e.g. IoT products often rely on cloud services).
- Their value chain is complex, and involves many actors whose economic interests may be misaligned or even opposite. The code owner best the placed to fix a newly discovered vulnerability may not be the final product's vendor.
- Their broader ecosystem is complex, and involves many stakeholders who may have a positive (e.g. security researchers) or negative (e.g. malicious actors) impact on the product's level of digital security.
- Smart products are part of a global market, and are often subject to many jurisdictions. The development of policy tools without co-operation carries the risk of inconsistencies across jurisdictions as well as norm proliferation and fragmentation.
- At the national level, smart products are subject to various policy areas, which often rely on different conceptual frameworks (e.g. digital security, consumer protection, privacy, product safety, liability, law enforcement, etc.).
- The concept of "smart products" is very broad and covers a wide range of product categories and contexts of use. Some digital security features may be relevant in one sector (or "vertical", e.g. health) and less so in another one. In the same time, some products designed for consumers are often used in an industrial context, which may make the "vertical approach" difficult to implement.

To address this complexity, the report discusses high-level principles, which by nature are flexible enough to adapt to various product categories and contexts. In particular, the principle of "proportionality and risk management" (see section 3.6) and the design of "smart regulation" (see section 4.1) are key to tackle smart products' complexity.

2.1.2. Market incentives are insufficient

The in-depth analysis report (OECD, 2021[2]) has shown that market dynamics on their own often fail to incentivise stakeholders to optimise the digital security of products. This market failure results from a misperception of digital security risk, a misalignment of incentives, as well as significant information asymmetries and externalities.

Digital security risk is often silent, and therefore difficult to identify and manage. While consumers can test the brakes on a bike before going for a ride, vulnerabilities in products, and the consequences of their exploitation by malicious actors, are more difficult to perceive. Often, the victims of a digital security incident affecting the products they use are not aware of its occurrence, and many intrusions go unnoticed for months or even years (Kregs on Security, 2020[6]). This misperception of digital security risk builds on a lack of awareness and education, and contributes to explain in part why many consumers and organisations do not implement security updates in a timely manner, continue to use products after they reach their EOL or misconfigure their cloud services. The complexity described in section 2.1.1 further increases the misperception of digital security risk, and makes it more difficult for organisations, in particular "mainstream users" such as SMEs or institutions in the healthcare sector, to accurately assess and treat digital security risk.

For many smart products, market incentives are not sufficiently aligned to reach an optimal level of digital security. Supply-side actors are often incentivised to minimise costs and time to market, rather than to build in appropriate digital security measures and maintain the products for a reasonable period through timely security updates (DHS and DoC, 2018[7]). Market incentives need to be realigned to promote a better balance between digital security and other factors such as usability, features and price.

In addition, information asymmetries are very significant for products that contain code. They result from a lack of transparency regarding their components, their digital security features and the policies put in place by code owners to maintain the product throughout its lifecycle (e.g., length of support). Usually, end-users do not know "what's in the box" as they cannot access the source code[2] of the product or a list of the product's code components. In addition, third-parties are usually not authorised to test or reverse-engineer the product's code (e.g. because of intellectual property rights). These information asymmetries have an impact on both the demand-side and the supply-side, as they prevent end-users from assessing the digital security of products accurately, and supply-side actors that invest in digital security from differentiating their products on the market.

Finally, in many cases, significant externalities prevent the markets for smart products to deliver optimal outcomes. DDoS attacks are a typical example of the prevalence of externalities for smart products, as the economic agents that make the decision about how much risk to take, or what level of digital security is sufficient, are not the economic agents bearing the costs of the digital security attacks. In the IoT market, product manufacturers are "unlikely to face immediate economic costs borne by a DDoS attack conducted through their devices, and, therefore, they do not face sufficient commercial incentive to invest in a secure by design approach" (DCMS, 2018[8]). As there are no consequences, and no incentives, for the stakeholders that are the best placed to mitigate the risks (the producers, network operators and owners of the products that have been enrolled into a botnet), the scale and scope of DDoS attacks is likely to increase in the future, if no action is taken. The case of the Mirai botnet shows that malicious actors increasingly target poorly secure IoT devices in order to perform DDoS attacks.

To address this challenge, there is a need to increase transparency and information sharing (see section 3.1), raise awareness and empower stakeholders (see section 3.2), ensure the duty of care of supply-side actors (see section 3.3), facilitate co-operation (see section 3.4) and support innovation and competition (see section 3.5). Various policy tools may be used to achieve these objectives, as described in chapter 2.2

2.1.3. Responsibilities are unclear and often misallocated

There is often a misallocation of, and a lack of clarity about, stakeholders' responsibility for smart products, resulting from the complexity and opacity of the value chain. As products are often made of multiple layers of code, the end-user, and even the vendor, are often not aware of the identity and contact information of each code owner. Product manufacturers that integrate commercial off-the-shelf (COTS) software in their products often lack the ability to manage their digital security risk.

In many cases, the supply-side actors tend to place too much responsibility on the end-users, in particular mainstream users, even though they are often not the best placed to manage the risk associated with the product. This lack of security-by-default (see section 3.3.2) is particularly significant for IoT products and cloud services.

This misallocation also results from the limited liability of the supply-side actors (e.g. software designers and cloud providers), often determined through the strict license agreements that users have to accept, and which disclaim any liability in case of security incidents (Dean, 2018[9]; Schneier, 2018[10]).

To address this challenge, there is a need to clarify the roles and responsibilities (see sections 3.3 and 3.4), for instance through facilitating multi-stakeholder discussions in order to link each digital security control and layer of code with a specific actor.

2.1.4. Lack of co-operation

The challenges that explain the suboptimal level of digital security of many products are exacerbated by a lack of co-operation across stakeholder groups, government agencies and countries.

The digital security gaps that emerge during the product's commercial life often arise from a lack of co-operation between code owners and actors of the product's value chain. As a result, code owners do not provide security updates, or these updates are not timely deployed across the value chain. More broadly, the potential contribution of the multi-stakeholder community to enhance the digital security of products is still largely untapped. For instance, the co-operation between security researchers and the private sector to detect and report vulnerabilities (e.g. through vulnerability disclosure policies) is too often limited because of a lack of awareness, cultural gaps, legal barriers or a lack of trust (see the vulnerability treatment report (OECD, 2021[4])). Similarly, advanced users with extensive technical skills are often unable to enhance the digital security of the products they use because of intellectual property rights, e.g. they are not legally authorised to access the source code, to reverse engineer a product or to repair or maintain a product after its EOL.

As code is widespread in products across many sectors, it raises challenges in terms of governmental responsibility and oversight. In many cases, there is a convergence between sectoral regulators, horizontal authorities (consumer product safety, competition, data protection…) and authorities in charge of digital security. The in-depth analysis report (OECD, 2021[2]) details the challenges raised by the increasing convergence between digital security and product safety. If not properly anticipated and managed, this convergence might easily lead to overlap, contradictory recommendations for the industry or conflicts between institutions.

Finally, there is a risk that initiatives or rules developed nationally may not be sufficient to have a significant impact on the digital security of products. As noted by the United States' Department of Commerce and Department of Homeland Security (2018[7]), the case of botnets exemplifies how digital security risks in globally used products require international co-operation. In 2016, most attacks by the Mirai botnet targeted the United States, while most of the infected devices were located in other jurisdictions, for instance in Brazil, Colombia and Viet Nam (with more than 40 000 infected devices in each country) and in People's Republic of China, South Korea and Russia (with more than 15 000 infected devices in each country).

Therefore, any action aiming to identify and clean infected devices might fall short of its objectives if it remains limited to a national or even regional scope.

In addition, without international co-operation, there is a risk of fragmentation and inconsistencies across jurisdictions as governments across OECD countries develop divergent or contradictory regulatory frameworks. This could significantly increase the costs of compliance for businesses, and hinder the benefits brought by the digital transformation. In contrast, increased co-operation would enable governments, and other stakeholders more broadly, to define common rules and principles that could significantly raise the level of digital security for smart products, and create a level playing field.

To address this challenge, there is a need to intensify co-operation (see section 3.4), for instance through facilitating multi-stakeholder discussions and enabling interoperability between legal frameworks, at the national and international levels.

2.2. Priority areas

This section focuses on a few priority areas that have emerged from the cases studies developed in the in-depth analysis report (OECD, 2021[2]). The cases studies focused on identifying digital security gaps across three product categories: smartphones and desktop computers, IoT products and cloud services. For policy makers, the following takeaways are important:

- Gaps during design and development are less common in mature and more concentrated markets, but they are particularly significant in emerging and fragmented markets such as the IoT. In the latter, supply-side actors need to be better incentivised to implement standards and guidelines, e.g. through public procurement, certification, labels and *ex ante* requirements.
- The gaps that emerge during the commercial life of smart products (misconfiguration or limited deployment of security updates) are the most significant across product categories. All stakeholders need to be better incentivised to manage the product's digital security risks dynamically, throughout their commercial life (e.g. to deploy security updates). A priority could be to promote "security-by-default" (see section 3.3.2), and in particular automatic updates, through ensuring the duty of care of supply-side actors.
- The EOL gap is very significant for goods such as IoT products and smartphones, and needs to be addressed through effective policy tools.
- The market for IoT products should be addressed in priority, keeping in mind that all stages of their lifecycle need to be taken into account: enhancing "security-by-design" is a good first step but will not be enough.

2.2.1. Standards to integrate digital security in design & development are not widely used

Over the years, many voluntary standards and guidelines to enhance the digital security of products have been developed.[3] However, while these tools are widely available, they are not widely used (DHS and DoC, 2018[7]). For instance, the adherence to security-by-design guidelines greatly varies across markets and sectors: it tends to be high for leading tech companies such as Apple, Google and Microsoft, which are often very active in the development of technical standards, but much lower in less digitally mature sectors or for smaller companies entering the IoT market.

To address this challenge, policy makers could better incentivise supply-side actors to adhere to guidelines and technical standards, for instance through public procurement, certification, labels, ex ante requirements and ex post mechanisms (see chapter 2.2).

2.2.2. The dynamic nature of digital security risk is not sufficiently addressed

Even though the application of “security-by-design” standards can reduce the number of vulnerabilities, code will always contain undiscovered, or latent, vulnerabilities: it is unrealistic to attempt to “secure” a product “once and for all”. As many vulnerabilities are discovered after the product has been released, code owners need to provide security updates in order to fix newly discovered vulnerabilities. Updatability or “patchability” is widely recognised as a best practice to enhance the digital security of products (Schneier, 2018[10]).

However, the deployment of security updates is often suboptimal, both for “traditional” IT products like smartphones and computers, and for emerging markets such as IoT products. For example, in 2018, a study of 331 consumer IoT products in the UK showed that 90% of the manufacturers lack a vulnerability disclosure policy (IoT Security Foundation, 2018[11]). This often results from complex value chains that require action at various steps for security updates to be deployed (e.g. OEMs, network operators and end-users). In the United States, a report recently recognised the lack of a “clearly defined duty of care” regarding the development and deployment of patches, noting that recent research suggests that “50% of vulnerabilities remain without a patch for more than 438 days after disclosure” (Cyberspace Solarium Commission, 2020[12]).

To address this challenge, policy makers could raise awareness about the dynamic nature of digital security risk (see section 3.2) and better ensure the duty of care of supply-side actors by promoting “security-by-default’ (see section 3.3.2). Policy makers could also facilitate multi-stakeholder partnerships and set *ex ante* requirements.

2.2.3. The End-of-life (EOL) gap is a looming policy challenge

The EOL gap is the gap between the EOL and the EOU. It appears when end-users continue to use smart products while supply-side actors cease to provide security updates. Products that continue to be used after their EOL tend to become less secure. In fact, after EOL, the exploit maturity for known vulnerabilities is likely to increase, and latent vulnerabilities may be discovered. Security experts have also observed that some malicious actors take into account the EOL in their attack strategies, and may wait until the EOL to start exploiting zero-day vulnerabilities they have discovered, anticipating that no security updates will be provided by code owners.

The EOL gap is particularly pressing for goods such as smartphones and desktop computers. In January 2020 ((n.a.), 2021[13]), around 30% of iPhones and desktop computers running Windows worldwide ran on operating systems that had reached their EOL. Around 60% of Android smartphones worldwide ran on an outdated version of the OS. While there are no available statistics for IoT products at the international level, the EOL rate (i.e. the percentage of products that are no longer supported but still in use) is likely to be higher than for desktop computers and smartphones, and to grow significantly in the coming years (Schneier, 2018[10]). This may result in what some have called “the Internet of forgotten things”.

The EOL gap illustrates the misalignment of market incentives: producers’ preference is to reduce their costs and incentivise end-users to buy new products, while customers’ preference is to continue to use a product as long as it fulfills their needs. The EOL gap also raises environmental challenges, as it contributes to increase e-waste significantly, against Sustainable Development Goal (SDG) 12, and in particular target 12.5, which aims to substantially reduce waste generation through repair, recycling, and reuse.

To address the EOL gap, policy makers could raise awareness for users, in particular mainstream users that are more likely to continue using smart products after EOL. Policy makers could also increase the responsibility and duty of care for supply-side actors, so that they maintain their products for a longer period. They could also increase products’ “repairability”, by incentivising supply-side actors to allow other stakeholders to take responsibility after EOL (e.g. the user or open-source community). Effective policy tools to address this challenge could include public procurement, labels, *ex ante* requirements and *ex post* mechanisms (see chapter 4).

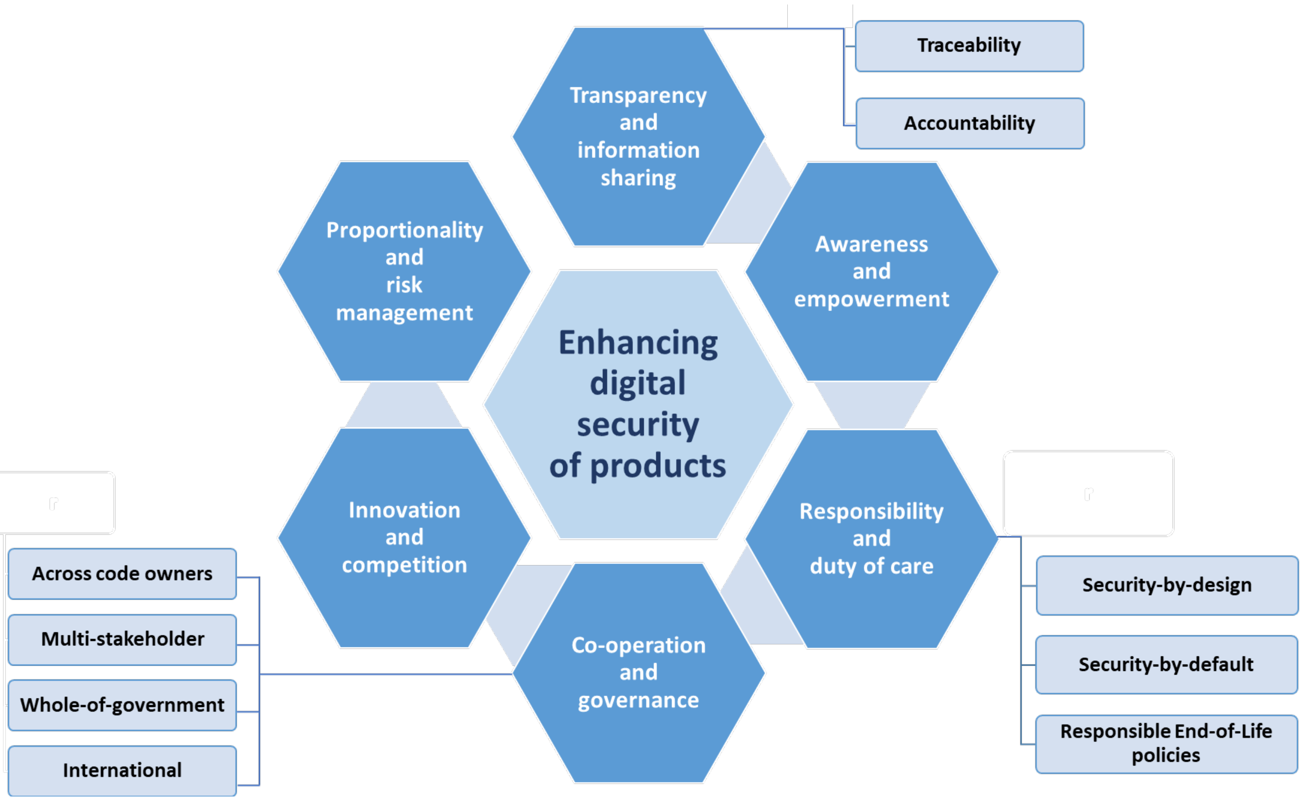
3 High-level principles

This chapter discusses high-level principles to address the key challenges identified in chapter 2.

To address information asymmetries, there is a need to increase transparency and information sharing. To tackle externalities and realign market incentives, it is key to ensure responsibility and duty of care for supply-side actors, for instance by promoting security-by-default. To take into account complexity, there is a need to address digital security with proportionality, through a risk-based approach. In fact, digital security requirements that may be necessary or effective for one market or product category may not be appropriate for another. Increasing co-operation, and enabling more innovation and competition, is also important to enhance the digital security of products.

The principles are based on emerging best practices across OECD countries. They can serve as building blocks or areas of focus for the design of public policies and strategies aiming to enhance the digital security of products, and as references for stakeholders involved in managing the digital security of products. Figure 3.1 provides an overview of the high-level principles.

Figure 3.1. Overview of the high-level principles


Traceability
Accountability
Transparency and information sharing
Proportionality and risk management
Awareness and empowerment
Enhancing digital security of products
Innovation and competition
Responsibility and duty of care
Co-operation and governance
Across code owners
Multi-stakeholder
Whole-of-government
International
Security-by-design
Security-by-default
Responsible End-of-Life policies

Source: OECD.

The high-level principles should be considered as interdependent and their effects as cumulative. For instance, the positive effects of increased product transparency will be amplified if markets are innovative and competitive enough to provide for meaningful consumer choice. Similarly, stakeholders will be incentivised to act responsibly if there is effective co-operation and clear governance across the product's value chain.

Importantly, the high-level principles focus on "what" should be promoted, rather than on "how" to promote their adoption in practice. In fact, the most appropriate tools to foster the adoption of the high-level principles are likely to vary across product categories and markets, which may face different challenges and constraints. Similarly, each government may be inclined to rely on those policy tools that are more consistent with its culture, history and style of government. The policy tools that can be used to foster the adoption of the principles are further discussed in chapter 4.

The high-level principles build on the principles of the 2015 Recommendation (Box 3.1). They also complement other relevant OECD standards in areas such as responsible business conduct (OECD, 2018[14]), artificial intelligence (OECD, 2019[15]) and consumer product safety (OECD, 2020[16]).

Box 3.1. Principles of the OECD Recommendation on Digital Security Risk Management

1. ***Awareness, skills and empowerment.*** All stakeholders should understand digital security risk and how to manage it.

2. ***Responsibility.*** All stakeholders should take responsibility for the management of digital security risk.

3. ***Human rights and fundamental values.*** All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.

4. ***Co-operation.*** All stakeholders should co-operate, including across borders.

5. ***Risk assessment and treatment cycle.*** Leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment.

6. ***Security measures.*** Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.

7. ***Innovation.*** Leaders and decision makers should ensure that innovation is considered.

8. ***Preparedness and continuity.*** Leaders and decision makers should ensure that a preparedness and continuity plan is adopted.

Source: (OECD, 2015[5]), https://oe.cd/dsrm

3.1. Transparency and information sharing

Increasing transparency and information sharing is key to reduce information asymmetries and increase trust. It can also enable stakeholders to better perceive risks and clarify responsibility. For governments, policy tools to increase transparency include labels, awareness-raising campaigns, certification, conformity assessments and *ex ante* requirements (see chapter 4).

Transparency can be defined as a situation in which relevant information is made available to all stakeholders in a standardised format, which allows for common understanding, accessibility, clarity and comparison. Alternatively, information sharing can be defined as a more tailored mechanism, which allows a limited group of stakeholders to share information. To be effective, it requires building trust between partners (e.g. business partners such as suppliers and manufacturers, or between a company and a governmental digital security agency).

The *Digital Security Risk Management Recommendation* (OECD, 2015[17]) states that "all stakeholders should understand digital security risk and how to manage it" and "take responsibility for the management of digital security risk". In the context of smart products, transparency can be considered as a condition to achieve awareness and empowerment, and to enable the application of the responsibility principle.

Increasing transparency and information sharing can improve product comparability, traceability and accountability. Traceability refers to a situation where there is clarity about the product's components and the actors involved in its value chain. Accountability refers to a situation where supply-side actors' processes and policies can be verified by other stakeholders. To increase transparency and information sharing, the following questions are important:

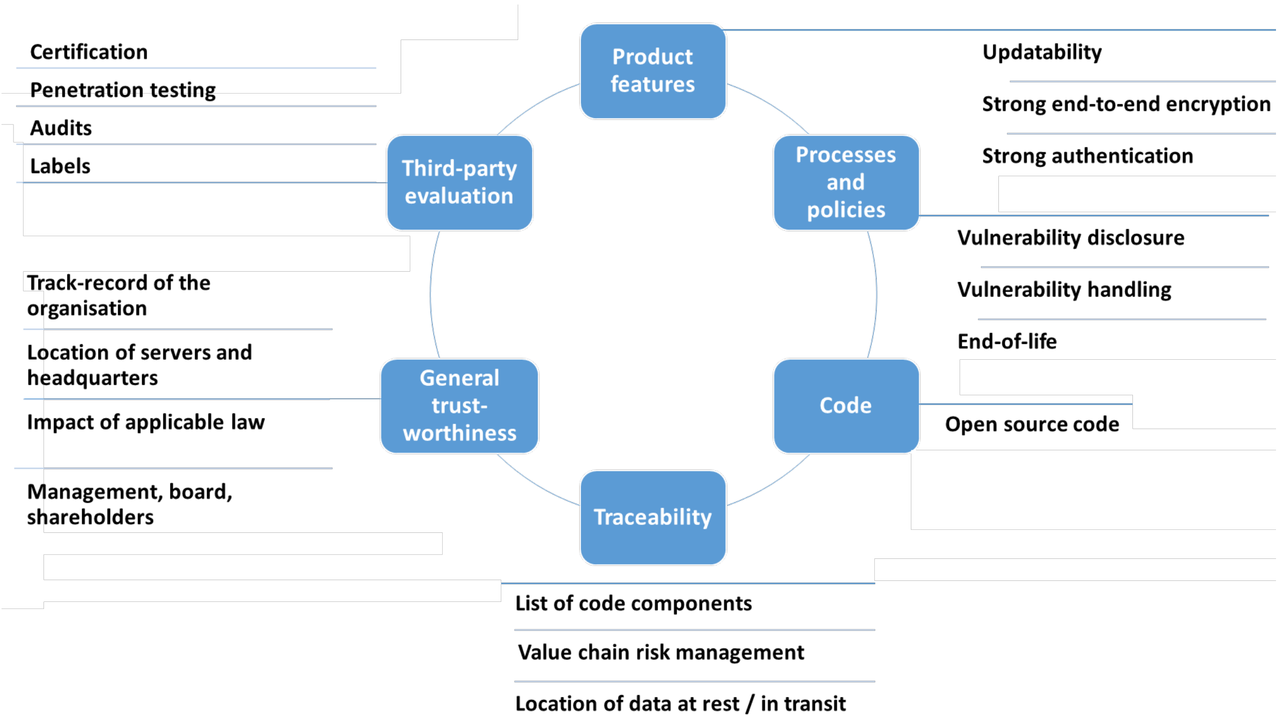
- What information could be made available?
- To whom and how?
- Is the information trustworthy?

3.1.1. What information could be made available?

Figure 3.2 provides an overview of six key areas where more transparency may be needed to reduce information asymmetries and enable customers to make more informed risk-based decisions:

- Product features for digital security, e.g. updatability and strong authentication.
- Processes and policies that are put in place by supply-side actors (e.g. EOL).
- The product's code: is the source-code open? Has it been scanned and tested by third-parties such as certification companies or governmental agencies?
- Traceability: is there is a list of code components? Is there enough clarity regarding the product's value chain? Where is the data stored and where does it transit?
- General trustworthiness: this area does not focus on the product itself, but rather on its broader ecosystem. What is the track-record of the organisation for managing digital security? Where are the servers, development teams and headquarters of the supply-side actors located? What is the impact of applicable domestic law (e.g. privacy, access to data, etc.)?
- Finally, third-party evaluation is key to increase transparency, and connects with the other five areas. For instance, certification can rely on assessing the level of digital security provided by the product's features, the producer's policies and processes and the product's code. Alternatively, a label could increase a product's general trustworthiness.

Figure 3.2. Potential areas of focus for product transparency and information sharing



Note: Examples are provided only for illustrative purposes, and do not aim to be exhaustive or applicable to each product category and context.
Source: OECD.

These areas of focus may also be used as building blocks for standards, certification and labelling schemes. For instance, recently adopted standards in the field of IoT have focused on product features, processes and policies, or “activities” (NIST, 2020[18]; ETSI, 2020[19]). The digital security labelling scheme developed in Finland includes, amongst other criteria, the fact that the product has been certified by a third-party (see section 4.7).

3.1.2. To whom and how should the information be made available?

Depending on the context and product category, it may be more suitable to make the information available to the general public (transparency) or to trusted partners only (information sharing). In addition, the tools used to increase transparency and information sharing need to take into account different levels of understanding and knowledge, based on the category of users they target. For instance, access to source code and conformity assessment for technical standards may be appropriate to reduce information asymmetries between advanced users and supply-side actors (see section 4.6). However, mainstream users may need a more accessible format, e.g. through labels (see section 4.7). Effective transparency measures could rely on a multi-layered approach, which would communicate easily accessible information to mainstream users (e.g. a graded-scheme label) while enabling advanced users to access more technical information (e.g. by scanning QR codes on the product).

Importantly, transparency measures should be proportionate (see section 3.6). If too much information is provided, or the information is not provided in an accessible format, such measures could easily lead to consumer fatigue while not being effective at reducing information asymmetries. For instance, there is a debate regarding the effectiveness of certain transparency measures that aimed to empower users to better manage their privacy online. In the wake of the privacy laws passed in the last decade (e.g. GDPR), there has been a proliferation of pop-up windows notifying consumers of the need to consent to the use of cookies or to the service provider's privacy policies. Recent research questions the effectiveness of such measures, as a majority of mainstream users seem to not read privacy policies thoroughly, accept the use of cookies almost automatically and consider pop-up windows mostly as annoyance rather than as an effective protection measure (Lomas, 2019[20]) (Litman-Navarro, 2019[21]) (Fowler, 2020[22]). This shows that it may not be effective to require supply-side actors to be more transparent about their policies, if the information provided does not enable meaningful consumer choice and comparison between products and organisations.

The COVID-19 pandemic provided another example of the difficulty to increase transparency in an effective manner. During the crisis, many organisations massively switched to teleworking and relied on teleconferencing tools to ensure business continuity. This provided a large-scale example of how information asymmetries often limit the ability of stakeholders, in particular consumers, SMEs and less digitally mature organisations, to make informed and risk-based decisions regarding the selection and use of a smart product. In fact, in the absence of labels or certifications, it was difficult to assess and compare the level of digital security of teleconferencing tools. In addition, there has been a debate on the trustworthiness of the information shared by supply-side actors (Hay Newman, 2020[23]), as self-assessment would often not match the certainty that could be provided by certification, i.e. third-party evaluation. As a result, the choice of the product often relied on other factors than digital security, such as a functionality and usability.

Various stakeholders (e.g. civil society and governments) published guidelines to assist organisations to choose the right teleconferencing tool for their specific needs and context. However, many of these guidelines focused on product features (Mozilla Foundation, 2020[24]) for digital security (e.g., end-to-end encryption) and, to a lesser extent, on the processes and policies of the supply-side actor. Other guidelines recognised the need for a broader perspective, to take into account, for instance, the product's source code or the jurisdictions the product may be subject to (e.g. where it has been developed, where the headquarters and servers are located, etc.). (Baksh, 2020[25]) An important aspect missing in many of these guidelines was the need for organisations to rely on a risk management approach. Such approach requires developing a clear risk management governance framework, defining baseline requirements for products' trustworthiness, and going through a thorough assessment of the organisation's legal environment, threat landscape, business needs and use cases.

This example shows that increasing transparency alone would not address the challenges discussed in chapter 2, and that raising awareness, ensuring responsibility, facilitating co-operation and supporting innovation and competition are key to enhance the digital security of products.

3.1.3. Is the information trustworthy?

In many cases, information on the key areas described in Figure 3.2 is unavailable. Even when supply-side actors provide such information, it is difficult for customers to trust it, in the absence of other mechanisms such as certification, conformity assessments, labels and *ex post* mechanisms (chapter 4).

Furthermore, in many OECD countries, privacy regulations require data processors to notify the data subjects and the relevant authorities about personal data breaches, under certain circumstances (e.g. depending on the extent of the breach). Similarly, regulations could require supply-side actors to notify customers and relevant authorities in case significant vulnerabilities are discovered in their products. Documentation on vulnerabilities and on the deployment of patches would likely enable stakeholders to enhance the overall level of digital security of products in the long term. In the United States, a report recently noted the need to enable the government to "systemically collect cyber incident information reliably and at the scale necessary to inform situational awareness", and recommended to require "critical infrastructures entities to report cyber incidents to the federal government" (Cyberspace Solarium Commission, 2020[12]). In the European Union, similar requirements are already in place since the adoption of the directive on the security of networks and information systems (NIS) in 2016 (EU, 2016[26]).

Without *ex ante* requirements and *ex post* mechanisms, there are little incentives for supply-side actors to be more transparent and to be held accountable on its trustworthiness (see section 2.1.2 and chapter 4).

3.2. Awareness and empowerment

Enabling stakeholders to be more aware and empowered is key to reduce information asymmetries and realign market incentives. Stakeholders that are more aware and empowered are also more likely to better perceive risk. For governments, policy tools to enable stakeholders to be aware and empowered include awareness-raising campaigns, education programs, multi-stakeholder partnerships, conformity assessments and labels.

"All stakeholders should understand digital security risk and how to manage it" (OECD, 2015[17]). For the digital security of products, customers in particular need to be made more aware of the risk and empowered to make more informed decisions. In this context, at least two categories of customers could be distinguished: "mainstream users" and "advanced users" (concepts introduced in the in-depth analysis report (OECD, 2021[2])) while recognising that many products could be used by both categories.

3.2.1. Empowering mainstream users

"Mainstream users" include consumers and some corporate users like SMEs. They may have limited skills and knowledge about digital security, and therefore may not have the ability to accurately identify and manage digital security risk.

Mainstream users need to be made more aware of the digital security risk associated with the products they purchase. They should be able to assess whether products meet certain digital security criteria (e.g. adherence to industry best practices, length of commercial support, etc.), for instance through labels and clear statements by the relevant supply-side actors (e.g. the product manufacturer). Labels can be developed by or with the industry, and could take into account various categories of information (e.g. traceability for the product's components, digital security policies, adherence to standards, etc.). Public policies need to incentivise stakeholders to provide mainstream users with clear and easily accessible information about a product, in order to allow for comparability and informed choices. The opportunities and challenges associated with labels are further discussed in chapter 4 of this report.

In addition, educating mainstream users about basic digital security "hygiene" is key. In fact, phishing and other techniques relying on user interaction are amongst the most common attack vectors (Verizon, 2019[27]). Governments, as well as supply-side actors and civil society, can play a role in enhancing digital security risk education for mainstream users, for instance through awareness-raising campaigns, the development of content and guidelines, and by supporting educational programs.

Beyond awareness raising, there is also a need to support the development of skills for SMEs and less digitally mature companies, for instance through capacity building and training programs. In particular, mainstreaming risk management approaches amongst these organisations can prove effective to enhance their overall level of digital security. From a development co-operation perspective, such capacity building measures could also usefully address the needs of low-income cities, regions and countries.

However, most mainstream users should not be expected to develop advanced digital security skills. While raising the awareness of mainstream users is important, it should not be considered as a way to lift supply-side actors' responsibility and duty of care. Products could be designed[4] so that mainstream users have as little responsibility as possible for the management of digital security. For instance, to the extent possible, security updates should be automatic.

Beyond awareness raising and developing skills, effective consumer protection is key to empower mainstream users. Principles to ensure effective consumer protection include, inter alia (OECD, 2016[28]; OECD, 2007[29]; OECD, 2020[16]; OECD, 2012[30]; UN, 2016[31]):

- Fair and equitable treatment;
- Disclosure and transparency;
- Protection of privacy;
- Dispute resolution mechanisms;
- Protecting vulnerable and disadvantaged consumers;
- Protecting consumers from hazards to their health and safety;
- Protecting the economic interests of consumers.

3.2.2. Empowering advanced users

"Advanced" users are typically more aware and able to manage digital security risk associated with smart products than mainstream users. This category of more experienced and autonomous users is heterogeneous, ranging from "geeks" and tech savvy hobbyists to users in professional environments, and trained security experts. Advanced users could be empowered to adjust the level of digital security of the smart products they use, based on their own risk assessment, in particular by being able to:

- Access and modify security settings;
- Test or reverse engineer a product if the source code is not open (analyse "what is in the box"). The conditions for such practices can be specified in the terms of use or within policies developed by the producer, in order to bring more legal certainty for the individual or organisation performing the test or reverse engineering;
- Opt out from security defaults such as automatic updates, and test security updates before deployment;
- Examine "telemetry" data, or metadata about usage and access to detect anomalies (ETSI, 2019[32]). For instance, access a login history to identify unauthorised access.

Ultimately, empowering advanced users can contribute to raising awareness for mainstream users. For instance, on the basis of raw information (e.g. a list of a product's components, or the product's source code), advanced users could also develop their own labels and make them available to the public (e.g. through barcode scanning applications).

3.3. Responsibility and duty of care

Ensuring responsibility and duty of care is key to realign market incentives towards optimal outcomes and better allocate responsibility. For governments, policy tools to ensure responsibility and duty of care include *ex ante* requirements, certification, conformity assessments, *ex post* mechanisms and public procurement.

3.3.1. A shared responsibility: the need for more ownership of digital security risk.

"All stakeholders should take responsibility for the management of digital security risk" (OECD, 2015[5]). In fact, no single stakeholder can be held entirely responsible for the digital security of products.

As noted in section 3.2, there is an important role for users in managing digital security risk, as they are ultimately the most knowledgeable about the context of use of smart products. In the United States, a report recently estimated that a third of all breaches still stem from a malign actor's success in persuading individuals to open phishing emails" (Cyberspace Solarium Commission, 2020[12]), confirming that individuals are "important guarantors of collective cybersecurity". While acknowledging the important role of users, the same report recognised the need for supply-side actors "to develop security frameworks that do not overburden end users" (Cyberspace Solarium Commission, 2020[12]).

To enable stakeholders to take ownership, there is a need to make them more aware and empowered, for instance through education (see section 3.2), to increase co-operation and to clarify their roles (see section 3.4). Guidance and standards (see section 4.5) can help to define which stakeholder is responsible for which security control. Ensuring the effectiveness of *ex post* mechanisms (e.g. insurance and liability law, see section 4.8) is also key in incentivising stakeholders to take responsibility.

3.3.2. The duty of care of supply-side actors

However, the level of responsibility is not the same for all stakeholders, and depends on "their roles, ability to act and the context" (OECD, 2015[17]). In the context of smart products, supply-side actors (vendors and manufacturers), as they put products on the market and benefit from their sale (EU Expert Group on Liability and New Technologies, 2019[33]), have a specific responsibility, which can be referred to as a "duty of care". This duty of care can:

- Be oriented towards other stakeholders: to the extent possible, supply-side actors should be responsible for managing the digital security of their products. They should not shift their responsibility towards other stakeholders, in particular mainstream users.
- Cover the product's lifecycle. The smart products put on the market should be developed and designed in accordance with relevant recognised standards. Supply-side actors should timely and effectively manage the digital security vulnerabilities in their products during their commercial life, and implement a responsible EOL policy.

While there is broad agreement on the need to realign market incentives for supply-side actors, it can be difficult to precisely attribute responsibility for digital security gaps. As underlined in chapter 2, value chains of smart products are often global, complex and opaque. The discovery of the Spectre and Meltdown vulnerabilities in 2018 showed how vulnerabilities in components may affect a wide range of final products. The vendors of these final products may not always be the best placed to provide fixes, if they are not responsible for the vulnerable layer of code. As discussed in the in-depth analysis report (OECD, 2021[2]), the concept of "code owners" could facilitate the identification of the responsible parties and bring clarity regarding the allocation of responsibility. Ideally, for each smart product, there should be a list of code components and a clear allocation of responsibility for each code owner. Therefore, to ensure the responsibility of supply-side actors, it is also key to increase transparency regarding the product's components (i.e. traceability) and to reinforce co-operation across code owners.

The duty of care should be proportionate to the context and stakeholders' ability to act, in particular in relation with other code owners. The principle of duty of care can be broken down in five sub-principles: security-by-design, security-by-default, dynamic management of digital security, responsible EOL policies and the digital security of the organisation. Assessing the effectiveness of the duty of care can be done through various means, depending on the risk level. For instance, the conformity of a product's design for lower risk categories could be done through self-assessment, while certification could be mandatory for higher risk categories (see chapter 4).

Security-by-design

At a high level, security-by-design could be defined as the principle and the practice of developing products with digital security in mind. Supply-side actors have a responsibility to build and sell products that meet minimum security requirements. Security-by-design requirements usually rely on both product features (e.g. an update mechanism) and processes and policies developed by supply-side actors (e.g. a vulnerability disclosure policy). To achieve security-by-design, supply-side actors have to:

- Integrate digital security at every stage of the product's development, starting from its design and ending with its release, as opposed to adjusting or adding security features afterwards.
- Adopt a risk-based approach and assess how their products may pose digital security risk to their end-users, e.g. with use-case scenarios, threat modelling and penetration testing.
- Define security requirements and metrics in accordance with the findings of the risk assessment.
- Take into account the "state of the art"[5] to make sure their products do not pose unreasonable risks for their end-users. To do so, they should follow security-by-design methodologies (Box 3.2).

Box 3.2. Security-by-design methodologies

Security-by-design methodologies are usually available as industry standards or guidelines, e.g. Microsoft' Security Development Lifecycle (SDL), SAFECode's Fundamental Practices for Secure Software Development, the Open Web Application Security Project (OWASP) or ISO/IEC 27034 series for application security. At a high-level, the following principles are key to ensure security-by-design:

- Ensuring the product's updatability;
- Defining security requirements and metrics;
- Modelling threats;
- Scanning for common and known vulnerabilities;
- Designing strong access control measures (e.g. identity management and authentication);
- Following the "least privilege" principle, which requires that any module or user should be able to access only the resources necessary for legitimate purposes;
- Designing and implementing audit mechanisms and penetration testing;
- Minimising the attack surface;
- Ensuring data protection;
- Ensuring resilience in case of attacks or outages;
- Following the "defense in depth" principle, i.e. designing several layers of security measures;
- Encrypted communication with other products, e.g. using Transport Layer Security (TLS) protocols.

DevOps (for Development & Operations) is another important concept in code development. It can be defined as an application development philosophy focused on the automation of development and deployment (Cloud security alliance, 2017[34]) through an agile framework.

DevSecOps (for Development, Security & Operations) is an emerging code development good practice that focuses on integrating security practices within the DevOps process. DevSecOps considers security as a shared responsibility and promotes a 'Security as Code' culture with ongoing, flexible collaboration between engineering teams and security teams. The goal of DevSecOps is to bridge traditional gaps between IT and security teams while ensuring fast, safe delivery of code. In particular, the following elements are key in DevSecOps:

- Code analysis – delivering code in small chunks so vulnerabilities can be identified quickly;
- Change management – allowing anyone to submit changes, followed by review;
- Compliance monitoring – ongoing compliance audits;
- Threat investigation – identifying potential emerging threats with each code update;
- Vulnerability assessment – identifying new vulnerabilities, analysing how quickly they are patched;
- Security training – training software and IT engineers with guidelines for set routines.

Security-by-default

At a high level, security-by-default is a situation where supply-side actors take an appropriate level of responsibility for managing the digital security of their products, and do not shift this responsibility to end-users. The ultimate objective of this principle would be to make it easy for end-users to do the right thing, hard to do the wrong thing and almost impossible to do the catastrophic thing.

In a security-by-default approach, supply-side actors circulate products with default values that provide appropriate security, and rely as little as possible on end-users to manage the digital security gaps of their products. In particular, supply-side actors:

- Pre-configure and activate security features by default, as opposed to an "opt-in" approach. For instance, a messaging application would automatically encrypt communications, instead of letting users choose to activate or deactivate this option. Connected devices would require end-users to set strong passwords at first use, as opposed to letting them keep the default password indefinitely. Multi-Factor Authentication (MFA), which requires the use of more than one authentication method, could also be integrated as a default setting on smart products, as recent research suggests that it could "prevent 96% of bulk phishing attacks" (Cyberspace Solarium Commission, 2020[12]). The European Standard adopted by ETSI (2020[19]) also recommends the use of MFA to increase digital security for consumer IoT products.
- Provide a comprehensive yet simple security configuration guide that employs minimal steps and follows security best practices on usability. Support could be available on demand to assist end-users in configuring their products.
- Provide users with free and automatic security updates during the product's commercial life, distinguished from other functionality updates. Advanced users could choose to opt out from automatic updates and test them before deployment. In case of automatic updates, users should be notified of the deployment.

Importantly, the principle of security-by-default should be applied differently for each category of users. Advanced users should have the possibility to opt out from secured defaults if they wish, e.g. to test the updates before implementation, have more control on the process and decide on other digital security settings according to their own risk assessment.

Finally, as noted in section 3.3.1, there is a need for stakeholders to clarify roles and responsibilities for supply-side actors and users. Responsible supply-side actors need to communicate such information to their customers in an effective manner, for instance through the use of a responsibility control matrix

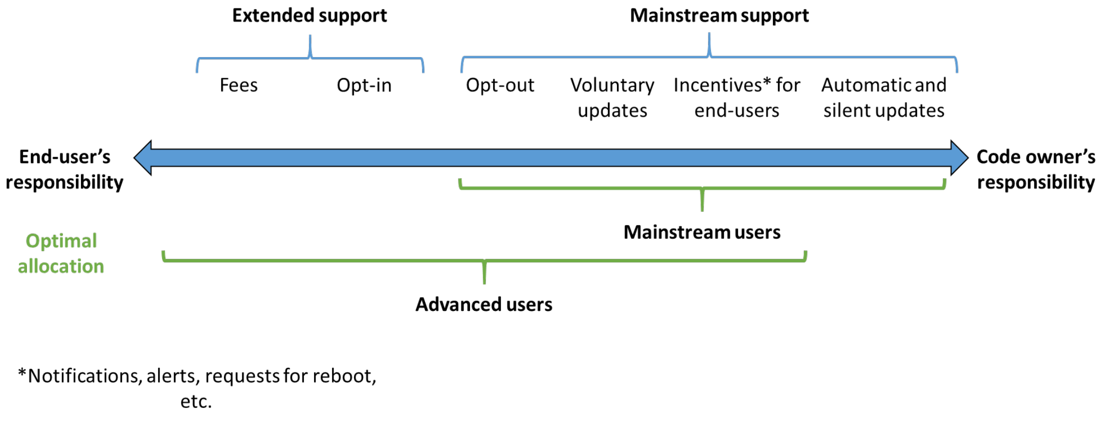
Dynamic management of digital security

Supply-side actors and other code owners have a duty of care to maintain the digital security of the products they put on the market throughout their commercial life. In particular, they need to:

- Continually monitor for, identify and mitigate security vulnerabilities in their products during their commercial life.[6] If the vulnerabilities are managed by another code owner, they should notify the party best placed to mitigate them.
- Adopt a clear and public co-ordinated vulnerability disclosure policy, which indicates a public point of contact so that researchers can report vulnerabilities.
- Adopt a vulnerability handling process and prioritise vulnerabilities through a risk-based approach.
- Incentivise third-parties such as security researchers to identify and disclose security vulnerabilities in their products.
- Communicate with customers about security updates and risk related to newly discovered vulnerabilities.
- Develop and distribute timely updates, on a regular or *ad hoc* basis. Typical update cycles range from seven to ninety days, though this may vary greatly depending on the nature of the product. This should be balanced with the need, in some cases, to test and deploy security updates progressively.
- Separate security updates from functional updates, or upgrades (ETSI, 2020[19]).
- For mainstream users, provide automatic and free security updates (ETSI, 2020[19]).

- Consider the need to make security updates for critical vulnerabilities automatic for all users.
- Enable advanced users to opt out from automatic updates (for non-critical vulnerabilities), as they may value privacy and control (e.g. in complex industrial environments that may be disrupted by automatic patching). Figure 3.3 provides an example of possible update practices based on user categories.

Figure 3.3. Better allocating responsibility according to categories of end-users


Extended support
Mainstream support
Fees
Opt-in
Opt-out
Voluntary updates
Incentives* for end-users
Automatic and silent updates
End-user's responsibility
Code owner's responsibility
Optimal allocation
Mainstream users
Advanced users
*Notifications, alerts, requests for reboot, etc.

Source: OECD

Importantly, the dynamic management of digital security should be holistic, and take into account all components of the product's ecosystem.

Other aspects regarding the effective treatment of vulnerabilities, including for their discovery, disclosure, handling and management, are further discussed in the vulnerability treatment report **Invalid source specified.**.

Responsible EOL policies

Supply-side actors have a duty of care to maintain the digital security of the products for a reasonable period corresponding to the expected length of use of the product, and ensure their repairability (i.e. the ability for third-parties to maintain a product).

The first section below proposes universal basic rules that could apply to all smart products. The following sections explore possible options to manage the EOL gap. Each option may be more suitable for certain categories of products or within specific contexts. However, there is a need for supply-side actors to choose at least one of these options to address the EOL gap effectively. Therefore, in line with the proportionality principle (section 3.6), a gradual approach could be followed. For instance, supply-side actors could be incentivised to provide extended support for a fee, or to enable users to upgrade for free or for a discount. In case they do not, then they could be compelled to enable other stakeholders to be responsible to maintain the product, for instance by transferring intellectual property rights and design information to the user or open-source community. Such gradual approach could also benefit from analysing the specific dynamics and negotiating power within each market: in case there is a lack of interoperability or competition, more compelling policies could be put in place (see section 3.5).

Reasonable and transparent length of support

There is a need for supply side-actors to ensure a reasonable and transparent length of support, to the extent possible, by:

- Designing and implementing a clear and transparent EOL policy for their products.
- Publicly stating the minimum length of time for which a product will receive software updates, the reasons for the duration of the support period and the envisioned EOL period.
- Determining the EOL on the basis of the date of end-of-sale (EOS, last purchase through official vendors) as opposed to the date of general availability, allowing for a reasonable time period between EOS and EOL.

Duty of care after the EOL

Supply-side actors could ensure duty of care after the EOL by:

- Monitoring the use of their products after their EOL and provide, upon request, relevant data to the regulator (e.g. number of products still in use after EOL).
- Under certain circumstances, continuing to ensure duty of care after EOL. If critical vulnerabilities are discovered in EOL products that are still widely in use and are likely to pose unreasonable risk for end-users[7] in case of exploitation, including safety risk, supply-side actors would have a duty of care to either *i)* provide security updates or fixes or *ii)* enable other stakeholders to mitigate these risks (see below). This principle could be applied only to certain products, e.g. entailing “systemic” risks (see Annexes).
- Under certain circumstances, terminating or disconnecting products when they reach their EOL.[8] However, this would come with significant downsides in terms of consumer rights, fair business practices and e-waste generation. In the United States, several States introduced draft laws banning the use of such “kill-switches” as unsafe and unfair business practices. (Povich, 2018[35]) This solution seems also dangerous regarding liability, and does not address the power asymmetry between supply and demand.

Repairability

Supply-side actors should not be expected to maintain the digital security of their products indefinitely. However, these reasonable limitations to their duty of care should not prevent other stakeholders from taking over this responsibility. As a result, when a product has reached its EOL, supply-side actors could put in place, for example, one of the following strategies:

- Incentivise end-users to stop using a product when it reaches the end of its commercial life, for instance through EOL notifications, and discounted or free upgrades.
- Enable third-parties (e.g. advanced users or the open source community) to maintain the product, for instance through source code escrow[9] or transferring proprietary design information and rights, including credentials for security updates, directly to trusted stakeholders (Zittrain, 2018[36]; NIST, 2016[37]).

The repairability principle should also be considered in relation to the environmental impact of EOL products. Digital security should be balanced with other important policy objectives, such as the need to reduce e-waste (see SDG 12). Repairability can also be approached as a means to ensure resilience, as defined in section 3.3.2. In the United States, several States have introduced some draft laws promoting a “right to repair” for smart products have been introduced (Gartenberg, 2018[38]).

Digital security of the organisation

The duty of care of supply-side actors for the digital security of the products they put on the market should be approached holistically.

Beyond the digital security of the product, there is a need to ensure the digital security of the organisations that are part of the product’s value chain. Even though a product meets security-by-design and security-by-default requirements, it may be compromised through the networks of the manufacturer or of other code owners. The NotPetya malware in 2017 showed how update mechanisms could be compromised to insert malware in products. This is particularly relevant if parts of the product are managed in the cloud, such as the backend of an IoT device.

Therefore, supply-side actors need to adopt strategies to ensure they meet a satisfactory level of digital security for their organisations. These actors could be incentivised to follow international standards such as ISO 31000. Adherence to such standards can be demonstrated by conformity assessments and certifications (see section 4.5).

3.4. Co-operation and governance

Increasing co-operation and developing effective governance are key to better allocate responsibility and realign market incentives.

For governments, policy tools to increase co-operation include multi-stakeholder partnerships, *ex ante* requirements and *ex post* mechanisms.

To manage digital security risk, all stakeholders should co-operate, including across borders (OECD, 2015[5]). For the digital security of products, four areas of focus are important to increase co-operation in an effective manner:

- Between code owners across the product’s value chain;
- Between stakeholder groups and across sectors;
- Between regulators and across the whole government;
- At the international level.

3.4.1. Increasing co-operation amongst code owners across the value chain

The value chain of smart products is often complex. Smart products are usually made of multiple components and various code layers, which can be developed by a wide range of actors, from open source communities and independent developers to corporations, including both digitally mature companies and SMEs that may have limited technical resources. In addition, smart products are usually part of a wider ecosystem, which involves many actors such as network operators, cloud providers and large ICT companies.

Vulnerabilities in any code layer, any component and any part of a product’s ecosystem can affect its digital security. Consequently, co-operation across code owners is key to enhance the effectiveness of identifying and mitigating digital security gaps.

Clear allocation of responsibility for each component and code layer of the product is necessary. Technical and organisational measures should be in place to facilitate co-operation between code owners (e.g. security bulletins, procurement guidelines throughout the value chain).

In the context of industrial IoT, trustworthiness, i.e. the ability of suppliers to meet the expectations of a contract partner in a verifiable way, is key to increase co-operation of stakeholders across the value chain. To build trustworthiness, there may be a need to implement new technical tools (e.g. unique digital identities for processes, products and organisations) and incentivise the use of digital certificates and certification / conformity assessments (PI4.0 & RRI, 2020[39]).

For each product, an institutionalised coordinator could facilitate the identification of code owners and their co-operation. Depending on the context and the product, the coordinator may be the vendor, the manufacturer, a third-party (e.g. the network operator or the operating system designer) or a government agency.

3.4.2. Multi-stakeholder co-operation

Co-operation should also involve actors within the broader ecosystem. In particular, co-operation mechanisms could include:

- Security researchers, for instance through bug bounties and vulnerability disclosure policies.
- Competitors within the same sector, for instance through information sharing and analysis centres (ISACs) and sector or product-centred Computer Emergency Response Teams (CERTs).
- Stakeholders across sectors, for instance through forums gathering various ISACs and CERTs.
- Other stakeholder groups, such as consumer associations.

Governments should, to the extent possible, consult all relevant stakeholders when they design and implement policy tools aiming to enhance the digital security of products.

3.4.3. Whole-of-government approach

The development of the IoT and other emerging technologies raises challenges that spread across policy silos. More and more, the products that entail safety risks are becoming “smart”. For instance, IoT products are becoming more and more common in healthcare and transportation, while raising concerns regarding safety and privacy. For many smart products, there is increasingly an overlap between sectoral regulators (finance, health, automotive…), horizontal authorities (consumer product safety, competition, data protection…) and authorities in charge of digital security. If not properly anticipated and managed, this may result in inconsistent and potentially contradictory recommendations for the industry, or conflicts between institutions.

To address this issue, it is fundamental that policy makers develop a whole-of-government approach to the digital security of products, and make sure that the development, application and evaluation of the policy response are coherent and involve all relevant public actors. This holistic approach would involve all relevant government agencies, including agencies in charge of horizontal regulations (e.g. privacy, consumer protection) and institutions in charge of sectoral regulations (e.g. health, banking).

3.4.4. International co-operation

Initiatives or rules developed nationally may not be sufficient to have a significant impact on the digital security of products. In fact, the market for smart products is increasingly global, both from a supply-side perspective and from a demand-side perspective. The value chain of smart products often involves many actors from various jurisdictions, and supply-side actors often circulate their products across many countries. The case of botnets further exemplifies the need for more international co-operation to address digital security vulnerabilities in globally used products, as the targets of DDoS attacks and the infected computers enrolled in botnets are often located in different countries.

In the United States, a report recently highlighted the need to design and enforce “a system of norms, built through international engagement and cooperation”, for instance through “a coalition of like-minded allies and partners willing to collectively support a rules-based international order in cyberspace” (Cyberspace Solarium Commission, 2020[12]). International cooperation may also be needed to facilitate the identification of and information sharing regarding vulnerabilities[10] in smart products, as well for the status of security updates for products that are widely used globally.

From the industry's perspective, the fragmentation of regulatory requirements across OECD countries also represents a significant challenge. The need to assess the conformity of products with many guidelines and standards, in particular through third-party certification, incurs significant costs.

Consequently, policy makers should seek to increase international co-operation and agree on common terminology and strategies where applicable. Another important aspect to take into consideration is the importance of interoperability between legal frameworks (see section 4.8).

3.5. Innovation and competition

Promoting innovation and competition is key to realign market incentives towards optimal outcomes and enhance the overall level of digital security for smart products.

For governments, policy tools to promote innovation and competition include research and development, *ex ante* requirements, labels, *ex post* mechanisms and public procurement. Other tools can also be used, but they go beyond the scope of this report (e.g. competition law).

3.5.1. Digital security and innovation

According to the *Digital Security Risk Management Recommendation,* "leaders and decision makers should ensure that innovation is considered" (OECD, 2015[17]). The relationship between innovation and digital security is complex (OECD, 2020[40]). Innovation is key to develop new architectures and technical standards that are likely to raise the level of digital security of products. In the same time, market incentives often lead innovators to favor time-to-market and usability over digital security concerns. Unnecessary and disproportionate digital security requirements (e.g. legacy regulations) may also be considered as a barrier to innovation and may limit the ability of stakeholders to fully reap the benefits of digital transformation (see section 3.6).

Promoting innovation entails recognising that product development is an iterative process. Innovation goes hand in hand with a certain tolerance to mistakes and failures. However, these mistakes and failures can only be tolerated within a certain framework. They should be addressed in a timely manner, responded to, and enable stakeholders to learn and improve.

For policy makers, the challenge is to strike the right balance between:

- Ensuring a duty of care for supply-side actors, in order to protect mainstream users from unreasonable risks;
- Allowing for iterations and mistakes, which are an inherent part of innovation.

To overcome this challenge, it is essential to define clear responsibilities, and allow for a lift of responsibility (or "safe harbour") only in a specific context. Regulatory sandboxes are an example of policies enabling innovation in a responsible manner (OECD, 2020[41]). For product developers, leveraging communities of early adopters and advanced users to test and improve products can also be a key element in order to balance innovation with responsibility.

Importantly, recognising the importance of iterations should not be understood as a dismissal of the importance of security-by-design and security-by-default guidelines. To the contrary, the innovation principle also highlights the need for supply-side actors to develop their products with effective and up-to-date technical means. Their digital security measures should take into account the "state of the art".

3.5.2. Digital security and competition

In the context of smart products, competition is also a key element that could enable stakeholders to choose from a wide range of products and select the products that are the most appropriate, according to the context and their preferences.

A suboptimal level of competition in a given market may generate an asymmetry of powers between stakeholders. The lack of substitutability of certain smart products may limit the negotiating power of customers, and lead to unfair business practices (e.g. regarding the EOL, see section 3.3).

Therefore, the assessment of the level of competition in a given market is key to determine the level of regulatory requirements to enhance the digital security of products. In line with the proportionality principle, policy makers could follow a gradual approach. They could encourage voluntary frameworks if the level of competition is high, and consider developing requirements that are more stringent if the level of competition is low, and if business practices do not lead to satisfactory results regarding the duty of care of supply-side actors.

3.6. Proportionality and risk management

Proportionality and risk-based approaches are key to take into account the complexity of smart products (see section 2.1.1) and ensure that technical and policy measures to increase digital security are adapted to the context (e.g. product category, use-case, threats…).

Although digital security measures aim to protect economic and social activities, they can also inhibit them by increasing costs, reducing performance and altering the open and dynamic nature of the digital environment, which is essential to realising the full benefits of digital transformation. Therefore, it is key to determine if digital security measures, and policy tools aiming to enhance digital security, are proportionate.

The *Digital Security Risk Management Recommendation* (OECD, 2015[17]) states that stakeholders "should ensure that digital security risk is treated on the basis of continuous risk assessment". More broadly, a risk-based approach involves evaluating risk on the basis of its probability and severity, based on the context (i.e. risk assessment), and addressing this risk by deciding to accept, mitigate, transfer or avoid it (i.e. risk treatment).

The *Digital Security Risk Management Recommendation* (OECD, 2015[17]) also states that security measures should be "appropriate to and commensurate with the risk", or, in other words, "proportionate". Proportionality can be defined as the principle of balancing the means used with the intended aims. This balancing exercise requires to evaluate the potential benefits of an action as well as their potential negative consequences, usually through impact assessment. Importantly, such evaluation should integrate the negative consequences of inaction[11] and the impact on all relevant stakeholders[12].

The digital security of products is a complex area (see section 2.1.1), which spans across various sectors (or "verticals") and policy areas. In particular, the heterogeneity of smart products and the context-dependence of risk levels make one-size-fits-all approaches unlikely to succeed. Consequently, the use of policy tools should be adapted to each situation, and the responsibility of stakeholders should take into account their ability to act (OECD, 2015[5]).

This complexity, however does not preclude the need for and relevance of baseline requirements for all smart products (e.g. updatability), while recognising the possibility of exceptions[13], and the need for further requirements for specific product categories or contexts of use, e.g. critical activities (OECD, 2019[42]). To implement the proportionality principle in a practical manner, it is therefore important to develop maturity models (NIST, 2018[43]) and tiered or multi-layered approaches, rather than binary models.

The definition of relevant thresholds is complex, and would require co-operation between stakeholders, across the government and at the international level (see section 3.4). Some initiatives are already underway and may provide useful insights on how to define these thresholds, for instance through developing specific requirements for certain sectors or certain categories of products, e.g. with safety risk (see, for instance, the tiered approach for IoT digital security in Japan, outlined in section 4.7.2).

Another important aspect of proportionality is the need for balance. In particular, stakeholders should strive to balance:

- The high-level principles themselves, as they may be conflicting with one another in certain cases, e.g. innovation and duty of care.
- Digital security with other important public policy goals, e.g. the openness of the Internet and emerging technologies, as well as fundamental values such as privacy (OECD, 2015[17]). In that regard, policies to enhance the digital security of smart products shall also ensure that personal data collection and processing meet applicable legal requirements (e.g. purpose limitation, data minimisation, etc.).
- The interests of various stakeholders and communities.

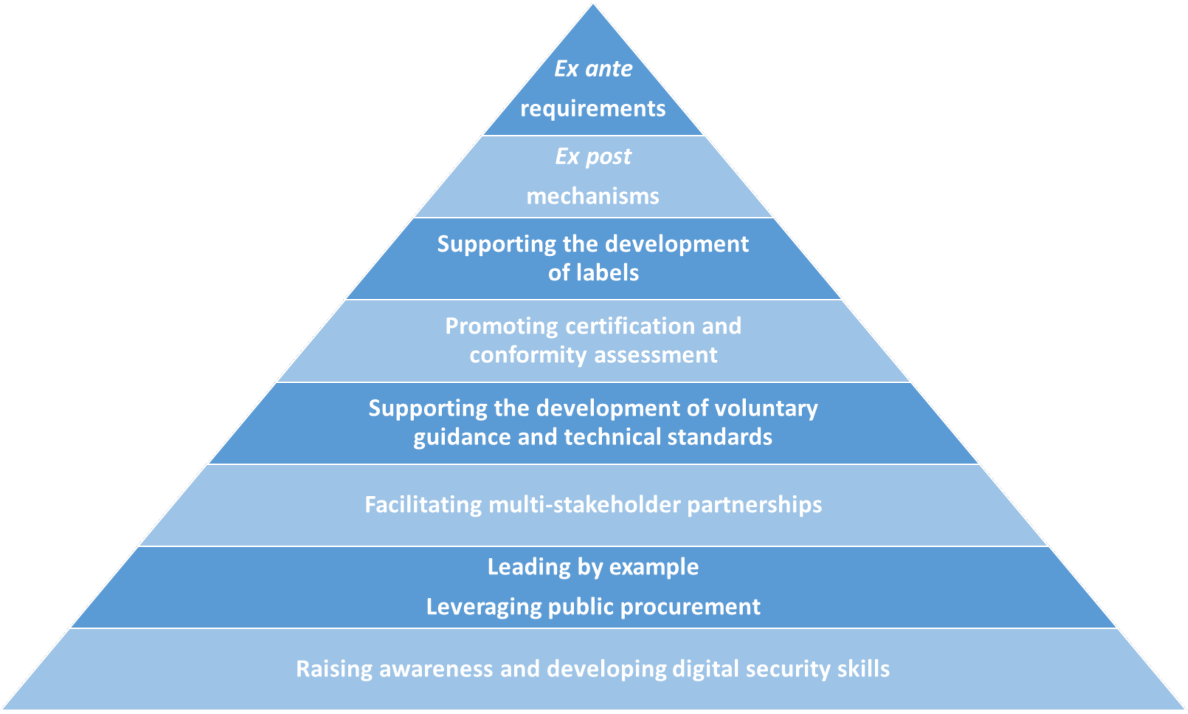
4 Policy toolkit

This chapter explores the broad spectrum of policy options available for governments to enhance the digital security of products. The policy tools described below address the key challenges introduced in chapter 2 and foster the adoption of the high-level principles discussed in chapter 3. While previous chapters focused on "what" needs to be fixed (chapter 2) or promoted (chapter 3), this chapter discusses "how" policy makers can take action.

Policy makers may approach this toolkit as an instrument pyramid (see Figure 4.1). The structure of this pyramid, and of this chapter, invites policymakers to consider a gradual approach to enhancing the digital security of products. In a way, policy makers should approach digital security policy as software engineers approach product development: through an iterative and end-user centric process. Light-touch, voluntary mechanisms, at the bottom of the pyramid, could be implemented as a first step. If those are not successful, or if the industry and consumers – the "end-users" of policies – are not receptive, then the use of more stringent regulatory instruments, such as *ex post* mechanisms and *ex ante* requirements, at the top of the pyramid, could be explored. This gradual approach is further detailed in section 4.1, which discusses the concept of "smart regulation".

Figure 4.1. Overview of the policy toolkit

Smart policies for smart products


Ex ante requirements
Ex post mechanisms
Supporting the development of labels
Promoting certification and conformity assessment
Supporting the development of voluntary guidance and technical standards
Facilitating multi-stakeholder partnerships
Leading by example
Leveraging public procurement
Raising awareness and developing digital security skills

Source: OECD.

Importantly, these tools are not mutually exclusive, and there is no panacea: one single tool alone would not solve all the challenges identified in chapter 2, for all smart products. A strategy to enhance the digital security of products will likely rely on a mix of these policy tools to be most effective.

For instance, the use of voluntary labels for IoT products could be useful to help the most responsible product manufacturers to differentiate their products on the market. However, if used in isolation, their effects may be limited, as consumers are likely assume that all IoT products available on the market meet minimum standards of security. Similarly, resorting solely to *ex ante* requirements, while successfully raising the bar for all products, could lead to a "race to the bottom" where manufacturers would not be incentivised to go beyond the minimum mandatory requirements. Alternatively, the use of both policy tools, as undertaken in Japan, would have a much higher net effect, as it would enforce a minimum level of digital security for all IoT products while also encouraging innovation and competition so that supply-side actors develop more advanced digital security features.

Some governments in OECD countries have favoured so far industry-led approaches. This reflected concerns that government interventions could stifle innovation and competition, or worse, actually lower the level of security, e.g. through laws that would cast in stone requirements that could get outdated quickly, in comparison to fast-adapting industry best practices.

However, significant trends seem to call for more proactive policy developments. These trends include the changing nature of digital security risk (e.g. the evolving threat environment); stronger evidence that a market failure prevents optimal outcomes from emerging; and a growing pressure from various stakeholders such as citizens/end-users, civil society and businesses, to increase the level of digital security of products. In the United States, a report recently recognised that "the status quo is not getting the job done" (Cyberspace Solarium Commission, 2020[12]). Furthermore, the dichotomy of government intervention v. "laissez-faire" is increasingly considered as too simplistic to capture the broad spectrum of options available to policy makers.

Finally, while these tools are often developed at the national level, policy makers should take into consideration the broader international context as well. Some cutting-edge national policy tools have formed the basis of emerging international norms. For instance, the UK's Code of Practice for the digital security of consumer IoT (DCMS, 2018[44]) paved the way for ETSI's Technical Specification TS 103 645 on "Cyber Security for Consumer Internet of Things" (2019[32]), and for ETSI's European Standard EN 303 645 on "Cyber Security for Consumer Internet of Things: Baseline Requirements" (2020[19]). International co-operation is therefore instrumental to leverage policy tools that have proved successful elsewhere and to enable interoperability between national approaches, a key element to avoid the proliferation, fragmentation and potential inconsistencies of norms.

4.1. Designing smart regulation

"Smart" regulation intends to find a balance between "over-regulation" (i.e. unnecessary, disproportionate policy measures) and "under-regulation" (i.e. the belief that market dynamics on their own will "naturally" solve public policy challenges).

The principles of proportionality (see section 3.6) and necessity are at the core of designing smart regulations. In connection with the former, the latter entails that no lighter measure, which would be equally effective, is available to achieve the intended policy goal. If the policy goal could be achieved by a lighter yet as effective measure, then the means chosen can be considered as unnecessary.

In order to design smart regulations, there is a need for policy makers to answer a few important questions before developing a policy tool (OECD-APEC, 2005[45]):

- What are the precise policy objectives of this tool?

- What specific challenges will it address?
- What types of products and sectors will it cover?
- What incentives and behaviours will it influence?
- What will be the impact on stakeholders, including potential unintended consequences (this could include an economic impact assessment)?
- What is the process for multi-stakeholder input and co-operation?
- What will be relationship between this tool and other instruments already in place or in development?
- What is the process and timeline for reviewing the effectiveness of this tool?

More broadly, the following points are key for the design of “smart regulation” (Drahos, 2017[46]):

- In the majority of circumstances, using multiple rather than single policy instruments, and involving a broader range of regulatory actors, are likely to produce better outcomes. However, in line with the principle of necessity, the preference for a policy mix does not entail that all instruments should be used, but rather than only the minimum number necessary to achieve the desired result should be used.
- Approaching policy tools as an instrument pyramid: less interventionist measures should be preferred in the first instance.
- Relying on multi-stakeholder co-operation to gather input and build responsiveness.
- Maximising opportunities for win–win outcomes by encouraging businesses to go ‘beyond compliance’ within existing legal requirements.

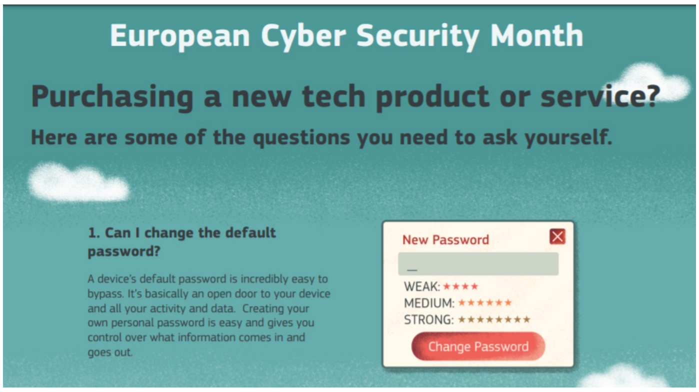
As articulated in the sections below, there is no silver bullet to enhance the digital security of products, and each policy tool has specific benefits, limits and challenges.

4.2. Raising awareness and developing digital security skills

Policy makers can raise awareness on digital security risk through media campaigns and education programs on basic skills for digital literacy. They can also support the development of a workforce with advanced skills by promoting digital security in curricula for schools, university and retraining programs. These tools are important to raise awareness for mainstream users, empower advanced users and support innovation.

In the European Union, the Cyber Security Month is organised every year in October. Stakeholders from various EU countries participate, for instance by sharing resources and advice, organising conferences and webinars, providing training and publishing press releases. The aim is to raise awareness of digital security threats, promote digital security among citizens and organisations and equip mainstream users with resources to protect themselves online. In 2019, the European Union Agency for Cybersecurity, ENISA, focused its campaign on key questions consumers should ask before purchasing smart products (see Figure 4.2).

Figure 4.2. Example of an awareness-raising campaign: Cyber Security Month in the EU



European Cyber Security Month

Purchasing a new tech product or service?

Here are some of the questions you need to ask yourself.

1. Can I change the default password?

A device's default password is incredibly easy to bypass. It's basically an open door to your device and all your activity and data. Creating your own personal password is easy and gives you control over what information comes in and goes out.

Source: ENISA.

While not developed by governments, the website "have I been pwned?"[14] (https://haveibeenpwned.com/) offers an interesting perspective on awareness-raising campaigns. This website is an "*ex post*" (i.e. after a digital security incident) awareness-raising initiative that allows Internet users to check whether their personal data has been compromised by data breaches, by entering their email address. The service then searches the databases associated with known data breaches and provides a list of the occurrences where the e-mail appears. This shows how innovative data-mining and communication tools can be developed to raise awareness, sometimes with more effectiveness than traditional approaches.

4.2.1. Benefits, challenges and limits

For governments, raising awareness of digital security risk and developing digital security skills form the basis of any strategy to enhance the digital security of products. Without an appropriate level of awareness and skills, any effort to increase transparency may fall short of its objectives, as stakeholders may not be able to leverage additional information into meaningful decisions.

From a supply-side perspective, producers need a trained workforce to raise the level of digital security of the products they design and develop. However, while many academic institutions, coding boot camps and job retraining programs teach code development, they do not always equip their graduates with digital security education. For governments, facilitating the development of digital security skills at the national level is key to enable the emergence of a skilled workforce and a vibrant technical community. Mainstreaming advanced digital security skills in engineering, coding, and integrating digital security in more general curricula (e.g. management, legal) should be a priority for policy makers in OECD countries. More broadly, governments should promote and support clear and attractive academic and career paths for digital security professionals.

To be more effective, programs to raise awareness and develop skills can leverage multi-stakeholder co-operation (see sections 3.4 and 4.4). An important advantage of policy tools that raise awareness and develop digital security skills is that they carry no potential for distorting the market, of disproportionate use or of a negative impact on other stakeholders.

However, the use of awareness-raising and education policy tools alone would likely not be sufficient to address the challenges identified in chapter 2. In fact, it is unrealistic to expect mainstream users such as consumers and SMEs to become digital security experts or leverage resources similar to those of large companies. Other policy tools are necessary to increase transparency and empower mainstream users to make informed decision, e.g. labels and conformity assessments. In addition, in many cases, the parties that are the most able to act to enhance the digital security of products are actors within the supply-side.

Consequently, awareness raising campaigns should not be considered as a way to lift producers from their duty of care, in particular regarding security-by-default.

Finally, awareness-raising campaigns should not be the primary tool to ensure the conformity of products with basic minimum requirements. Mainstream users should not be put in a situation where they can purchase products that pose unreasonable risks. For instance, one would not expect a government-backed awareness-raising campaign to advise consumers to only buy cars that are equipped with brakes. Similarly, mainstream users expect the government to ensure that basic digital security features are imposed upon producers of smart products through regulatory requirements.

4.3. The role of governments as economic agents

Beyond their role as regulators, governments are also economic agents. In this role, they need to lead by example (e.g. by a timely deployment of security updates and by taking into account the EOL of the products they use) and can leverage public procurement to shape market incentives towards more optimal outcomes.

Policy makers can support demand for products with a higher level of digital security by requiring producers and contractors to meet certain requirements to be able to bid for public procurement. A recent report in the United States suggested to require all vendors bidding for public procurement for ICT products to certify their products through recognised standards (DHS and DoC, 2018[7]). The draft "IoT Cybersecurity Improvement Act" (Kovacs, 2020[47]), currently examined by the US Congress, proposes to require the federal government to only purchase IoT products that are compliant with relevant NIST standards (2020[18]).

Beyond technical measures and certification, governments may integrate in their public procurement policies the need for diversification when acquiring smart products. Such requirements could have a positive impact on competition and innovation (see section 3.5) and address potential lock-in effects and dependency to certain companies in strategic areas.

4.3.1. Benefits, challenges and limits

The role of governments as economic agents is often neglected, as public attention focuses on their role as regulators. However, as customers of smart products, governments can significantly impact the behaviour of other economic agents and shape market incentives towards more optimal outcomes. This policy tool can be effective in mainstreaming best practices for duty of care, in particular in markets where government is a significant customer. Similarly, leading by example is key to support a government's policy objectives. On the contrary, a lack of consistency between a government's policy objectives and its own behaviour may severely impact its credibility, and *in fine*, the adherence of stakeholders to other policy tools.

The advantage of leveraging public procurement is that it has a low potential of distorting the market or having wide-ranging consequences, unlike *ex ante* regulations. However, it has a moderate potential of disproportionate use, in case the requirements set by the public procurement policies are too high or drafted in a way that could be considered as discriminatory. Currently, most digital security requirements for public procurement in OECD countries focus on organisational aspects rather than on product features.

Resorting to public procurement only will likely not be sufficient to address the challenges identified in chapter 2. Some product categories (e.g. consumer IoT) may not be significantly impacted by a change in public procurement policies, as government is often not a significant customer in these markets. In addition, such policies could send mixed signals to the industry, suggesting that lower requirements are not acceptable for public procurement while being acceptable for mainstream users.

4.4. Facilitating multi-stakeholder partnerships

Policy makers can facilitate multi-stakeholder partnerships, i.e. coalitions of actors from various communities that aim to enhance the digital security of products. These tools are important to increase co-operation, support innovation and enable certain stakeholders to take more responsibility.

Some governments in OECD countries have facilitated the development of multi-stakeholder partnerships to tackle the issue of botnets (e.g. by through funding, or convening relevant actors). Examples include "*botfrei*" in Germany and "NOTICE" (*National Operation Towards IoT Clean Environment*) in Japan. In Japan, the National Institute of Information and Communications Technology (NICT) surveys IoT devices to assess password vulnerabilities. The results are transmitted to Internet service providers (ISPs), which then contact users and issue alerts. Users can reach a support centre at the Ministry of Internal Affairs and Communications (MIC), which provides them with guidance for appropriate digital security measures. Many experts commend these initiatives as they address the negative externalities often associated with smart products (see section 2.1.2) and tend to mainstream ownership of digital security risk.

Other multi-stakeholder partnerships can take place at the operational level (e.g. ISACs and CERTs), at the strategic level (e.g. Paris call for trust and security in cyberspace) or focus on very specific issues (e.g. Software Heritage). For a more detailed discussion of some of these initiatives, see the Annexes.

4.4.1. Benefits, challenges and limits

Facilitating multi-stakeholder partnerships is a key policy tool for governments in order to address externalities and gaps that one actor alone would not be able to fix. These partnerships are instrumental in order to build trust, facilitate dialogue and co-operation and better align incentives across the value chain. The advantage of multi-stakeholder partnerships also lies in their agility, and their ability to leverage resources and talent from a wide range of actors. Governmental facilitation can take various shapes, e.g. financial and institutional support, or a more strategic role in gathering the relevant parties, defining objectives and facilitating consensus.

Multi-stakeholder partnerships have little potential of distorting the market or negatively affecting other stakeholders, as they rely on voluntary co-operation. As they are not a regulatory tool, a disproportionate use is unlikely.

However, resorting to multi-stakeholder partnerships only will likely not be sufficient to address the challenges identified in chapter 2. First, these partnerships rely on voluntary commitment. Even though peer pressure can often be an effective way to influence behaviour, they will not have the wide-ranging effects of regulatory instruments. While it is often easy for stakeholders to agree on common values, it is more difficult to agree on common rules, in particular when trade-offs have to be made between public interest and corporate objectives or individual preferences.

4.5. Developing voluntary guidance and technical standards

Policy makers can develop voluntary frameworks and guidance to empower supply-side actors to enhance the digital security of products, or support the development of technical standards by other stakeholders (e.g. the industry) at the national and international levels. These tools can be defined as sets of principles or requirements that are proposed by the government or other institutions such as standardisation organisations.

To be successful, voluntary frameworks need to leverage the multi-stakeholder community that will ultimately make use of them, from the design phase to the implementation phase. The involvement of the relevant stakeholders will enable policy makers to leverage their knowledge and resources, and create the conditions for the adoption of the framework at a later stage. While their implementation is usually undertaken on a voluntary basis, stakeholders may incentivise economic agents to use these standards: for instance, large corporations can require conformity with them in their contracts (see section 4.6) and governments can require conformity in their procurement policies (see section 4.3). The best format[15] for the framework will likely depend on the context. Depending on the context, certain stakeholders may prefer principles-based and outcomes-oriented frameworks, while others may prefer clear technical requirements (see section 4.8).

In the United States, NIST has developed a voluntary framework to provide guidance to supply-side actors in the IoT market, for both consumer and industrial IoT, and across verticals (NIST, 2020[18]). Given its wide scope, the framework focuses on manufacturers' processes and policies (or "activities") rather than on product features. The framework identifies six cores activities for supply-side actors and intends to "lessen the efforts needed by customers" to manage digital security risk. In the UK, the government has developed a Code of Practice for Consumer IoT (DCMS, 2018[44]) that proposes thirteen outcomes-oriented guidelines for stakeholders, in particular for producers of IoT devices. These guidelines address many aspects of the digital security of products, from access control and authentication to data protection and security updates. On the basis of this framework, ETSI has developed a technical specification, TS 103 645 on "Cyber Security for Consumer Internet of Things" (2019[32]), and a European standard, EN 303 645 on "Cyber Security for Consumer Internet of Things: Baseline Requirements" (2020[19]).

As these frameworks were developed recently, there is a need to schedule regular reviews of their uptake by relevant stakeholders, in order to assess their effectiveness. In the absence of significant uptake, there may be a need to develop other policy tools such as *ex ante* requirements and *ex post* mechanisms.

4.5.1. Benefits, challenges and limits

Voluntary frameworks are effective tools to provide guidance to stakeholders, in particular supply-side actors. They can be effective at realigning market incentives and reducing misperception of risk, and can also enable supply-side actors to assess their maturity regarding digital security risk management. Voluntary frameworks are also an important tool to address the challenge of complexity (see section 2.1.1), as different standards can be developed for different contexts of use (e.g. various sectors or "verticals", consumer v. industrial, etc.). They are also more flexible than legal requirements, and can therefore adapt quickly to technological change. As they are voluntary, they have little potential for disproportionate use or market distortion.

However, industry-led approaches can be captured by certain actors, e.g. large organisations that can afford to participate to and influence such processes, as opposed to SMEs. These actors could drive the results of industry-led processes towards their interests, which may not be aligned with optimal outcomes for society. To address this pitfall, the development of voluntary frameworks should be as inclusive and fair as possible, and could rely on independent third-parties (e.g. a government agency or external experts) to bring neutral perspectives.

Furthermore, the use of voluntary frameworks may prove insufficient to address the challenges identified in chapter 2. Voluntary frameworks only address the supply-side of the value chain. In the absence of labels, they may not empower end-users to make better purchasing decisions nor increase transparency on the market. In addition, the uptake of such frameworks is uncertain and varies greatly across industries.[16] In particular, the uptake seems limited in fragmented or emerging markets, and in markets where externalities and information asymmetries are significant.

Consequently, depending on the specific market, there may be a need for governments to complete voluntary frameworks with other policy tools, to better incentivise stakeholders to adhere to standards. In the UK, for instance, the government has decided, after a public consultation and limited results from the publication of their voluntary framework for IoT security, to proceed with mandating minimum requirements for all IoT products through *ex ante* regulation. In the EU, while the cybersecurity certification scheme envisioned in the EU Cybersecurity Act is designed as voluntary, the regulatory framework also recognises that governments may need to make such certification schemes mandatory where deemed necessary, for certain categories of products or sectors (EU, 2019[48]).

More generally, voluntary frameworks may be a good starting point for governments, as the design of such frameworks is also an occasion to start a dialogue with relevant stakeholders, e.g. producers, vendors and consumers. However, if the uptake is limited and the impact insufficient, policy makers should explore other avenues such as *ex ante* requirements and *ex post* mechanisms.

4.6. Promoting certification and conformity assessment

Policy makers can promote certification and conformity assessments to reduce information asymmetries and realign market incentives. In the United States, a report recently recommended the creation of a "National Cybersecurity Certification and Labelling Authority, empowered to establish and manage a program on security certifications and labelling of ICT products" (Cyberspace Solarium Commission, 2020[12]).

Conformity assessments can be defined as mechanisms to evaluate whether products, processes or organisations meet specific requirements, which can be defined through voluntary guidance and technical standards (see section 4.5). They may be voluntary or mandatory, self-assessed or evaluated by a third-party.

The definition of certification varies across sectors and OECD countries. Certification can be defined as a mechanism to assess with more certainty, through evaluation by an independent third-party, whether products, processes or organisations meet a certain level of digital security. In that regard, some other experts consider that certification does not necessarily need to rely on a conformity assessment: for instance, penetration testing may be used to certify that a product or an organisation meets a certain level of maturity regarding digital security, while not relying on technical standards. Alternatively, other experts consider that certification is one way of assessing conformity, along with other methods such as self-assessment.

4.6.1. Benefits, challenges and limits

Certification and conformity assessments are widely used in some sectors (e.g. food, energy, industry) to reduce information asymmetries and ensure that products meet a certain level of quality or safety. They are effective tools to build trust, increase transparency (see section 3.1), ensure the duty of care of supply-side actors (see section 3.3) and promote innovation and competition (see section 3.5). They also fuel co-operation (see section 3.4) as they enable stakeholders to verify products' quality and connect the technical state of the art (standards) with the market.

For the demand-side, the impact of certification conformity assessments can be high for advanced users, which may be familiar with voluntary frameworks and technical standards. However, for mainstream users, their impact without accessible labels (see section 4.7) is likely to be more limited.

For the supply-side, conformity assessments are associated with significant costs, depending on each model (e.g. certification, self-assessment…). Therefore, the use of certification and conformity assessment should be proportionate to the risk (see section 3.6). For the self-assessment model, there is a significant risk of non-compliance or poor implementation. For the certification model, schemes are usually only valid within a specific jurisdiction. A company would therefore have to undergo new certification processes for every new market they intend to target, which may incur significant additional costs. Cross-border recognition can support the "business case" for certification, as companies would need to go through only one process to obtain a certification that would be valid for a significant market. The European Union's

Cybersecurity Act aims to facilitate cross-border recognition of certifications across EU countries (EU, 2019[48]).

The digital transformation also challenges the nature and scope of certification. In many OECD countries, certifications are only valid for a finished and tangible product, whereas more and more products contain intangible code, and can be updated in the course of their commercial life. If an update modifies their code, their conformity assessments may no longer be valid (Schmitt, 2019[49]). When such certification is mandatory, it can become an obstacle to the implementation of security updates, an issue pointed out as "insecurity-by-compliance" (OECD, 2019[1]).

Policy makers can promote certification and conformity assessments through other policy tools such as public procurement, labels and *ex ante* regulatory requirements (see sections 4.3, 4.7 and 4.8). They can also use *ex post* mechanisms (see section 4.8), e.g. liability regimes and insurance, to incentivise producers to use conformity assessments. For instance, producers that had their products certified by a third-party could be exempted from certain liability risks, while such waivers would not be granted to products that did not go through conformity assessments or whose conformity was only self-assessed. Many risks and limits associated with conformity assessment depend on the other policy tools used to promote them.

4.7. Promoting labels

Labels can be displayed on the product's package, on the producer's website or on the customer's smartphone after scanning a product's identification (e.g. barcode or QR code). Labelling models include information-only (e.g. list of ingredients), binary (e.g. "seal of approval"), traffic lights and graded schemes. They can be awarded by public authorities or industry-led organisations.

Like conformity assessments, they can be voluntary or mandatory, and rely on self-assessment or certification, by a third-party (see section 4.6). Some labelling schemes include certification as a criterion for awarding the label. The main difference between labels and conformity assessments is the accessibility of the information provided: labels are developed in order to increase transparency for mainstream users.

As of November 2020, at least three OECD countries are considering launching, or have launched already, labelling schemes for the digital security of products: Finland, Germany and Japan. A draft label that could be associated with the EU cybersecurity certification schemes is also discussed in the EU. These initiatives are further detailed in section 4.7.2. In the United States, a report recently suggested that the "government should convene industry, civil society, and government stakeholders in a multi-stakeholder process to explore requirements for a viable labelling approach […] so security-conscious consumers can make informed choices and create market incentives for secure-by-design product development" (DHS and DoC, 2018[7]). More recently, another report recommended the creation of a "National Cybersecurity Certification and Labelling Authority, empowered to establish and manage a program on security certifications and labelling of ICT products" (Cyberspace Solarium Commission, 2020[12]).

4.7.1. Benefits, challenges and limits

Labels are an important policy tool to increase transparency, and make stakeholders more aware and empowered. They are effective at realigning market incentives and reducing information asymmetries, in particular for mainstream users.

Labels are often considered as a balanced tool, which has a positive impact on market dynamics while not imposing disproportionate obligations or costs on producers. They are even considered by some as "low-hanging fruit", i.e. a policy tool that would be easy to develop and bring quick and tangible benefits, with a low risk of negatives consequences. However, these perceptions may underestimate the complexity of developing labelling policies, and some of the risks that they carry. Certain flaws often limit the effectiveness of labelling schemes, e.g. lack of comparability and lack of uptake by the industry. If labels are not based on recognised public standards (e.g. international ones), they may lack transparency and consistency regarding the criteria used to award the label. In case international co-operation is limited, there is also a significant risk of label proliferation that may be detrimental to both producers (raising their costs) and customers, in particular mainstream users (e.g. fuelling complexity and consumer fatigue).

There is therefore a need for governments to approach labels with the principles of smart regulation in mind (see section 4.1), in order to ensure that labelling schemes are proportionate and consistent across sectors and countries, and with other policy instruments. Policy makers should consider *i)* which type of label is the more adapted to their objectives (mandatory or voluntary, binary or multi-layered, etc.); and *ii)* the scope of the label: will it apply to all smart products, or only to specific verticals (e.g. consumer IoT, routers…). While general labels may be beneficial to ensure the simplicity and universality of the labelling scheme – two key factors for its effectiveness –, they may also be difficult to implement as digital security challenges and best practices may vary across sectors, for which various technical standards may be available. While it may seem easier to implement binary voluntary labels on specific market segments, the use of mandatory labels that rely on a tiered approach (e.g. a graded scheme) is more likely to have wide-ranging effects on market dynamics.

To conclude, while labels are promising, they should not be considered as a panacea to enhance the digital security of products. In 2019, the UK government has considered developing a voluntary label for IoT security. However, the government decided to rather resort to a regulatory approach after a public consultation highlighted important gaps that may not be addressed by the development of voluntary labels only. In particular, the consultation indicated that consumers expected minimum requirements to be in place through regulations, and would not consider the absence of label as a sign of increased risks. Labels could be useful to help consumers decide between products with a reasonable level of digital security but would be insufficient to impose a minimum level of digital security for all products.

A more detailed discussion of the different types of labels, of labelling schemes developed in other sectors, and of the opportunities and challenges associated with labels, is provided in the Annexes.

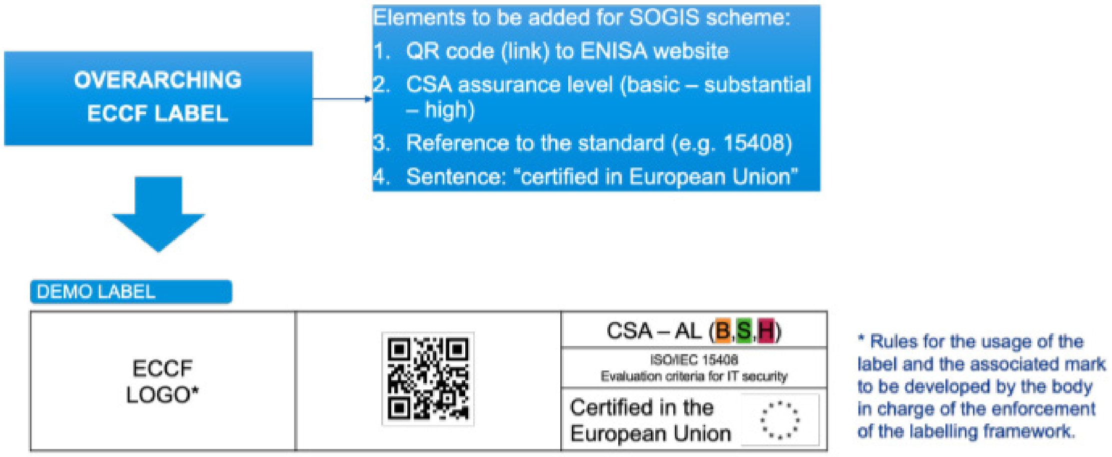
4.7.2. Digital security labelling schemes developed in OECD countries

This section provides an overview of the digital security labelling schemes that have been discussed or developed in OECD countries.

European Union

In a report published in July 2020, ENISA, the European Union Agency for Cybersecurity, discussed the development of an EU label that would enable customers to identify products certified in accordance with EU cybersecurity certification schemes (ENISA, 2020[50]). As outlined in Figure 4.3, the proposed label would include an easily recognisable logo, three levels of assurance (basic, substantial and high), references to relevant standards, as well as a QR code that could deliver more information upon scanning.

Figure 4.3. Draft EU Cybersecurity label


OVERARCHING
ECCF LABEL
Elements to be added for SOGIS scheme:
1. QR code (link) to ENISA website
2. CSA assurance level (basic – substantial – high)
3. Reference to the standard (e.g. 15408)
4. Sentence: "certified in European Union"
DEMO LABEL
ECCF LOGO*
CSA – AL (B,S,H)
ISO/IEC 15408
Evaluation criteria for IT security
Certified in the European Union
* Rules for the usage of the label and the associated mark to be developed by the body in charge of the enforcement of the labelling framework.

Note: ECCF stands for European Cybersecurity Certification Framework.
Source: (ENISA, 2020[50]).

Finland

In November 2019, the Finnish Transport and Communications Agency (Traficom) launched an "information security" label for IoT devices. The label will be awarded to IoT products if they meet certain certification criteria, based on the ETSI technical specification on Cyber Security for Consumer IoT (2019[32]).

The initiative results from a private-public partnership between the National Cyber Security Centre Finland (NCSC-FI) at Traficom and the following companies: Cozify Oy, DNA Plc and Polar Electro Oy. The label's website (Traficom, 2019[51]) references the products that have been awarded the label and publishes information about the label. In addition, the website provides information to businesses on how they can apply for the label. The labelling scheme relies on several criteria, including certifications awarded to the product or the producer (e.g. STAR certification by the Cloud Security Alliance), support period, the updatability, vulnerability disclosure policy, encryption and privacy protection.

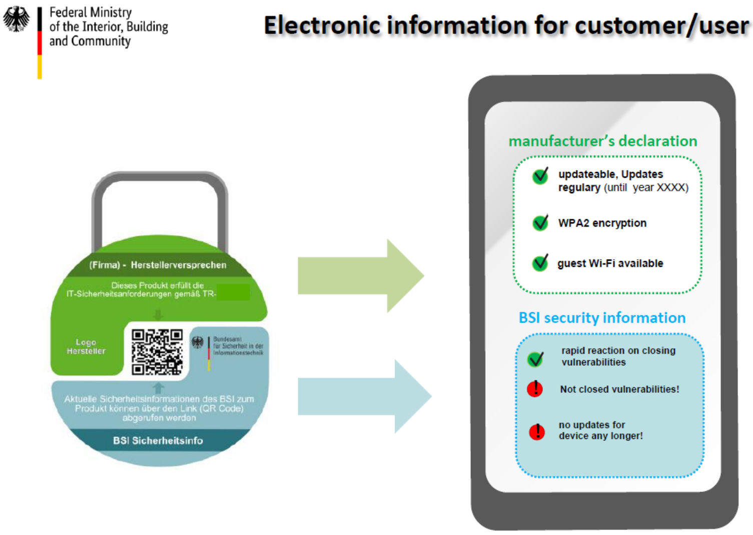
Germany

In Germany, the agency in charge of digital security (BSI) partnered with the industry to launch in 2020 a voluntary labelling scheme, "IT Security". The labelling scheme would be available for all IT products, even though the criteria used to award the labels would be adapted for each category of products (e.g. routers, meters…).

For the government, the objective of the label is to supplement existing statements by product manufacturers, which often lack visibility, relevance and comparability between products. In comparison, the IT security label is standardised, easily understandable by customers and up-to-date.

The label takes the form of a QR code present in the product's package, which, upon scanning, presents two sets of information to the customer: the manufacturer's self-declaration and the BSI security information (Figure 4.4). The latter is intended to inform the consumer about security gaps or other security-relevant IT characteristics, while the manufacturer's declaration assures that the product has certain IT security characteristics.

Figure 4.4. Proposed IT label in Germany

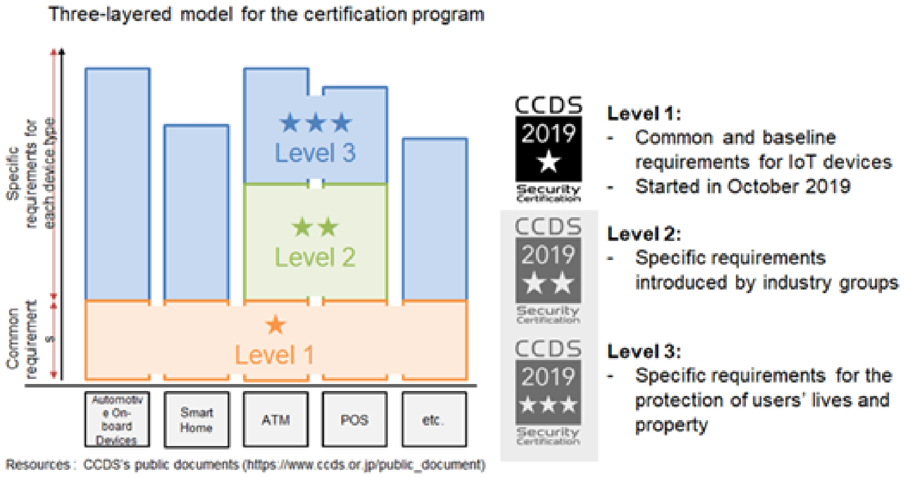

Federal Ministry
of the Interior, Building
and Community
Electronic information for customer/user
(Firma) - Herstellerversprechen
Dieses Produkt erfüllt die
IT-Sicherheitsanforderungen gemäß TR-
Logo
Hersteller
Bundesamt
für Sicherheit in der
Informationstechnik
Aktuelle Sicherheitsinformationen des BSI zum
Produkt können über den Link (QR Code)
abgerufen werden
BSI Sicherheitsinfo
manufacturer's declaration
updateable, Updates regulary (until year XXXX)
WPA2 encryption
guest Wi-Fi available
BSI security information
rapid reaction on closing vulnerabilities
Not closed vulnerabilities!
no updates for device any longer!

Source: BSI

Japan

In Japan, the Connected Consumer Device Security Council (CCDS), a business association to improve the security of consumer devices including IoT devices, started a voluntary labelling program for IoT devices in October 2019. The labelling program relies on the certification of products. In this certification program, the level of security measures for IoT devices is classified into a three-layer model as shown in Figure 4.5.

Figure 4.5. Japan's labelling scheme for IoT products


Three-layered model for the certification program
Specific requirements for each device type
Common requirements
★★★ Level 3
★★ Level 2
★ Level 1
Automotive On-board Devices
Smart Home
ATM
POS
etc.
Resources : CCDS's public documents (https://www.ccds.or.jp/public_document)
CCDS 2019 ★ Security Certification
CCDS 2019 ★★ Security Certification
CCDS 2019 ★★★ Security Certification
Level 1:
- Common and baseline requirements for IoT devices
- Started in October 2019
Level 2:
- Specific requirements introduced by industry groups
Level 3:
- Specific requirements for the protection of users' lives and property

Note: Levels 2 and 3 have been launched in October 2020.
Source: Japanese government, MIC.

The level 1 certification is based on the regulatory requirements set by the regulator's Amendment of the Technical Standards of Terminal Equipment for IoT security. This regulation makes the following elements mandatory for the provision of IoT devices: access control function; feature to encourage users to change the default IDs/passwords; firmware update feature for the future security fixes.

The level 2 certification will be developed within specific sectors (e.g. banking, industry) while the level 3 certification will be developed for product safety.

4.8. Ex post mechanisms

Ex post mechanisms include liability regimes (e.g. strict liability, negligence…), consumer protection (e.g. against unfair and deceptive practices), contract law, insurance and guarantees. They can be defined as policy tools that enable stakeholders to claim compensations in case of defects or incidents, *after* their occurrence. They often rely on assessing the alignment of a product's quality, or of an organisation's responsibility (e.g. producers and vendors) with what could be reasonably expected. In case of misalignment, *ex post* mechanisms sanction the responsible actors (e.g. with fines). Such controls take place after the product has been released on the market, and may use conformity assessments with applicable standards and norms as a way to determine the responsibility of each actor.

4.8.1. Benefits, challenges and limits

Ex post mechanisms are an important policy tool to ensure responsibility and duty of care. They are effective at incentivising stakeholders along the value chain to provide higher standards of security for their products (Dean, 2018[9]). They have been implemented in other policy areas (e.g. product safety), usually in combination with other tools such as *ex ante* requirements, certification and conformity assessments.

The main advantage of *ex post* mechanisms is that they can incentivise stakeholders to act more responsibly without prescribing wide-ranging, horizontal norms, as they rather let stakeholders determine what is optimal in each context (e.g. certain markets or product categories). This flexibility is important to address the issue of complexity inherent to smart products (see section 2.1.1).

However, the application of *ex post* mechanisms to smart products raises a number of challenges. These mechanisms take time to adapt to new products and technological change, and to result in effective changes on market dynamics and stakeholder behaviour. Relying exclusively on such mechanisms to address the challenges identified in chapter 2 of this report would be likely insufficient.

In addition, recent research suggests that current norms and regulations need to be adapted to facilitate the application of *ex post* mechanisms to smart products (EU Expert Group on Liability and New Technologies, 2019[33]). In the United States, a recent report recommended to "pass a law establishing that final goods assemblers of software, hardware and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities for as long as they support a product or service" (Cyberspace Solarium Commission, 2020[12]). More broadly, there may be a need for policy makers to review existing legal regimes that support *ex post* mechanisms, to examine their effectiveness for smart products, and to explore solutions to bridge potential gaps. Defining clear roles and responsibilities for all relevant stakeholders (e.g. supply-side actors, network operators, end-users and other code owners) is key to enable *ex post* mechanisms to be effective. Similarly, the development of cyber insurance is limited due to the lack of available data to define and set the price of coverage in an optimal manner. The use of other policy tools (e.g. multi-stakeholder partnerships) could be effective to enable more information sharing between insurance companies and other relevant parties.

4.9. Ex ante requirements

Ex ante requirements can be defined as obligations set in laws or regulations, which stakeholders such as producers and vendors have to comply with before placing a product on the market. They are considered necessary where risks are misperceived or too high (e.g. safety), where there is evidence of market failure (e.g. because of externalities and information asymmetries) and where other policy tools have proved insufficient to address significant gaps.

4.9.1. Benefits, challenges and limits

Ex ante requirements can be considered as a very effective policy tool to ensure responsibility and duty of care, to increase transparency and to realign market incentives. They have been successfully implemented in other sectors (e.g. food, energy, automobile) to set minimum requirements for products and organisations. On markets where consumer awareness is limited and significant risks often misperceived, *ex ante* requirements are paramount.

However, *ex ante* requirements can be disproportionate and considerably disrupt markets. Hence, they should be carefully drafted so that they accurately balance digital security considerations with other aspects, e.g. economic interests of supply-side actors and consumer rights. Designing *ex ante* requirements on the basis of international standards is also key to limit inconsistencies across jurisdictions. Inconsistencies can also be addressed by establishing of technology-neutral, principles-based and outcomes-oriented regulations, coupled with the publication of clear guidance such as technical specifications. *Ex ante* requirements should also provide flexibility for legacy products (i.e. that were designed or produced before the enactment of the requirements).

The use of *ex ante* requirements alone may prove insufficient to address the challenges identified in chapter 2, in particular to reduce information asymmetries. In fact, setting minimum requirements only would not enable stakeholders to differentiate between various levels of digital security, and, while raising the bar, could lead to a “race to the bottom”. In addition, *ex ante* requirements are often intertwined with conformity assessments and *ex post* mechanisms, as effective liability law, for instance, is key to ensure the enforcement of *ex ante* requirements.

4.9.2. Increasing product transparency

First, *ex ante* requirements can aim to increase product transparency. The lack of systemic transparency regarding the code components of smart products contributes substantially to the misperception of risk and persistent information asymmetries.

The initiative launched in the US to develop a software bill of materials (SBOM) relies on a voluntary framework (see section 4.5) rather than on mandatory requirements. This approach could be useful as a first step in order to identify which product features or components would require more transparency. However, it could fall short of its objectives if the uptake by the industry is limited. This outcome is likely if the perceived costs and challenges exceed the perceived benefits for the industry, and in the absence of pressure from the government or other stakeholders. Alternatively, mandatory transparency requirements for supply-side actors could be more effective at addressing the significant information asymmetries identified in this report. Such obligations have proved effective for products in other markets (e.g. ingredients for food, energy efficiency for certain products such as home appliances).

In particular, such information could include elements (see section 3.1) relative to:

- Product traceability: a software bill of materials listing all code components and software libraries used in the product, along with the associated code owners.

- Supply-side actors' accountability: security-by-design, security-by-default, dynamic management of vulnerabilities, responsible EOL policies and digital security of the organisation.

These mandatory transparency requirements could be developed through descriptive information labels (see section 4.7) and through self-assessment (see sections 4.5 and 4.5). Compliance could be verified through market surveillance and product testing, and associated with strong and effective *ex post* mechanisms (e.g. application of liability laws, see section 4.8). For products that could be associated with a higher risk, third-party assessments (certifications) could be made mandatory (see section 4.5). Regulatory requirements on product transparency would be most effective if they rely on frameworks that are, if not similar, at least interoperable at the international level (see sections 4.9.3 and 4.9.7).

However, the tools used to increase transparency and information sharing need to take into account different levels of understanding and cognitive abilities, based on the category of users they target. For instance, access to source code and conformity assessment for technical standards may be appropriate to reduce information asymmetries between advanced users and supply-side actors (see section 4.6). However, mainstream users may need a more accessible format, e.g. through labels (see section 4.7). Effective transparency measures could usefully rely on a multi-layered approach, which would communicate easily accessible information to mainstream users (e.g. through a graded-scheme label) while also enabling advanced users to access more technical information (e.g. through scanning a QR code on the product).

Importantly, in line with the principle of proportionality (see section 3.6), transparency requirements should be proportionate and necessary. If transparency requirements are not proportionate and the information not provided in an accessible format, it could easily lead to consumer fatigue while not being effective at reducing information asymmetries. For instance, there is a debate regarding the effectiveness of certain transparency measures that aimed to empower users to better manage their privacy online. In the wake of the GDPR and other privacy laws in the last decade, there has been a proliferation of pop-up windows notifying consumers of the need to consent to the use of cookies or to the service provider's privacy policies. Recent research questions the effectiveness of such measures, as a majority of consumers seem to not read privacy policies thoroughly and to accept the use of cookies almost automatically, considering the pop-up windows mostly as annoyance rather than as an effective protection measure (Lomas, 2019[20]) (Litman-Navarro, 2019[21]) (Fowler, 2020[22]). This shows that it may not be effective to require supply-side actors to be more transparent about their policies, if the information provided does not enable meaningful consumer choice and comparison between products and organisations.

Compared with other *ex ante* requirements (e.g. technical requirements or principles-based and outcomes-oriented regulations), transparency requirements are often considered as carrying less potential for a disproportionate use. In fact, even though they are mandatory, they do not impose specific features or conducts on supply-side actors. On the contrary, they rely on market forces to drive positive changes, considering that these forces will be more effective if information asymmetries are appropriately addressed.

4.9.3. The challenges associated with ex ante requirements

In addition to increasing transparency, *ex ante* requirements can aim to ensure duty of care through compliance with high-level principles or with technical specifications.

However, governments are sometimes reluctant to impose *ex ante* requirements, as they have a significant impact on market dynamics and can be disproportionate. *Ex ante* requirements that would be too heavy could prevent certain stakeholders to access the market and therefore have a negative impact on growth and well-being. There is often a gap between the speed of innovation and the time needed by legislative bodies to adapt to these changes, e.g. by drafting and adopting new laws, or modifying existing ones (in the United States, the Telecommunications Act was adopted in 1996 and has not been modified since). In addition, it has been argued that regulations that are too prescriptive or technical may quickly become obsolete, hinder innovation or limit consumer choice (OECD, 2019[1]). This argument is particularly valid in certain markets, where the speed of innovation (e.g. IoT) is so high that detailed technical regulations could result in "insecurity-by-compliance" after a few years (OECD, 2019[1]).

For instance, there is a broad consensus in the Internet technical community that the adoption of IPv6 would reduce network complexity and bring tremendous benefits in terms of user experience, stability and security (NTIA, n.d.[52]). However, the adoption of IPv6 remains low in many countries, and many stakeholders have called for more proactive measures to accelerate IPv6 adoption (de Natris, 2020[53]). In this context, the French Parliament passed a law in 2016 mandating that all "terminal equipment" for sale or rental in France shall be "IPv6 compatible" by 2018. However, the law adopted by the French Parliament considerably underestimated the complexity of the issue. In fact, its applicability was very limited, first because of the broad range of products covered by the term "terminal equipment", which all faced different challenges regarding IPv6 adoption. In addition, the law did not include a transition period for manufacturers to adapt their catalogues and production lines, and for vendors to sell their stocks of legacy, non-IPv6 compatible products. The negative impact of the measure on fundamental rights or freedoms at the national and EU level (e.g. entrepreneurship, free movement of goods and services…) was also overlooked. As a result, the law was adopted but never enforced. The French government decided a few years later to change the law and remove this obligation, considering it was disproportionate and noting that its applicability has been in fact difficult if not impossible (CMS Francis Lefebvre, 2019[54]).

To take another example, a law that would mandate all IoT devices to have strong passwords could become obsolete if other innovative and more effective authentication or access control mechanisms become more widespread (e.g. MFA). One could argue that such *ex ante* requirements are disproportionate, as they would limit consumer choice, impose unnecessary costs, limit the ability of producers to take advantage of innovation and incentivise them to focus on compliance rather than on actually enhancing digital security. Recent reports considered that "mandating specific regulations may address some risks, but they can carry with them a greater burden while still leaving the broader ecosystem insecure or sending the signal that complying with the regulation is sufficient rather than the minimum necessary" requirements (DHS and DoC, 2018[7]).

4.9.4. Technology-neutral, principles-based and outcomes-oriented regulations

To avoid these pitfalls, a good practice is to design regulations or laws that are technology-neutral, principles-based and outcomes-oriented. These laws, such as the EU's GDPR, outline the outcomes that stakeholders should aim to and the main principles that should guide them in achieving these outcomes (e.g. data minimisation for GDPR).

While these regulations do not impose specific technical means to achieve these outcomes, they can incentivise or require producers to follow recognised international or industry standards. For instance, Article 32 of the GDPR ("*Security of processing*"), states that data processors should take into account the "state of the art" to "implement appropriate technical and organisational measures to ensure a level of security". The article also states that "adherence to an approved code of conduct" or "an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements" (GDPR, 2018[55]). These standards are agile enough to evolve rapidly and cope with the speed of innovation.

By setting a general framework, principles-based and outcomes-oriented regulations allow stakeholders to choose which international standards or technical specifications are the most appropriate, in their specific context, to enable them to achieve the objectives set in the regulations. In general, various standards are available to meet regulatory requirements. In some cases, *ex ante* requirements can also foster innovation and competition (e.g. the requirements set in GDPR for data portability).

4.9.5. The need for clear guidance

However, one could also argue that principles-based and outcomes-oriented regulations sometimes lack clarity, and may leave stakeholders in disarray on how to actually comply with the regulation. Producers with limited resources in particular (e.g. SMEs) need to know easily if their products comply or not, e.g. with a checklist or a set of clear organisational or technical requirements.

How can policy makers overcome the paradox between the need for clear guidance and the importance of principles-based and outcomes-oriented regulations? This issue can be addressed through articulating appropriate levels of responsibility across the regulatory value chain. Some initiatives in OECD countries have shown how laws can set principles while regulators can provide guidance, e.g. through technical specifications. Leveraging the modularity of the “pyramid of norms” could help solve the issue of “legal rigidity” and enable governments to enhance security without stifling innovation or creating unnecessary burdens.

In Japan, the law states that regulators have the power to require technical specifications for terminal equipment connected to the networks of telecommunications operators. These requirements are met through product conformity assessments (which can be self-assessed) that are visible to consumers through the “T” mark, similar to the “CE” mark in the European Economic Area (EEA). For IoT products, the Japanese regulator specifies these requirements through a document called the “Technical Standards of Terminal Equipment for IoT security”. This way, the regulator has enough flexibility to update their requirements as industry standards evolve (as opposed to updating a law, which would require Parliamentary approval and take much more time). In March 2019, the Japanese regulator updated the Technical Standards to require producers of IoT to incorporate three features on their devices: firmware updates; access control; and incentives for users to change default passwords or set strong passwords. These requirements are effective in Japan since April 2020.

In Korea, the government revised the “Act on Promotion of Information and Communications Network Utilization and Information Protection” in order to include in its scope the producers and vendors of smart products. The revised act also broadens regulatory objectives to enable the government to recommend supply-side actors to follow “information protection guidelines”, for instance through certification. In addition, the Ministry of Science and ICTs (MSIT) established mandatory minimum requirements for image processing devices (e.g. IP cameras), including measures to incentivise users to set a new and strong password upon purchase of the product.

Similarly, in 2020, the UK government decided to develop regulatory instruments to require the supply-side actors of the IoT to comply with the first three recommendations of their Code of Practice for consumer IoT (DCMS, 2018[44]): no default passwords; transparency about the provision of security updates; establishing a vulnerability disclosure policy. This decision followed a public consultation in the UK, which suggested that voluntary commitments by the industry, e.g. though labels, would likely be insufficient in addressing the digital security challenges raised by the development of consumer IoT. The results of the consultation showed a large support for *ex ante* legal requirements that would mainstream baseline requirements for all IoT products.

More broadly, there is a need to clarify, e.g. through regulation, the roles and responsibilities of various stakeholders, in particular supply-side actors.

4.9.6. The case for ex ante requirements for smart products

In light of the significant challenges described in chapter 2 of this report, and of the strong evidence of market failure fuelled by externalities and information asymmetries, there is a clear argument in favour of *ex ante* requirements for the supply-side actors of smart products.

In the United Sates, a recent report outlined the need to "adjust incentives" and "align market forces", which, in some cases, "where those forces either are not present or do not adequately address risk", could take the form of "legislation, regulation, executive action" (Cyberspace Solarium Commission, 2020[12]).

Such *ex ante* requirements could take the form of:

- Technology-neutral, principles-based and outcomes-oriented regulations: the law could ensure that producers, vendors and other codes owners act responsibly according to their duty of care. The principles could include security-by-design and security-by-default (see section 3.3).
- Obligations to adhere to relevant and recognised code of conducts or international standards (e.g. ISO, ETSI…), through self-assessment or certifications.
- Mandatory features for products and organisations, which could be set through guidance. For instance, such requirements could include the need for smart products to be updatable, testable and have robust access controls (e.g. strong authentication). Other types of requirements could include the need for producers to have a vulnerability disclosure policy, provide timely updates and have a responsible EOL policy.

These obligations could be associated with strong transparency requirements to enable traceability (e.g. information about components and value chain) and address information asymmetries (see section 4.9.1).

Importantly, these requirements should be design and technology neutral, consistent with other policy areas (e.g. privacy) and take into account the need for exceptions and proportionality (see section 3.6).

4.9.7. Addressing regulatory fragmentation

From the industry's perspective, the potential fragmentation of regulatory requirements across OECD countries represents a significant challenge. The need to assess the conformity of products with many guidelines and standards, in particular through third-party certification, incurs significant costs. One may also argue that each additional conformity assessment does not necessarily bring much value compared to the previous one. For end-users, the fragmentation of standards and requirements could also bring confusion (e.g., consumer fatigue if too many labels are available, see section 4.7).

The use of principles-based, outcomes-oriented regulations may be considered as a way to avoid such fragmentation, as they allow producers to choose the industry or international standard most fit for their need, instead of imposing specific technical requirements that may vary across countries. Regulations can rely on existing industry or international standards, for instance through requiring alignment with those, instead of creating entirely new requirements.

Another important aspect to take into consideration is the importance of interoperability between legal frameworks. For instance, the GDPR recognises that other privacy frameworks may provide an equivalent level of data protection. In January 2019, the EU Commission (European Commission, 2019[56]) adopted an adequacy decision on Japan, allowing personal data to flow freely between the two economies on the basis of strong protection guarantees. Such interoperability should also be promoted for the digital security of products.

References

(n.a.) (2021), *Global Stats statcounter*, https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/#monthly-201901-202001. [13]

(n.a.) (2021), *National Council of ISACs*, https://www.nationalisacs.org/. [63]

(n.a.) (2021), *Paris Call*, https://pariscall.international/en/supporters. [84]

Akerlof (1970), *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, The Quarterly Journal of Economics, http://www.jstor.org/stable/1879431. [75]

Bakies, E. et al. (n.d.), *The CMMC Has Arrived: DoD Publishes Version 1.0 of Its New Cybersecurity Framework and Discusses Planned Rollout*, Lexology, https://www.lexology.com/library/detail.aspx?g=b9423e51-620a-4d86-8713-f98e809a0066 (accessed on 1 February 2021). [62]

Baksh, M. (2020), *Zoom or Not? NSA Offers Agencies Guidance for Choosing Videoconference Tools*, Nextgov, https://www.nextgov.com/cybersecurity/2020/04/zoom-or-not-nsa-offers-agencies-guidance-choosing-videoconference-tools/164953/ (accessed on 1 February 2021). [25]

Blythe and Johnson (2018), *Rapid evidence assessment on labelling Schemes for IoT Security*, PETRAS, https://www.gov.uk/government/publications/rapid-evidence-assessment-on-labelling-schemes-for-iot-security. [68]

Cloud security alliance (2017), *Security Guidance*, https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf. [34]

CMS Francis Lefebvre (2019), *Communications électroniques : Que prévoit le projet de loi sur la "surtransposition" des directives européennes en matière de communications électroniques ?*, CMS Francis Lefebvre, https://cms.law/fr/fra/publication/que-prevoit-le-projet-de-loi-sur-la-surtransposition (accessed on 1 February 2021). [54]

Cyberspace Solarium Commission (2020), *Cyberspace Solarium Commission Report*, https://www.solarium.gov/. [12]

DCMS (2018), *Code of Practice for Consumer IoT Security*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf. [44]

DCMS (2018), *Mapping of IoT Security Recommendations*, https://aioti.eu/wp-content/uploads/2019/06/DCMS_Mapping_of_IoT__Security_Recommendations_Guidance_an [58] d_Standards_to_CoP_Oct_2018.pdf.

DCMS (2018), *Secure by Design report*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf. [8]

de Natris (2020), *Setting the Standard for a more Secure and Trustworthy Internet*, IGF, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9615/2023. [53]

Dean, B. (2018), *Strict Products Liability and the Internet of Things*, Center for Democracy and Technology. [9]

DHS and DoC (2018), *Report on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets"*, https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets. [7]

Drahos, P. (2017), *Regulatory Theory: Foundations and applications*, http://dx.doi.org/10.22459/RT.02.2017. [46]

Dutch Government, M. (2018), *Roadmap for digital hard- and software security*, https://www.government.nl/documents/reports/2018/04/02/roadmap-for-digital-hard--and-software-security. [64]

ENISA (2020), *Cybersecurity Certification Candidate Scheme*, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme. [50]

ENISA (2019), *IoT Security Standards Gap Analysis*, https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis. [59]

ENISA (2017), *Baseline Security Recommendations for IoT*, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. [80]

ETSI (2020), *Cyber Security for Consumer Internet of Things: Baseline Requirements*, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf. [19]

ETSI (2019), *Technical specification : Cyber Security for Consumer Internet of Things*, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf. [32]

EU (2019), *The EU Cybersecurity Act*, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act. [48]

EU (2016), *NIS directive*, https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive. [26]

EU Expert Group on Liability and New Technologies (2019), *Liability for Artificial Intelligence and other emerging technologies*, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608. [33]

European Commission (2019), *European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows*, European Commission, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421 (accessed on [56]

1 February 2021).

FDA (2016), *Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software"*, FDA, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/information-healthcare-organizations-about-fdas-guidance-industry-cybersecurity-networked-medical (accessed on 1 February 2021). [69]

Fowler, G. (2020), *Sen. Sherrod Brown's new DATA act would shift the burden to protect personal data from consumers to companies*, The Washington Post, https://www.washingtonpost.com/technology/2020/06/18/data-privacy-law-sherrod-brown/ (accessed on 1 February 2021). [22]

Frei, S. (2020), *ETH Zurich / ICT Switzerland*, https://techzoom.net/. [67]

Gartenberg, C. (2018), *California becomes the 18th state to introduce right to repair bill*, The Verge, https://www.theverge.com/2018/3/8/17097256/california-right-to-repair-bill-apple-microsoft-service-replace-parts (accessed on 1 February 2021). [38]

GDPR (2018), *GDPR*. [55]

Geneva Dialogue (2020), *Output document on good practices*, https://genevadialogue.ch/goodpractices/. [65]

Hay Newman, L. (2020), *So Wait, How Encrypted Are Zoom Meetings Really?*, WIRED, https://www.wired.com/story/zoom-security-encryption/ (accessed on 1 February 2021). [23]

IEEE (2017), *Internet of Things (IoT) Security Best Practices*, https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf. [60]

Injury Facts (2011), *Car Crash Deaths and Rates*, Injury Facts, https://injuryfacts.nsc.org/motor-vehicle/historical-fatality-trends/deaths-and-rates/ (accessed on 1 February 2021). [78]

IoT Security Foundation (2018), *Crazy! Less than 10% of consumer IoT companies follow Vulnerability Disclosure guidelines*, IoT Security Foundation, https://www.iotsecurityfoundation.org/less-than-10-of-consumer-iot-companies-follow-vulnerability-disclosure-guidelines/ (accessed on 1 February 2021). [11]

ISO (2018), *27000*, https://www.iso.org/fr/standard/73906.html. [57]

Kovacs, E. (2020), *U.S. House Passes IoT Cybersecurity Bill*, SecurityWeek.Com, https://www.securityweek.com/us-house-passes-iot-cybersecurity-bill?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29&mc_cid=3f16ae8bed&mc_eid=b9a93a33e4 (accessed on 1 February 2021). [47]

Kregs on Security (2020), *Hackers Were Inside Citrix for Five Months — Krebs on Security*, Kregs on Security, https://krebsonsecurity.com/2020/02/hackers-were-inside-citrix-for-five-months/ (accessed on 1 February 2021). [6]

Krugman (2008), *The Return of Depression Economics and the Crisis of 2008*. [61]

Litman-Navarro, K. (2019), *We Read 150 Privacy Policies. They Were an Incomprehensible* [21]

Disaster., The New York Times, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (accessed on 1 February 2021).

Lomas, N. (2019), *Most EU cookie 'consent' notices are meaningless or manipulative, study finds*, TechCrunch, https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/ (accessed on 1 February 2021). [20]

Mozilla Foundation (2020), **privacy not included - Zoom*, Mozilla Foundation, https://foundation.mozilla.org/en/privacynotincluded/zoom/ (accessed on 1 February 2021). [24]

NIST (2020), *NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers*, https://doi.org/10.6028/NIST.IR.8259. [18]

NIST (2018), *Cybersecurity Framework*, https://www.nist.gov/cyberframework. [43]

NIST (2016), *Intel Corporation Supply Chain Risk Management*, https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Intel-Case-Study.pdf. [37]

North, O. (2019), *Understanding the economics of bug bounty programs*. [83]

NTIA (n.d.), *Technical and Economic Assessment of Internet Protocol, Version 6 (IPv6)*, NTIA: National Telecommunications and Information Administration, https://www.ntia.doc.gov/legacy/ntiahome/ntiageneral/ipv6/final/IPv6final3.htm (accessed on 1 February 2021). [52]

OECD (2021), *Encouraging vulnerability treatment: background report - Responsible management, handling and disclosure of vulnerabilities*, https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf. [3]

OECD (2021), *Encouraging vulnerability treatment: overview for policy makers*, OECD Publishing, Paris, https://doi.org/10.1787/20716826. [4]

OECD (2021), *Understanding the digital security of products - an in-depth analysis*, https://www.oecd.org/sti/ieconomy/security.htm. [2]

OECD (2020), *Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation*, http://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf. [73]

OECD (2020), *Encouraging Digital Security Innovation*. [40]

OECD (2020), *Enhancing the Availability of Data for Cyber Insurance Underwriting, The Role of Public Policy and Regulation*, http://www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-CyberInsurance-Underwriting.pdf. [72]

OECD (2020), *Recommendation on Consumer Product Safety*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0459. [16]

OECD (2020), *The role of sandboxes in promoting flexibility and innovation*, https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf. [41]

OECD (2019), *Principles on artificial intelligence*, https://www.oecd.org/going-digital/ai/principles/. [15]

OECD (2019), *Recommendation on the Digital Security of Critical Activities*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. [42]

OECD (2019), *Summary Report of the Inaugural Event Global Forum on Digital Security for Prosperity*, https://doi.org/10.1787/20716826. [1]

OECD (2018), *Guidance for responsible business conduct*, http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf. [14]

OECD (2016), *Recommendation on Consumer Protection in E-Commerce*, https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf. [28]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en. [17]

OECD (2015), *Recommendation on Digital Security Risk Management*, https://oe.cd/dsrm. [5]

OECD (2012), *Recommendation on the Protection of Children Online*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [30]

OECD (2007), *Recommendation on Consumer Dispute Resolution and Redress*, https://www.oecd.org/sti/ieconomy/oecdrecommendationonconsumerdisputeresolutionandredress.htm. [29]

OECD-APEC (2005), *Integrated checklist on regulatory reform*, https://www.oecd.org/regreform/34989455.pdf. [45]

Perlroth, N. (2017), “Why Car Companies Are Hiring Computer Security Experts”, *The New York Times*, https://www.nytimes.com/2017/06/07/technology/why-car-companies-are-hiring-computer-security-experts.html (accessed on 6 October 2019). [81]

PETRAS (2018), *Summary literature review of industry recommendations and international developments on IoT security*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775854/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf. [70]

PI4.0 & RRI (2020), *IIoT Value Chain Security – The Role of Trustworthiness*, https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.html. [39]

Povich, E. (2018), *Late Payment A Kill Switch Can Strand You and Your Car*, The Pew Charitable Trusts, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/11/27/late-payment-a-kill-switch-can-strand-you-and-your-car (accessed on 1 February 2021). [35]

Ralph Nader (1965), *Unsafe at any speed*. [77]

Schmitt, B. (2019), *It’s 2019, why doesn’t every car have OTA updates?*, The Drive, https://www.thedrive.com/tech/26679/why-havent-over-the-air-updates-taken-over-the-auto-industry (accessed on 1 February 2021). [49]

Schneier, B. (2018), *Click here to kill everybody*, Norton. [10]

Schneier, B. (2016), *Security Design: Stop Trying to Fix the User*, Schneier on Security, [7 https://www.schneier.com/blog/archives/2016/10/security_design.html (accessed on 1 February 2021). 9]

Traficom (2019), *Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products*, Traficom, https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label (accessed on 1 February 2021). [51]

Traficom (2019), *IoT Information Security Label Concept introduction*. [71]

UN (2016), *United Nations Guidelines for Consumer Protection*, https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf. [31]

Verizon (2019), *Data breach investigation report*, https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/. [27]

Voreacos, D., K. Chiglinsky and R. Griffen (2019), *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, Bloomberg, https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war (accessed on 1 February 2021). [74]

WEF (2020), *Global Risk Report*, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. [66]

Wilson, M. (2013), *Infographic: How Many Lines Of Code Is Your Favorite App?*, https://www.fastcompany.com/3021256/infographic-how-many-lines-of-code-is-your-favorite-app (accessed on 5 May 2020). [82]

Woods, D. and T. Moore (2020), "Cyber warranties: Market Fix or Marketing Trick?", *Communications of the ACM*, Vol. 63/4, pp. 104-107, http://dx.doi.org/10.1145/3360310. [76]

Zittrain (2018), *From West World to Best World*, https://www.nytimes.com/2018/06/03/opinion/westworld-internet-of-things.html. [36]

Annexes

Annex A provides a detailed version of the high-level principles.

Annex B provides a detailed version of the policy toolkit.

Annex C discusses the merits and limits of the analogy between car safety in the 20th century and the digital security of IoT in the 21st century.

Annex A. Detailed high-level principles

This Annex contains a detailed version of the high-level principles presented in chapter 3. They can serve as building blocks or areas of focus for the design of public policies and strategies aiming to enhance the digital security of products, and as references for stakeholders involved in managing the digital security of products. Figure 3.1 provides an overview of the high-level principles.

Importantly, these principles should be considered as interdependent, and their effects as cumulative. For instance, the positive effects of increased product transparency will be amplified if markets are innovative and competitive enough to provide for meaningful consumer choice. Similarly, stakeholders will be incentivised to act responsibly if there is effective co-operation and clear governance across the product's value chain. To be effective, the proportionality principle requires transparency about roles and responsibilities of actors across the value chain.

These draft principles were developed through the analysis of case studies (see the in-depth analysis report (OECD, 2021[2])) and of a literature review of existing standards and recommendations such as (ISO, 2018[57]; DCMS, 2018[58]; ETSI, 2020[19]; ENISA, 2019[59]; NIST, 2020[18]), and (IEEE, 2017[60]). As this report is policy-oriented, some recommendations were not taken into account because they were too technical, while others were reformulated into policy-oriented terms. These high-level principles are also intended to be practical and flexible enough to stand the test of time in a rapidly evolving field.

These principles also intend to complement other relevant existing OECD standards in areas such as responsible business conduct (OECD, 2018[14]), artificial intelligence (OECD, 2019[15]) and consumer product safety (OECD, 2020[16]).

Transparency and information sharing

Increasing transparency and information sharing is key to reduce information asymmetries and increase trust. It can also enable stakeholders to better perceive risks and clarify responsibility.

For governments, policy tools to increase transparency include labels, awareness-raising campaigns, certification, conformity assessments and ex ante requirements (see chapter 4).

Transparency can be defined as a situation in which relevant information is made available to all stakeholders in a standardised format, which allows for common understanding, accessibility, clarity and comparison.

Alternatively, information sharing can be defined as a more tailored mechanism, which allows a limited group of stakeholders to share information. To be effective, it requires to build trust between partners (e.g. business partners such as suppliers and manufacturers, or between a company and a governmental digital security agency).

The Digital Security Risk Management Recommendation (OECD, 2015[17]) states that "all stakeholders should understand digital security risk and how to manage it" and "take responsibility for the management of digital security risk". In the context of smart products, transparency can be considered as a condition to achieve awareness and empowerment, and to enable the application of the responsibility principle.

Business interests such as cost-effectiveness, trade secrets and intellectual property are often at odds with transparency and limit the ability and willingness of stakeholders to increase it. These interests should be balanced with the benefits of transparency to determine the optimal equilibrium, in line with the proportionality principle (see section 3.6). In some cases, information sharing between two trusted parties may provide more optimal results than wide-ranging transparency requirements. For instance, a software engineer may be less reluctant to share its products' source code with a public authority or a certification body for vulnerability scanning, than to make the source code available to the wider public and its competitors.

Benefits

Increasing transparency and information sharing can improve product comparability, traceability and accountability.

There is often a lack of information regarding the digital security features of smart products (e.g. updatability, MFA). Increasing transparency for the digital security features of smart products would empower customers to make more informed purchasing decisions. Increasing transparency can also enable the broader multi-stakeholder community to take more responsibility in managing the digital security of products. For instance, providing consumers with raw information regarding a product's code components would not directly enable mainstream users to make more optimal purchasing decisions. However, this raw information can be used by third-parties to develop labels that provide simple and comparable information, which could eventually empower consumers.

In addition, smart products are often developed through global, complex and opaque value chains. This results in a lack of clarity about which individual or organisation owns which layer of code, which paves the way for moral hazard (Krugman, 2008[61]). To reduce value chain opacity, smart products and their components need to be easily traceable. Traceability allows which stakeholders to easily track components and products through the value chain.

At each step of the value chain, every supply-side actor could provide to their customers clear and complete information about the product's code components, including information regarding software libraries. This information could be circulated ultimately to the final product's manufacturer and vendor, which would be able to provide a clear list of components and associated code owners for the products they circulate on the market. This list of components and code owners could be public (e.g. on the product's package, website or in the product itself) or be made available on demand for public authorities and advanced users.

Furthermore, there is often a lack of transparency regarding the policies put in place by supply-side actors (e.g. regarding EOL). There may also be a lack of transparency regarding broader elements of trustworthiness (e.g. access to source code, applicable law for where the servers of headquarters of the supply-side actors are headquarters. To increase accountability, information regarding the supply-side actors' policies for each stage of the product's lifecycle needs to be available, on the basis of the main elements of their duty of care (see section 3.3).

Key questions and areas of focus

To increase transparency and information sharing, the following questions are important:

- What information should be made available?
- To whom?
- Where and how?
- Is the information trustworthy?

What information should be made available?

Figure 3.2 provides an overview of five key areas where more transparency may be needed in order to reduce information asymmetries and enable customers to make more informed risk-based decisions:

- Product features for digital security, e.g. updatability and strong authentication.
- Processes and policies that are put in place by supply-side actors (e.g. EOL).
- The product's code: is the source-code open? Has it been scanned and tested by third-parties such as certification companies or governmental agencies?
- Traceability: is there is a list of code components? Is there enough clarity regarding the product's value chain? Where is the data stored and where does it transit?
- General trustworthiness: this area does not focus on the product itself, but rather on its broader ecosystem. What is the track-record of the organisation for managing digital security? Where are the servers and headquarters of the supply-side actors located? What is the impact of applicable law (e.g. privacy, access to data, etc.)? These areas of focus may also be used as building blocks for standards, certification and labelling schemes. For instance, recently adopted standards in the field of IoT have focused on product features, processes and policies, or "activities" (NIST, 2020[18]; ETSI, 2020[19]).

To whom the information should be made available?

Depending on the context and product category, it may be more suitable to make the information available to the general public (e.g. consumer IoT) or to trusted partners only (see definitions for transparency and information sharing above).

Where and how should the information be made available?

The tools used to increase transparency and information sharing need to take into account different levels of understanding and cognitive abilities. For instance, access to source code and conformity assessment for technical standards may be appropriate to reduce information asymmetries between advanced users and supply-side actors (see section 4.6). However, mainstream users may need a more accessible format, e.g. through labels (see section 4.7).

Is the information trustworthy?

In many cases, information on the key areas described in Figure 3.2 is unavailable. Even when supply-side actors provide such information, it is difficult for customers to make use of it and to trust it, in the absence of other mechanisms such as certification, conformity assessments and labels (see chapter 4).

Finally, in many OECD countries, privacy regulations require data processors to notify the data subjects and the relevant authorities of personal data breaches, under certain circumstances (e.g. the extent of the breach). Similarly, regulations could require supply-side actors to notify customers and relevant authorities in case significant vulnerabilities are discovered in their products. Documentation on vulnerabilities and on the deployment of patches will likely enable stakeholders to enhance the overall level of digital security of products in the long term. In the United States, a report recently noted the need to enable the government to "systemically collect cyber incident information reliably and at the scale necessary to inform situational awareness", and recommended to require "critical infrastructures entities to report cyber incidents to the federal government" (Cyberspace Solarium Commission, 2020[12]).

Without *ex ante* requirements and *ex post* mechanisms, there are little incentives for supply-side actors to provide such information and to be held accountable on its trustworthiness (see section 2.1.2 and chapter 4).

Awareness and empowerment

Enabling stakeholders to be more aware and empowered is key to reduce information asymmetries and realign market incentives. Stakeholders that are more aware and empowered are also more likely to better perceive risks.

For governments, policy tools to enable stakeholders to be aware and empowered include awareness-raising campaigns, education programs, multi-stakeholder partnerships, conformity assessments and labels.

All stakeholders should understand digital security risk and how to manage it (OECD, 2015[17]). For the digital security of products, customers in particular need to be made more aware of the risks and empowered to make more informed decisions. In this context, at least two categories of customers should be distinguished: “mainstream users” and “advanced users”, while recognising that many products could be used by both categories.

Empowering mainstream users

“Mainstream users” include consumers and some corporate users like SMEs. They may have limited skills and knowledge about digital security, and therefore may not have the ability to accurately identify and manage digital security risk.

Mainstream users need to be made more aware of the digital security risks associated with the products they purchase. They should be able to assess whether products meet certain digital security criteria (e.g. adherence to industry best practices, length of commercial support, etc.), for instance through labels and clear statements by the relevant supply-side actors (e.g. the product manufacturer). Labels can be developed by or with the industry, and should take into account various categories of information (e.g. traceability for the product’s components, digital security policies, adherence to standards, etc.). Public policies need to incentivise stakeholders to provide mainstream users with clear and easily accessible information about a product, in order to allow for comparability and informed choices. The opportunities and challenges associated with labels are further discussed in chapter 4 of this report.

In addition, educating mainstream users about basic digital security “hygiene” is key. In fact, phishing and other techniques relying on user interaction are amongst the most common attack vectors (Verizon, 2019[27]). Governments, as well as supply-side actors and civil society, can play a role in enhancing digital security risk education for mainstream users, for instance through awareness-raising campaigns, the development of content and guidelines, and by supporting educational programs.

Beyond awareness-raising, there is also a need to support the development of skills for SMEs and less digitally mature companies, for instance through capacity building and training programs. In particular, mainstreaming risk management approaches amongst these organisations can prove effective to enhance their overall level of digital security.

However, most mainstream users should not be expected to develop advanced digital security skills. While raising the awareness of mainstream users is important, it should not be considered as a way to lift supply-side actors’ responsibility and duty of care. Products should be designed[17] so that mainstream users have as little responsibility as possible for the management of digital security. For instance, to the extent possible, security updates should be automatic (see section 3.3.2).

Beyond awareness raising and developing skills, effective consumer protection is key to empower mainstream users. Principles to ensure effective consumer protection include, inter alia (OECD, 2020[16]; UN, 2016[31]):

- Fair and equitable treatment;
- Disclosure and transparency;

- Protection of privacy;
- Dispute resolution mechanisms;
- Protecting vulnerable and disadvantaged consumers;
- Protecting consumers from hazards to their health and safety;
- Protecting the economic interests of consumers.

Empowering advanced users

"Advanced" users are typically more aware and able to manage the digital security risks associated with smart products than mainstream users. This category of more experienced and autonomous users is heterogeneous, ranging from "geeks" and tech savvy hobbyists to users in professional environments, and trained security experts. Advanced users should be empowered to adjust the level of digital security of the smart products they use, based on their own risk assessment, in particular by being able to:

- Access and modify security settings ;
- Test or reverse engineer a product (analyse "what is in the box") if the source code is not open. The conditions for such practices can be specified in the terms of use or within other policies developed by the producer, in order to bring more legal certainty for the individual or organisation performing the test or reverse engineering ;
- Opt out from security defaults such as automatic updates, and test security updates before deployment;
- Examine "telemetry" data, or metadata about usage and access, in order to detect anomalies (ETSI, 2019[32]). For instance, access a login history in order to identify unauthorised access.

Ultimately, empowering advanced users can contribute to raising awareness for mainstream users. For instance, on the basis of raw information (e.g. a list of a product's components, or the product's source code), advanced users could also develop their own labels and make them available to the public (e.g. through barcode scanning applications).

Responsibility and duty of care

Ensuring responsibility and duty of care is key to realign market incentives towards optimal outcomes and better allocate responsibility.

For governments, policy tools to ensure responsibility and duty of care include *ex ante* requirements, conformity assessments, labels, *ex post* mechanisms and public procurement.

A shared responsibility: the need for more ownership of digital security risk.

"All stakeholders should take responsibility for the management of digital security risk" (OECD, 2015[5]). In other words, no single stakeholder can be held entirely responsible for the digital security of products.

As noted in section 3.2, there is an important role for users in managing digital security risk, as they are ultimately the most knowledgeable about the context of use of smart products. In the United States, a report recently estimated that a third of all breaches still stem from a malign actor's success in persuading individuals to open phishing emails" (Cyberspace Solarium Commission, 2020[12]), confirming that individuals are "important guarantors of collective cybersecurity". While acknowledging the important role of users, the same report recognised the need for supply-side actors to "to develop security frameworks that do not overburden end users" (Cyberspace Solarium Commission, 2020[12]).

To enable stakeholders to take ownership, there is a need to make them more aware and empowered, for instance through education (see section 3.2), to increase co-operation and to clarify their roles (see section 3.4). Guidance and standards (see section 4.5) can help to define which stakeholder is responsible for which security control. Ensuring the effectiveness of *ex post* mechanisms (e.g. insurance and liability law, see section 4.8) is also key in incentivising stakeholders to take responsibility.

The duty of care of supply-side actors

However, the level of responsibility is not the same for all stakeholders, and depends on "their roles, ability to act and the context" (OECD, 2015[17]). In the context of smart products, supply-side actors (vendors and manufacturers), as they put products on the market and benefit from their sale (EU Expert Group on Liability and New Technologies, 2019[33]), have a specific responsibility, which can be referred to as a "duty of care". This duty of care should be considered as:

- A duty of care towards other stakeholders: to the extent possible, supply-side actors should be responsible for managing the digital security of their products. They should not shift their responsibility towards other stakeholders, in particular mainstream users such as SMEs and consumers.
- A duty of care throughout the product's lifecycle. The smart products put on the market should be developed and designed in accordance with relevant recognised standards. Supply-side actors should timely and effectively manage the digital security vulnerabilities in their products during their commercial life, and implement a responsible EOL policy.

The duty of care should be proportionate to the context and stakeholders' ability to act, in particular in relation with other code owners.

The principle of duty of care can be broken down in five sub-principles: security-by-design, security-by-default, dynamic management of digital security, responsible EOL policies and the digital security of the organisation.

Assessing the effectiveness of the duty of care can be done through various means, depending on the risk level. For instance, the conformity of a product's design for lower risk categories could be done through self-assessment, while certification could be mandatory for higher risk categories (see chapter 4).

Security-by-design

At a high level, security-by-design could be defined as the principle and the practice of developing products with digital security in mind. Supply-side actors have a responsibility to build and sell products that meet minimum security requirements. Security-by-design requirements usually rely on both:

- Digital security features, for instance an update mechanism.
- Processes and policies developed by the supply-side actors, for instance a vulnerability disclosure policy.

To achieve security-by-design, supply-side actors should:

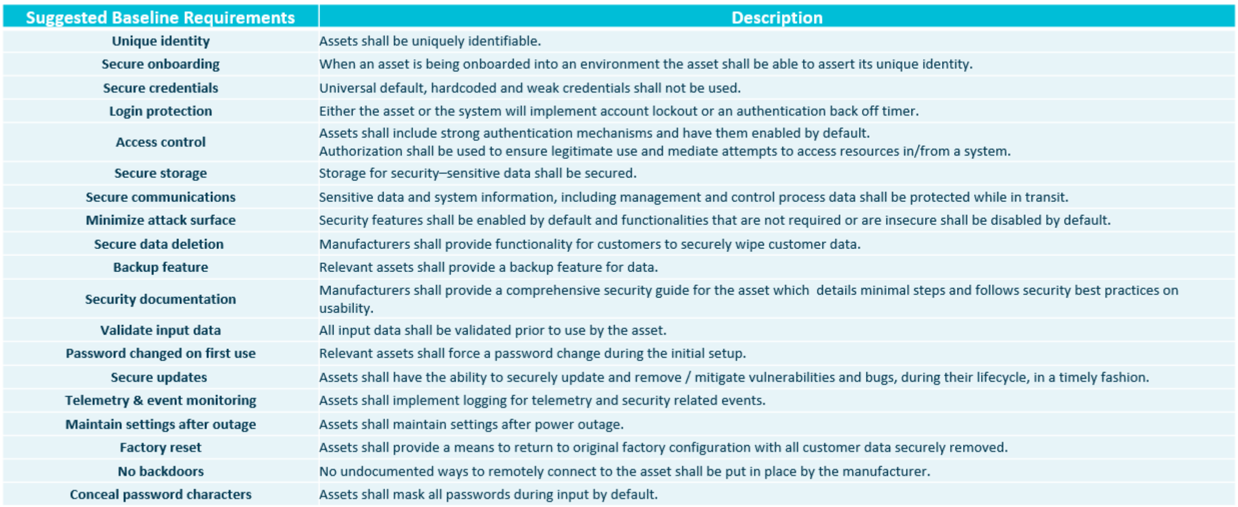
- Integrate digital security at every stage of the product's development, starting from its design and ending with its release, as opposed to adjusting or adding security features afterwards.
- Adopt a risk-based approach and assess how their products may pose digital security risks to their end-users, e.g. with use-case scenarios, threat modelling and penetration testing.
- Define security requirements and metrics in accordance with the findings of the risk assessment.
- Take into account the "state of the art" to make sure their products do not pose unreasonable risks for their end-users. To do so, they should follow security-by-design methodologies, which can be

available as industry standards or as product development guidelines,[18] and usually include the following high-level principles.

- **Product identity management**: products should have unique identifiers.
- **Testability and auditability**: products should be easily testable, for instance by reviewers or certification bodies. "Security-by-obscurity" should be avoided.
- **Attack surface minimisation**: unused software features and network ports should be closed. Software should run with least necessary privileges, taking account of both security and functionality.
- **Appropriate access control**: the scope of access should be tailored to specific user and privilege categories, based on the least-privilege principle, and credentials policy should follow best practices. For instance, remote access to administrator functions should be only authorised for users that have been authenticated through sufficiently strong procedures[19] (e.g. strong passwords defined by the user, as opposed to factory defaults).
- **Updatability**: all code components in a product, including firmware, should be easily and securely updatable.[20]
- **Resilience**: to the extent possible, smart products should to be able to function properly with minimal connection or without a connection[21] (Schneier, 2018[10]). Software should be designed to "fail safe" and a "fall-back framework" should be provided in case the connection is lost. More broadly, smart products should be designed to withstand, recover from, and adapt to adverse conditions, stresses or digital security attacks.
- **Data protection**: data should be protected according to their sensitivity, e.g. strong cryptography to protect credentials and personal data. Personal data processing should comply with applicable regulation.

Figure A A.1 and Figure A A.2 provide examples of two initiatives aiming to list key requirements to ensure that smart products are secured by design.

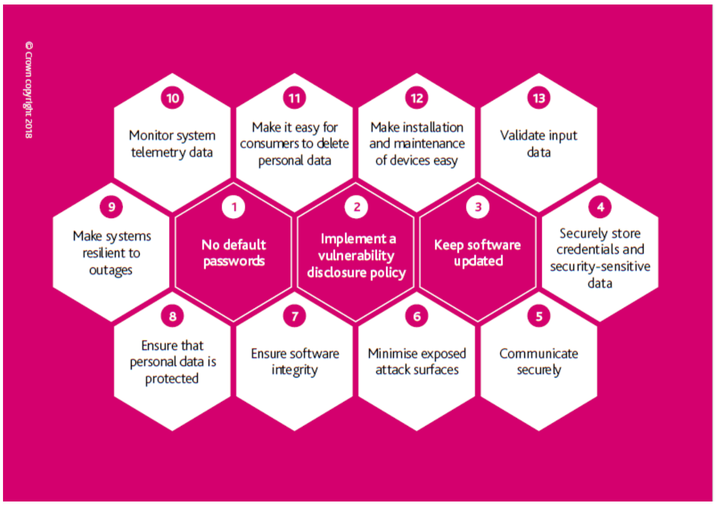
Figure A A.1. Draft baseline requirements for principle 3 of the Charter of Trust



Suggested Baseline Requirements	Description
Unique identity	Assets shall be uniquely identifiable.
Secure onboarding	When an asset is being onboarded into an environment the asset shall be able to assert its unique identity.
Secure credentials	Universal default, hardcoded and weak credentials shall not be used.
Login protection	Either the asset or the system will implement account lockout or an authentication back off timer.
Access control	Assets shall include strong authentication mechanisms and have them enabled by default. Authorization shall be used to ensure legitimate use and mediate attempts to access resources in/from a system.
Secure storage	Storage for security–sensitive data shall be secured.
Secure communications	Sensitive data and system information, including management and control process data shall be protected while in transit.
Minimize attack surface	Security features shall be enabled by default and functionalities that are not required or are insecure shall be disabled by default.
Secure data deletion	Manufacturers shall provide functionality for customers to securely wipe customer data.
Backup feature	Relevant assets shall provide a backup feature for data.
Security documentation	Manufacturers shall provide a comprehensive security guide for the asset which details minimal steps and follows security best practices on usability.
Validate input data	All input data shall be validated prior to use by the asset.
Password changed on first use	Relevant assets shall force a password change during the initial setup.
Secure updates	Assets shall have the ability to securely update and remove / mitigate vulnerabilities and bugs, during their lifecycle, in a timely fashion.
Telemetry & event monitoring	Assets shall implement logging for telemetry and security related events.
Maintain settings after outage	Assets shall maintain settings after power outage.
Factory reset	Assets shall provide a means to return to original factory configuration with all customer data securely removed.
No backdoors	No undocumented ways to remotely connect to the asset shall be put in place by the manufacturer.
Conceal password characters	Assets shall mask all passwords during input by default.

Note: These are the baseline requirements requested for the "Security-by-default' principle by the Charter of Trust. However, these characteristics are closer to the definition of "Security-by-design" in the context of this report.
Source: Charter of Trust, 2020.

Figure A A.2. Code of Practice for Consumer IoT – Secure by Design


© Crown copyright 2018
10 Monitor system telemetry data
11 Make it easy for consumers to delete personal data
12 Make installation and maintenance of devices easy
13 Validate input data
9 Make systems resilient to outages
1 No default passwords
2 Implement a vulnerability disclosure policy
3 Keep software updated
4 Securely store credentials and security-sensitive data
8 Ensure that personal data is protected
7 Ensure software integrity
6 Minimise exposed attack surfaces
5 Communicate securely

Source: Secure by Design Report (DCMS, 2018[8])

Security-by-default

At a high level, security-by-default can be defined as a situation where supply-side actors take an appropriate level of responsibility for managing the digital security of their products, and do not shift this responsibility to end-users. The ultimate objective of this principle would be to make it easy for end-users to do the right thing, hard to do the wrong thing and almost impossible to do the catastrophic thing.

Supply-side actors should circulate products with default values that provide appropriate security, and rely as little as possible on end-users to manage the digital security gaps of their products. In particular, supply-side actors should:

- Pre-configure and activate security features by default, as opposed to an “opt-in” approach. For instance, a messaging application should automatically encrypt communications, instead of letting users choose to activate or deactivate this option. Connected devices should require end-users to set strong passwords at first use, as opposed to letting them keep the default password indefinitely. MFA (a system that requires the use of both a password and an additional authentication method) could also be integrated as a default setting on smart products, as recent research suggests that it could “prevent 96% of bulk phishing attacks” (Cyberspace Solarium Commission, 2020[47]). The European Standard adopted by ETSI (2020[19]) also recommends the use of MFA to increase digital security for consumer IoT products.
- Provide a comprehensive yet simple security configuration guide that employs minimal steps and follows security best practices on usability. Support could be available on demand to assist end-users in configuring their products.
- Provide users with free and automatic security updates during the product’s commercial life, distinguished from other functionality updates. Advanced users could choose to opt out from automatic updates and test them before deployment. In case of automatic updates, users should be notified of the deployment.

Importantly, the principle of security-by-default should be applied differently for each category of users. Advanced users should have the possibility to opt out from secured defaults if they wish, e.g. to test the updates before implementation, have more control on the process and decide on other digital security settings according to their own risk assessment.

Finally, as noted in section 3.3.1, there is a need for stakeholders to clarify roles and responsibilities for supply-side actors and users. Responsible supply-side actors need to communicate such information to their customers in an effective manner, for instance through the use of a responsibility control matrix

Dynamic management of digital security

Supply-side actors and other code owners have a duty of care to maintain the digital security of the products they put on the market throughout their commercial life. In particular, they should:

- Continually monitor for, identify and mitigate security vulnerabilities in their products during their commercial life.[22] If the vulnerabilities are managed by another code owner, they should notify the party best placed to mitigate them.
- Adopt a clear and public co-ordinated vulnerability disclosure policy, which should indicate a public point of contact so that researchers can report vulnerabilities.
- Adopt a vulnerability handling process (see the vulnerability treatment report (OECD, 2021[4])) and rely on risk management to determine which vulnerabilities should be prioritised.
- Incentivise third-parties such as security researchers to identify and disclose security vulnerabilities in their products (see the vulnerability treatment report (OECD, 2021[4])).
- Communicate with customers about security updates and risks related to newly discovered vulnerabilities.
- Provide and deploy timely updates, on a regular or *ad hoc* basis. Typical update cycles range from seven to ninety days, though this may vary greatly depending on the nature of the product. This should be balanced with the need, in some cases, to test and deploy security updates progressively.
- Adopt a clear incident response process, including strategies, attack detection mechanisms, training, communication and risk management teams.
- Separate security updates from functional updates, or upgrades (ETSI, 2020[19]).
- For mainstream users, provide automatic and free security updates (ETSI, 2020[19]).
- Furthermore, there may be a need to make security updates for critical vulnerabilities automatic for all users.
- However, advanced users should be able to opt out from automatic updates (for non-critical vulnerabilities), as they may value privacy and control (e.g. in complex industrial environments that may be disrupted by automatic patching).
- Figure 3.3 provides an example of possible update practices based on user categories.

Importantly, the dynamic management of digital security should be holistic, and take into account all components of the product's ecosystem.

Responsible EOL policies

Supply-side actors and other code owners have a duty of care to maintain the digital security of the products for a reasonable period corresponding to the expected length of use of the product, and ensure their repairability (i.e. the ability to maintain a product).

The first section proposes universal basic rules that could apply to all smart products. The following sections explore possible options to manage the EOL gap. Each option may be more suitable for certain categories of products or within specific contexts. However, there is a need for supply-side actors to choose at least one of these options to address the EOL gap effectively. Therefore, in line with the proportionality principle (section 3.6), a gradual approach could be followed. For instance, supply-side actors could be incentivised to provide extended support for a fee, or to enable users to upgrade for free or for a discount.

In case they do not, then they could be compelled to enable other stakeholders to be responsible to maintain the product, for instance by transferring intellectual property rights and design information to the user or open-source community. Such gradual approach could also benefit from analysing the specific dynamics and negotiating power within each market: in case there is a lack of interoperability or competition, more compelling policies could be put in place (see section 3.5).

Reasonable and transparent length of support

To the extent possible, supply-side actors and other code owners should:

- Design and implement a clear and transparent EOL policy for their products;
- Publicly state the minimum length of time for which a product will receive software updates, the reasons for the duration of the support period and the envisioned EOL period;
- Determine the EOL on the basis of the date of end-of-sale (EOS, last purchase through official vendors) as opposed to the date of general availability, allowing for a reasonable time period between EOS and EOL.

Duty of care after the EOL

To the extent possible, supply-side actors and other code owners should:

- Monitor the use of their products after their EOL and provide, upon request, relevant data to the regulator (e.g. number of products still in use after EOL);
- Under certain circumstances, continue to ensure duty of care after EOL. If critical vulnerabilities are discovered in EOL products that are still widely in use and are likely to pose unreasonable risks for end-users[23] in case of exploitation, including safety risks, supply-side actors have a duty of care to either i) provide security updates or fixes or ii) enable other stakeholders to mitigate these risks (see above). This principle could be applied only to certain products, e.g. entailing "systemic" risks (see Annexes);
- Under certain circumstances, terminate or disconnect products when they reach their EOL[24]. However, this would come with significant down-sides in terms of consumer rights, fair business practices and e-waste generation. In the United States, draft laws banning the use of such "kill-switches", as unsafe and unfair business practices, have been introduced in several States (Povich, 2018[35]). This solution seems also dangerous regarding liability, and does not address the power asymmetry between supply and demand.

Repairability

Supply-side actors and other code owners should not be expected to maintain the digital security of their products indefinitely. However, these reasonable limitations to their duty of care should not prevent other stakeholders from taking responsibility. As a result, when a product has reached its EOL, supply-side actors and other code owners should put in place, for example, one of the following strategies:

- Incentivise end-users to stop using a product when it reaches the end of its commercial life, for instance through EOL notifications, and discounted or free upgrades;
- Enable third-parties (e.g. advanced users or the open-source community) to maintain the product, for instance through source code escrow[25] or transferring proprietary design information and rights, including credentials for security updates, directly to trusted stakeholders (Zittrain, 2018[36]; NIST, 2016[37]).

The repairability principle should also be considered in relation to the environmental impact of EOL products. Digital security should be balanced with other important policy objectives, such as the need to reduce e-waste (see SDG 12). Repairability can also be approached as a means to ensure resilience, as defined in section 3.3.2. In the United States, some draft laws promoting a “right to repair” for smart products have been introduced in several States (Gartenberg, 2018[38]).

Digital security of the organisation

The duty of care of supply-side actors for the digital security of the products they put on the market should be approached holistically.

Beyond the digital security of the product, there is a need to ensure the digital security of the organisations that are part of the product’s value chain. Even though a product meets security-by-design and security-by-default requirements, it may be compromised through the networks of the manufacturer or of other code owners. The NotPetya malware in 2017 showed how update mechanisms could be compromised to insert malware in products.

Therefore, supply-side actors should put in place strategies to ensure they meet a satisfactory level of digital security for their organisations. These actors should be incentivised to follow international standards such as ISO 31000. Adherence to such standards can be demonstrated by conformity assessments and certifications (see section 4.5).

Co-operation and governance

Increasing co-operation and developing effective governance are key to better allocate responsibility and realign market incentives.

For governments, policy tools to increase co-operation include multi-stakeholder partnerships, *ex ante* requirements and *ex post* mechanisms.

To manage digital security risks, all stakeholders should co-operate, including across borders (OECD, 2015[5]). For the digital security of products, four areas of focus are important to increase co-operation in an effective manner:

- Between code owners across the product’s value chain;
- Between stakeholder groups and across sectors;
- Between regulators and across the whole government;
- At the international level.

Increasing the co-operation of code owners across the value chain

The value chain of smart products is often complex. Smart products are usually made of multiple components and various code layers, which can be developed by a wide range of actors, from open source communities and independent developers to corporations, including both digitally mature companies and SMEs that may have limited technical resources. In addition, smart products are usually part of a wider ecosystem, which involves many actors such as network operators, cloud providers and large ICT companies.

The digital security of products may be impacted by vulnerabilities from any code layer, any component and any part of the ecosystem. Consequently, co-operation across code owners is key to enhance the effectiveness of identifying and mitigating digital security gaps.

There should be a clear allocation of responsibility for each component and code layer of the product. Technical and organisational measures should be in place to facilitate co-operation between code owners (e.g. security bulletins, procurement guidelines throughout the value chain).

In the context of industrial IoT, trustworthiness, i.e. the ability of suppliers to meet the expectations of a contract partner in a verifiable way, is key to increase co-operation of stakeholders across the value chain. To build trustworthiness, there may be a need to develop new technical tools (e.g. unique digital identities for processes, products and organisations) and incentivise the use of digital certificates and certification / conformity assessments (PI4.0 & RRI, 2020[39]).

For each product, an institutionalised coordinator could facilitate the identification of code owners and their co-operation. Depending on the context and the product, the coordinator may be the vendor, the manufacturer, a third-party (e.g. the network operator or the operating system designer) or a government agency.

Multi-stakeholder co-operation

Co-operation should also involve actors within the broader ecosystem. In particular, co-operation mechanisms should include:

- Security researchers, for instance through bug bounties and vulnerability disclosure policies;
- Competitors within the same sector, for instance through information sharing and analysis centres (ISACs) and sector or product-centred Computer Emergency Response Teams (CERTs);
- Stakeholders across sectors, for instance through forums gathering various ISACs and CERTs;
- Other stakeholder groups, such as consumer associations.

Governments should, to the extent possible, involve all relevant stakeholders when they design and implement policy tools aiming to enhance the digital security of products.

Whole-of-government approach

The development of the IoT and other emerging technologies raises challenges that spread across policy silos. More and more, the products that entail safety risks are becoming “smart”. For instance, IoT products are becoming more and more common in healthcare and transportation, while raising concerns regarding safety and privacy. For many smart products, there is increasingly an overlap between sectoral regulators (finance, health, automotive…), horizontal authorities (consumer product safety, competition, data protection, liability…) and authorities in charge of digital security. If not properly anticipated and managed, this may result in inconsistent and potentially contradictory recommendations for the industry, or conflicts between institutions.

To address this issue, it is fundamental that policy makers develop a whole-of-government approach to the digital security of products, and make sure that the development, application and evaluation of the policy response are coherent and involve all relevant public actors. This holistic approach should involve all relevant government agencies, including agencies in charge of horizontal regulations (e.g. privacy, consumer protection) and institutions in charge of sectoral regulations (e.g. health, banking).

International co-operation

Initiatives or rules developed nationally may not be sufficient to have a significant impact on the digital security of products. In fact, the market for smart products is increasingly global, both from a supply-side perspective and from a demand-side perspective. The value chain of smart products often involves many actors from various jurisdictions, and supply-side actors often circulate their products across many countries. The case of botnets further exemplifies how more international co-operation is needed to address digital security vulnerabilities in globally used products, as the targets of DDoS attacks and the infected computers enrolled in botnets are often located in different countries.

In the United States, a report recently highlighted the need to design and enforce "a system of norms, built through international engagement and cooperation", for instance through "a coalition of like-minded allies and partners willing to collectively support a rules-based international order in cyberspace" (Cyberspace Solarium Commission, 2020[12]). International cooperation may also be needed to facilitate the identification of and information sharing regarding vulnerabilities[26] in smart products, and regarding the status of security updates for products that are widely used globally.

From the industry's perspective, the fragmentation of regulatory requirements across OECD countries also represents a significant challenge. The need to assess the conformity of products with many guidelines and standards, in particular through third-party certification, incurs significant costs.

Consequently, policy makers should seek to increase international co-operation and agree on common terminology and strategies where applicable. Another important aspect to take into consideration is the importance of interoperability between legal frameworks (see section 4.8).

Innovation and competition

Promoting innovation and competition is key to realign market incentives towards optimal outcomes and to enhance the overall level of digital security for smart products.

For governments, policy tools to promote innovation and competition include *ex ante* requirements, labels, *ex post* mechanisms and public procurement. Other tools can also be used, but they go beyond the scope of this report (e.g. competition law).

Digital security and innovation

The *Digital Security Risk Management Recommendation* (OECD, 2015[17]) recognised that "leaders and decision makers should ensure that innovation is considered" (OECD, 2015[17]). The relationship between innovation and digital security is complex (OECD, 2020[40]). Innovation is key to develop new architectures and technical standards that are likely to raise the level of digital security of products. In the same time, market incentives often lead innovators to favor time-to-market and usability over digital security concerns. Unnecessary and disproportionate digital security requirements (e.g. legacy regulations) may also be considered as a barrier to innovation and may limit the ability of stakeholders to fully reap the benefits of digital transformation (see section 3.6).

Promoting innovation entails recognising that product development is an iterative process. Innovation goes hand in hand with a certain tolerance to mistakes and failures. However, these mistakes and failures can only be tolerated within a certain framework. They should be addressed in a timely manner, responded to, and enable stakeholders to learn and improve.

For policy makers, the challenge is to strike the right balance between:

- Ensuring a duty of care for supply-side actors, in order to protect mainstream users from unreasonable risks;
- Allowing for iterations and mistakes, which are an inherent part of innovation.

To overcome this challenge, it is essential to define clear responsibilities, and allow for a lift of responsibility (or "safe harbour") only in a specific context. Regulatory sandboxes are an example of innovative policies enabling innovation in a responsible manner (OECD, 2020[41]). For product developers, leveraging communities of early adopters and advanced users to test and improve products can also be a key element in order to balance innovation with responsibility.

Importantly, recognising the importance of iterations should not be understood as a dismissal of the importance of security-by-design and security-by-default guidelines. To the contrary, the innovation principle also highlights the need for supply-side actors to develop their products with effective and up-to-date technical means. Their digital security measures should take into account the "state of the art".

Digital security and competition

In the context of smart products, competition is also a key element that could enable stakeholders to choose from a wide range of products and select the products that are the most appropriate, according to the context and their preferences.

A suboptimal level of competition in a given market may generate an asymmetry of powers between stakeholders. The lack of substitutability of certain smart products may limit the negotiating power of customers, and lead to unfair business practices (e.g. regarding the EOL, see section 3.3).

Therefore, the assessment of the level of competition in the given market is key to determine the level of regulatory requirements to enhance the digital security of products. In line with the proportionality principle, policy makers could follow a gradual approach: encourage voluntary frameworks if the level of competition is high, and consider developing more stringent requirements through ex ante and ex post mechanisms if the level of competition is low, and if business practices do not lead to satisfactory results regarding the duty of care of supply-side actors.

Proportionality and risk management

Proportionality and risk-based approaches are key to take into account the complexity of smart products (see section 2.1.1) and ensure that technical and policy measures to increase digital security are adapted to the context (e.g. product category, use-case, threats…).

Although digital security measures aim to protect economic and social activities, they can also inhibit them by increasing costs, reducing performance and altering the open and dynamic nature of the digital environment, which is essential to realising the full benefits of the digital transformation. Therefore, it is key to determine if digital security measures, and policy tools aiming to enhance digital security, are proportionate.

The *Digital Security Risk Management Recommendation* (OECD, 2015[17]) states that stakeholders "should ensure that digital security risk is treated on the basis of continuous risk assessment". More broadly, a risk-based approach involves evaluating risks on the basis of their probability and severity, based on the context (i.e. risk assessment), and addressing these risks by deciding to accept, mitigate, transfer or avoid them (i.e. risk treatment).

The *Digital Security Risk Management Recommendation* (OECD, 2015[17]) also states that security measures should be "appropriate to and commensurate with the risk", or, in other words, "proportionate". Proportionality can be defined as the principle of balancing the means used with the intended aims. This balancing exercise requires to evaluate the potential benefits of an action as well as their potential negative consequences, usually through impact assessment. Importantly, such evaluation should integrate the negative consequences of inaction[27] and the impact on all relevant stakeholders[28].

The digital security of products is a complex area (see section 2.1.1), which spans across various sectors (or "verticals") and policy areas. In particular, the heterogeneity of smart products and the context-dependence of risk levels make one-size-fits-all approaches unlikely to succeed. Consequently, the use of policy tools should be adapted to each situation, and the responsibility of stakeholders should take into account their ability to act (OECD, 2015[5]).

This complexity, however does not preclude the need for and relevance of baseline requirements for all smart products (e.g. updatability), while recognising the possibility of exceptions[29], and the need for further requirements for specific product categories or contexts of use, e.g. critical activities (OECD, 2019[42]). To implement the proportionality principle in a practical manner, it is therefore important to use on maturity models (NIST, 2018[43]) and tiered or multi-layered approaches (see section 4.7.2), rather than binary models.

The definition of relevant thresholds is complex, and would require co-operation between stakeholders, across the government and at the international (see section 3.4). Some initiatives are already underway and may provide useful insights on how to define these thresholds, for instance through developing specific requirements for certain sectors or certain categories of products, e.g. with safety risk (see the labelling schemes in Japan in section 4.7.2).

Another important aspect of proportionality is the need for balance. In particular, stakeholders should strive to balance:

- The high-level principles themselves, as they may be conflicting with one another in certain cases, e.g. innovation and duty of care.
- Digital security with other important public policy goals, e.g. the openness of the Internet and emerging technologies, as well as fundamental values such as privacy (OECD, 2015[17]). In that regard, policies to enhance the digital security of smart products shall also ensure that personal data collection and processing meet applicable legal requirements (e.g. purpose limitation, data minimisation, etc.).
- The interests of various stakeholders and communities.

Annex B. **Detailed policy toolkit**

This Annex contains a detailed version of the policy toolkit developed in chapter 4. It intends to explore the broad spectrum of policy options available for governments to enhance the digital security of products. The policy tools described below aim to address the key challenges (see chapter 2) and foster the adoption of the high-level principles (see chapter 2.2) discussed above.

Raising awareness and developing digital security skills

Policy makers can raise awareness on digital security risk through media campaigns and education programs on basic skills for digital literacy. They can also support the development of a workforce with advanced skills by promoting digital security in curricula for schools, university and retraining programs. These tools are important to raise awareness for mainstream users, empower advanced users and support innovation.

Benefits, risks and limits

For governments, raising awareness of digital security risk and developing digital security skills form the basis of any strategy to enhance the digital security of products. Without an appropriate level of awareness and skills, any effort to increase transparency may fall short of its objectives, as stakeholders may not be able to leverage additional information into meaningful decisions. To be more effective, programs to raise awareness and develop skills can leverage multi-stakeholder co-operation (see sections 3.4 and 4.4).

An important advantage of policy tools that raise awareness and develop digital security skills is that they carry no risk of distorting the market, of disproportionate use or of a negative impact on other stakeholders.

However, the use of awareness-raising and education policy tools alone would likely not be sufficient to address the challenges identified in chapter 2. In fact, it is unrealistic to expect mainstream users such as consumers and SMEs to become digital security experts or leverage resources similar to those of large companies. Other policy tools are necessary to increase transparency and empower mainstream users to make informed decision, e.g. labels and conformity assessments. In addition, in many cases, the parties that are the most able to act to enhance the digital security of products are actors within the supply-side. Consequently, awareness raising campaigns should not be considered as a way to lift producers from their duty of care, in particular regarding security-by-default.

Finally, awareness-raising campaigns should not be the primary tool to ensure the conformity of products with basic minimum requirements. Mainstream users should not be put in a situation where they can purchase products that pose unreasonable risks. For instance, one would not expect a government-backed awareness-raising campaign to advise consumers to only buy cars that are equipped with brakes. Similarly, mainstream users expect the government to ensure that basic digital security features are imposed upon producers of smart products through regulatory requirements.

Discussion of relevant programs across OECD countries

In the European Union, the Cyber Security Month is organised every year in October. Stakeholders from various EU countries participate, for instance by sharing resources and advice, organising conferences and webinars, providing training and publishing press releases. The aim is to raise awareness of digital security threats, promote digital security among citizens and organisations and equip mainstream users with resources to protect themselves online. In 2019, the European Union Agency for Cybersecurity, ENISA, focused its campaign on the key questions consumers should ask before purchasing new smart products (Figure 4.2).

While not developed by governments, the website “have I been pwned?” (https://haveibeenpwned.com/) offers another perspective on awareness-raising. The name derives from “script kiddie” jargon term "pwn", which means to compromise or take control, specifically of another computer or application. Created by digital security expert Troy Hunt in 2013, this website could be described as an “*ex post*” (i.e. after a digital security incident) awareness-raising initiative that allows Internet users to check whether their personal data has been compromised by data breaches. The service collects and analyses hundreds of public databases containing information about leaked accounts, and allows users to search for their own information by entering their username or email address. Users can also sign up to be notified if their email address appears in the future in the databases scanned by the tool. In 2019, the website had on average one hundred and sixty thousand daily visitors, as well as three million active email subscribers. This shows how innovative data-mining and communication tools can be developed to raise awareness, sometimes with more effectiveness than traditional approaches.

From a supply-side perspective, producers need a trained workforce to raise the level of digital security of the products they design and develop. However, while many academic institutions, coding boot camps and job retraining programs teach code development, they do not always equip their graduates with digital security education (DHS and DoC, 2018[7]).

For governments, facilitating the development of digital security skills at the national level is key to enable the emergence of a skilled workforce and a vibrant technical community. Mainstreaming advanced digital security skills in engineering, coding, and integrating digital security in more general curricula (e.g. management, legal) should be a key objective for policy makers in OECD countries. More broadly, governments should promote and support clear and attractive academic and career paths for digital security professionals. In the United States, a report recently recommended to mainstream in school curricula more general cognitive skills, beyond basic digital literacy, such as “critical thinking and problem-solving skills, information on implicit vs. explicit messaging, and technology concepts”, in order to better enable individuals to protect themselves against phishing campaigns (Cyberspace Solarium Commission, 2020[12]). Supporting the technical community (e.g. through social recognition, funding or co-operation) could also be effective to leverage the untapped potential of the security researchers community.

The role of governments as economic agents

Beyond their role as regulators, governments are also economic agents. In this role, they need to lead by example and can leverage public procurement to shape market incentives towards more optimal outcomes.

Benefits, risks and limits

The role of governments as economic agents is often neglected, as public attention focuses on their role as regulators. However, as customers of smart products, governments can significantly impact the behaviour of other economic agents and shape market incentives towards more optimal outcomes. This policy tool can be effective in mainstreaming best practices for duty of care, in particular in markets where government is a significant customer. Similarly, leading by example is key to support a government’s policy objectives. On the contrary, a lack of consistency between a government’s policy objectives and its own behaviour may severely impact its credibility, and *in fine*, the adherence of stakeholders to other policy tools.

The advantage of leveraging public procurement is that it carries a low risk of distorting the market or having wide-ranging consequences, unlike *ex ante* regulations. However, it carries a moderate risk of disproportionate use, in case the requirements set by the public procurement policies are too high or drafted in a way that could be considered as discriminatory. Currently, most digital security requirements for public procurement in OECD countries focus on organisational aspects rather than on product features.

Resorting to public procurement only will likely not be sufficient to address the challenges identified in chapter 2. Some product categories (e.g. consumer IoT) may not be significantly impacted by a change in public procurement policies, as government is often not a significant customer in these markets. In addition, such policies could send mixed signals to the industry, suggesting that lower requirements are not acceptable for public procurement while being acceptable for mainstream users.

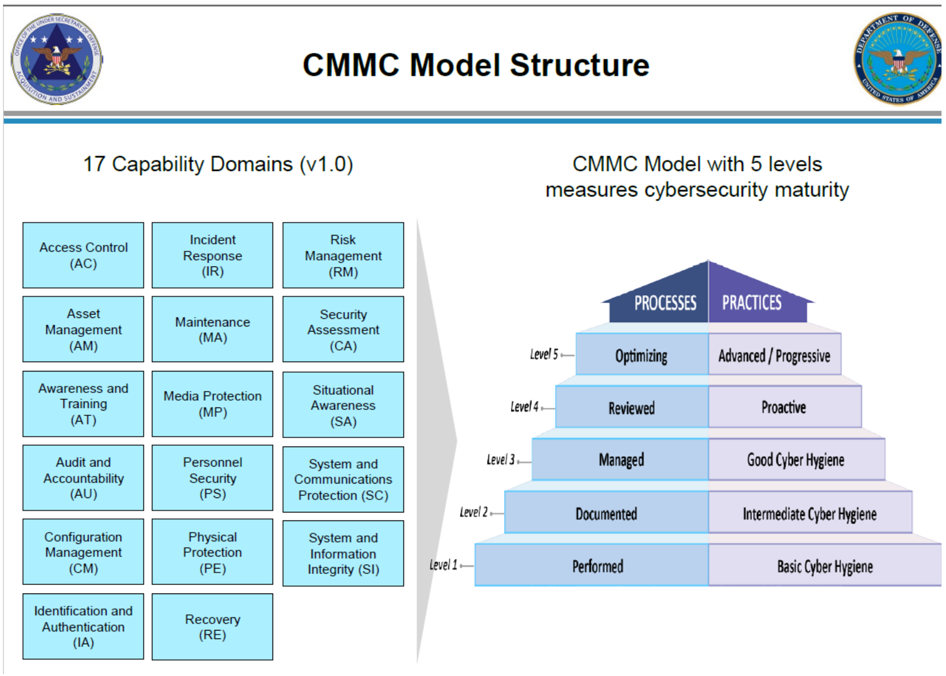
Discussion of relevant programs across OECD countries

As economic agents, governments need to lead by example regarding their digital security risk management practices. For instance, government entities at all levels (including both national and local) should integrate the need to dynamically address digital security risk, through the timely deployment of security updates, and taking into account the EOL of the products they use.

Policy makers can also support demand for products with a higher level of digital security by requiring producers and contractors to meet certain requirements to be able to bid for public procurement. These requirements can be aligned with recognised industry standards or international standards (e.g. ISO).

In the United States, the Department of Defense (DOD) released in 2020 (Bakies et al., n.d.[62]) a Cyber Maturity Model Certification (CMMC), which combines various digital security standards and best practices, and maps their controls and processes across several maturity levels, aiming to reduce risk against a specific set of digital security threats. By 2026, all companies that wish to bid for a contract with the DOD will be required to be certified through this scheme. The DOD only allows accredited third-parties to deliver this certification. The CMMC encompasses five maturity levels that ranges from "Basic" to "Advanced/Progressive" (Figure A B.1).

Figure A B.1. CMMC Model Structure



CMMC Model Structure

17 Capability Domains (v1.0)

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

CMMC Model with 5 levels measures cybersecurity maturity

	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced / Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

Note: Version released in January 2020.
Source: United States Department of Defense.

In a recent report, other agencies in the United States suggested to require all vendors bidding for public procurement for ICT products to certify their products through recognised standards (DHS and DoC, 2018[7]). A draft law, the "IoT Cybersecurity Improvement Act" (Kovacs, 2020[47]), currently examined by the US Congress, proposes to require the federal government to only purchase IoT products that are compliant with relevant standards developed by NIST, e.g. (2020[18]). The enforcement of such law would also require the development of certification programs to assess the conformity of IoT products with the above-mentioned standards (see section 4.6).

In the United Kingdom, all organisations that bid for central government contracts that involve handling personal information and providing certain ICT products must comply with the "Cyber Essentials" digital security scheme since 2014. The scheme applies for all organisations, in all sectors and of all sizes. There are two levels of assessment, Cyber Essentials and Cyber Essentials Plus:

- Cyber Essentials is awarded on the basis of self-assessment, undertaken through a questionnaire that needs to be approved by a senior executive such as the organisation's CEO. The decision to award the scheme is made by an independent third-party after reviewing the questionnaire.
- Cyber Essentials Plus requires a certification by an independent third-party, through remote and on-site vulnerability testing.

Beyond technical measures and certification, governments may integrate in their public procurement policies the need for diversification when acquiring smart products. Such requirements could have a positive impact on competition and innovation (see section 3.5) and address potential risks associated with lock-in effects and dependency to certain companies in strategic areas.

Facilitating multi-stakeholder partnerships

Policy makers can facilitate multi-stakeholder partnerships, i.e. coalitions of actors from various communities that aim to enhance the digital security of products. These tools are important to increase co-operation, support innovation and enable certain stakeholders to take more responsibility.

Benefits, risks and limits

Facilitating multi-stakeholder partnerships is a key policy tool for governments in order to address externalities and gaps that one actor alone would not be able to fix. These partnerships are instrumental in order to build trust, facilitate dialogue and co-operation and better align incentives across the value chain. The advantage of multi-stakeholder partnerships also lies in their agility, and their ability to leverage resources and talent from a wide range of actors. Governmental facilitation can take various shapes, e.g. financial and institutional support, or a more strategic role in gathering the relevant parties, defining objectives and facilitating consensus.

Multi-stakeholder partnerships carry little risk of distorting the market or negatively affecting other stakeholders, as they rely on voluntary co-operation. As they are not a regulatory tool, they carry little risk of a disproportionate use.

However, resorting to multi-stakeholder partnerships only will likely not be sufficient to address the challenges identified in chapter 2. First, these partnerships rely on voluntary commitment. Even though peer pressure can often be an effective way to influence behaviour, they will not have the wide-ranging effects of regulatory instruments. While it is often easy for stakeholders to agree on common values, it is more difficult to agree on common rules, in particular when trade-offs have to be made between public interest and corporate objectives or individual preferences. .

Operational partnerships: ISACs, CERTs and other initiatives

Multi-stakeholder partnerships can take the form of sector-specific coalitions aiming to share information and best practices for digital security risk management. These coalitions are often institutionalised through Information Sharing and Analysis Centres (ISAC). For instance, the Aviation ISAC (A-ISAC) provides an aviation-focused information sharing and analysis function to help protect global aviation businesses, operations and services (OECD, 2019[1]). Sector-based ISACs can also cooperate at the national level, for instance through a national council of ISACs ((n.a.), 2021[63]). Sectoral Computer Emergency Response Teams (CERTs) can also be considered as a good practice to facilitate information sharing between stakeholders within a trusted partnership.

In the United States, a recent report suggested that "Internet service providers and their peering partners should expand current information sharing to achieve more timely and effective sharing of actionable threat information" to enhance the digital security of IoT products, in particular to tackle the issue of botnets (DHS and DoC, 2018[7]). Such enhanced partnerships have been implemented in other countries. For instance, the Dutch Government (2018[64]) has launched an initiative to monitor and enhance the digital security of connected devices. The goal is to share information across supply-side actors as well as with end-users, so that product distributors can consider removing products from the shelves and consumers be incentivised to patch or deactivate their products if critical vulnerabilities are discovered. The partnership involves a variety of actors:

- A Dutch nonprofit association of internet service providers, Abuse Information Exchange (AIE), tracks infected IoT devices and transmits information to Internet Service Providers (ISPs).
- The Delft University of Technology (TU Delft) assesses the infection rate for IoT devices in the Netherland, based on the data collected by AIE.
- The Digital Trust Center, part of the ministry of Economic Affairs, explores short-term measures that manufacturers and other stakeholders could implement to secure infected devices.
- Internet service providers notify their customers so they can clear infected devices.

Other governments in the OECD have funded and/or facilitated the development of multi-stakeholder partnerships to tackle the issue of botnets. Examples include "*botfrei*" in Germany and "NOTICE" (*National Operation Towards IoT Clean Environment*) in Japan. In Japan, the government has modified existing law to allow the NICT (*National Institute of Information and Communications Technology*) to survey IoT devices to assess password vulnerabilities. The results are transmitted to Internet service providers (ISPs), which then contact users and issue alerts. Users can reach a support centre at the Ministry of Internal Affairs and Communications (MIC), which provides them with guidance for appropriate digital security measures. These initiatives are considered by many experts as key, as they address the negative externalities often associated with smart products (see section 2.1.2) and tend to mainstream ownership of digital security risk (see section 3.3.1).

Strategic coalitions: committing to shared objectives at a high level

Beyond operational partnerships, stakeholders can commit to enhance the digital security of products through high-level coalitions. Such multi-stakeholder partnerships can prove useful to signal institutional commitment, highlight critical issues, develop trust among partners and share best practices.

Charter of Trust

Founded in 2018 at the Munich Security Conference, the Charter of Trust gathers a number of leading global companies such as Siemens, Atos and Airbus. These companies all have different roles on the value chain, and bring the perspectives of both producers and corporate users of smart products. This initiative aims to mainstream digital security management best practices across the product value chain.

The signatories of the Charter of Trust intend to enhance the overall level of digital security of the products they are responsible for, in particular through demanding contractual policies with their suppliers. In particular, they commit to protect the data of individuals and companies, prevent damage to people, companies and infrastructures and create a reliable foundation on which confidence in a networked, digital world can take root and grow.

Cybersecurity Tech Accord

Similarly, the Cybersecurity Tech Accord, established in 2018, gathers many global companies, primarily from the ICT sector, such as Facebook, Microsoft and Cisco. These companies commit to protect their users and customers everywhere, oppose digital security attacks on "innocent citizens and enterprises", empower users, customers and developers to strengthen cybersecurity protection and partner with each other and likeminded groups to enhance digital security.

Paris call for trust and security

Launched in 2018 as well, the Paris Call for Trust and Security gathers more than 1100 stakeholders[30], including governments, the private sector and civil society organisations. The call promotes nine principles to enhance digital security in cyberspace, and invites all actors to co-operate to implement these principles.

Geneva Dialogue on Responsible Behaviour in Cyberspace

Launched in 2020, the Geneva Dialogue gathers some of the world's leading ICT companies such as Cisco, Huawei, Kaspersky, and Microsoft, as well as companies from other sectors such as Siemens and UBS. The dialogue enables global discussion on best practices that could be implemented to improve the digital security of products, and led to the publication of output documents (Geneva Dialogue, 2020[65]).

Issue-specific initiatives: fixing one problem at a time

Beyond operational partnerships and strategic coalitions, some initiatives have been launched to address specific issues that have a negative – and often considerable – impact on the digital security of products.

Google Project Zero

Launched in 2014, Google's Project Zero gathers a team of security researchers whose objective is to discover zero-day vulnerabilities in products that are widely relied upon by end-users around the world. The *modus operandi* of the team is to perform vulnerability scanning and testing on popular software like operating systems, web browsers and open source libraries. In the course its work, Project Zero has discovered zero-day vulnerabilities in the products of many other companies, including Apple and Microsoft. Upon discovery, Project Zero researchers follow a coordinated disclosure process where they inform the product's code owner before informing the wider public, with a maximum delay of 90 days between the discovery and the full disclosure. Other initiatives to facilitate co-ordinated vulnerability disclosure are discussed in the vulnerability treatment report (OECD, 2021[4]).

Software heritage

Launched in 2016 by INRIA, the national research centre on computer science in France, Software heritage is a multi-stakeholder initiative whose goal is to collect, preserve, and share software code – both freely licensed and not – in a universal software storage archive. Ultimately, the initiative aims to prevent the loss of cultural, technical, industrial and scientific knowledge that could result from software obsolescence in the coming decades or centuries. The project has been endorsed by many leading organisations such as

Creative Commons, the Free Software Foundation, GitHub, the Linux Foundation, and Microsoft. From a digital security perspective, the project could also empower stakeholders to maintain and repair products after they have reached their EOL.

Core infrastructure initiative (CII)

The core infrastructure initiative (CII) was founded in 2014, in the wake of the discovery of the Heartbleed vulnerability in the implementation of SLL protocols. The project was launched by the Linux Foundation and received support from many global companies, including Intel, Facebook, Cisco, Microsoft and Qualcomm. The initiative aims to address the suboptimal allocation of human and financial resources to maintain the digital security of open-source products that are widely used and critical to the functioning of the Internet. It can be considered as a public-interest mission addressing the risk of a "tragedy of the commons"[31] faced by open-source products, i.e. a situation where limited ownership rights for a resource results in suboptimal maintenance, even though the resource is widely used.

Industrial IoT value chain security

In Germany, the government has launched a multi-stakeholder partnership, "Platform Industrie 4.0" (PI4.0), gathering industry leaders, trade associations and academia, to facilitate the development of industrial IoT, defined as "the intelligent networking of machines and processes for industry with the help of information and communication technology". One of the working groups of this partnership focuses on the "security of networked systems". International co-operation, and the development of common understanding and norms, is at the core of this initiative. For instance, PI4.0 collaborated with the platform "Robot Revolution & Industrial IoT Initiative" (RRI) from Japan to identify the technical challenges faced by companies willing to trade with each other in the global market for industrial IoT. Both groups worked together to deliver a report which identifies key areas for further collaboration to increase trustworthiness for industrial IoT. These areas include the development and implementation of technical standards and solutions such as digital identities and certificates for, products and organisations (PI4.0 & RRI, 2020[39]).

Forward-looking: the need for more ambitious coalitions to address code vulnerabilities

Smart products belong to a global market. However, most vulnerability databases are developed at a national or regional level. Increased international co-operation on vulnerability registration could bring significant benefits for supply-side actors and end-users, accelerating and facilitating the process for vulnerability handling and management. The creation of a global registry for vulnerabilities, on the model of CVE, or of a portal enabling the co-operation of national and regional vulnerability registries, could therefore be explored.

From another perspective, there could be a need to "globalise" existing bug bounty initiatives. The suboptimal level of digital security of smart products enables digital security attacks, whose cost for society is immense. While it is difficult to measure this cost at a global level, common estimates consider that a reasonable range would be between 100 and 6 000 billion USD annually (WEF, 2020[66]). Compared to these costs, it could make sense, from a public policy perspective, to "buy" vulnerabilities in the most commonly used products pre-emptively, through a sort of global fund for bug bounties. This idea has been promoted by certain experts and security researchers (Frei, 2020[67]), as it would also enable stakeholders to address the issue of the grey and black markets for vulnerabilities (see the vulnerability treatment report (OECD, 2021[4])). Funding could come from governments, or from a general tax on supply-side actors, which produce and benefit from the sale of these products. This initiative could complement other initiatives (e.g. Google Zero, see above). However, this initiative focuses on the discovery of vulnerabilities, and would not address other issues such as the suboptimal deployment of security updates and the EOL gap. In addition, mainstreaming the use of security-by-design standards and guidelines could significantly reduce the number of vulnerabilities before products are released on the market.

Developing voluntary guidance and technical standards

Policy makers can develop voluntary frameworks and guidance to empower supply-side actors to enhance the digital security of products, or support the development of technical standards by other stakeholders (e.g. the industry) at the national and international levels. These tools can be defined as sets of principles or requirements that are proposed by the government or other institutions such as standardisation organisations.

Such guidance and technical standards are usually drafted through a multi-stakeholder process, and their implementation is undertaken on a voluntary basis. Voluntary frameworks can be effective at realigning market incentives and reducing misperception of risk.

Benefits, risks and limits

Voluntary frameworks are effective tools to provide guidance to stakeholders, in particular supply-side actors. They can be effective at realigning market incentives and reducing misperception of risk, and can also enable supply-side actors to assess their maturity regarding digital security risk management. Voluntary frameworks are also an important tool to address the challenge of complexity (see section 2.1.1), as different standards can be developed for different contexts of use (e.g. various sectors or “verticals”, consume v. industrial, etc.). They are also more flexible than legal requirements, and can therefore adapt quickly to technological change. As they are voluntary, they carry little risk of disproportionate use or of market distortion.

However, industry-led approaches carry a risk of being captured by certain actors, e.g. large organisations that can afford to participate to and influence such processes, as opposed to SMEs. These actors could drive the results of industry-led processes towards their interests, which may not be aligned with optimal outcomes for the whole of society. To address this pitfall, the development of voluntary frameworks should be as inclusive and fair as possible, and could rely on independent third-parties (e.g. a government agency or external experts) to bring neutral perspectives.

Furthermore, the use of voluntary frameworks only may prove insufficient to address the challenges identified in chapter 2 of this report. Voluntary frameworks only address the supply-side of the value chain. In the absence of labels, they may not empower end-users to make better purchasing decisions nor increase transparency on the market. In addition, the uptake of such frameworks is uncertain and varies greatly across industries[32]. In particular, the uptake seems limited in fragmented or emerging markets, and in markets where externalities and information asymmetries are significant.

Consequently, depending on the specific market, there may be a need for governments to complete voluntary frameworks with other policy tools, to better incentivise stakeholders to adhere to standards. In the UK, for instance, the government has decided, after a public consultation and limited results from the publication of their voluntary framework for IoT security, to proceed with mandating minimum requirements for all IoT products through *ex ante* regulation.

More generally, voluntary frameworks may be a good starting point for governments, as the design of such frameworks is also an occasion to start a dialogue with relevant stakeholders, e.g. producers, vendors and consumers. However, if the uptake is limited and the impact insufficient, policy makers should explore other avenues such as *ex ante* requirements and *ex post* mechanisms.

Important aspects

To be successful, voluntary frameworks need to leverage the multi-stakeholder community that will ultimately make use of them, from the design phase to the implementation phase. The involvement of the relevant stakeholders will enable policy makers to leverage their knowledge and resources, and will also create the conditions for the adoption of the framework at a later stage.

Recently adopted standards show that various methodologies can be used, as they can:

- Focus on product features, such as “no default passwords” (ETSI, 2019[32])[33].
- Focus on processes and policies, or “activities” (NIST, 2020[18]).
- Aim to increase transparency (e.g. recommending to develop a “bill of materials”).

The best format for the framework will likely depend on the context. Some stakeholders may prefer principles-based and outcomes-oriented frameworks, while others may prefer clear technical requirements (see section 4.8).

Policy makers should also take into account the following challenges when considering the use of voluntary frameworks and guidance:

- Fragmentation: governments should avoid creating new frameworks where industry or international standards are already available. Framework proliferation, in particular in case of inconsistencies, may be counterproductive and create confusion for producers. Governments should consider developing frameworks when there are gaps in the resources already available for stakeholders. Alternatively, frameworks could prove useful to contextualise existing international standards for national actors.
- Limited uptake, which could arise for many reasons, including the lack of peer pressure and coordination between the government and the industry, or in case the misalignment of market incentives, externalities and information asymmetries are too significant. If the uptake by the industry is insufficient, mandatory *ex ante* requirements and *ex post* mechanisms may prove more effective.

Discussion of relevant voluntary frameworks and technical standards developed in OECD countries

The following international standards are particularly relevant for the digital security of information systems and organisations:

- ISO/IEC 27000 family of standards, which defines requirements for information security.
- ISO/IEC 27001, which defines requirements for the establishment of an information security management system (ISMS) within organisations.
- ISO/IEC 27005, which defines requirements on how to conduct an information security risk assessment in accordance with the requirements of ISO 27001.
- ISO 27006, which defines requirements for the accreditation of bodies providing certification of ISMS.
- ISO 31000 family of standards, which defines requirements for risk management in general.

In 2016, the United States’ Food and Drug Administration (FDA) published a draft guidance for medical devices manufacturers, recommending to develop a “cybersecurity bill of materials,” defined as “a list of commercial and/or off-the-shelf software and hardware components of a device that could be susceptible to vulnerabilities”. Similarly, the United States’ National Telecommunications and Information Administration (NTIA) is exploring the feasibility of incentivising supply-side actors to provide a “software bill of materials” (SBOM) for the products they put on the market.

Still in the United States, NIST has developed a framework to help organisations to better manage digital security risk in general (NIST, 2018[43]). Adherence to this framework is mandatory for U.S. government agencies and voluntary for the private sector. It provides a good example of how policy makers can build tools that are principles-based and outcomes-oriented. The NIST framework focuses on five core security activities or functions (identify, protect, detect, respond and recover). The framework also provides for each activity a list of industry and international standards that may be used by the industry. However, the framework applies to organisations, not products.

More recently, NIST has developed a voluntary framework to provide guidance to supply-side actors in the IoT market, for both consumer and industrial IoT, and across verticals (NIST, 2020[18]). Given its wide scope, the framework focuses on processes and policies (or "activities") for manufacturers rather than on product features. The framework identifies six cores activities for supply-side actors. Some should be implemented before market release (e.g. identify customers and define use-cases) and others should be implemented after market release (e.g. communicate with customers). More broadly, the framework intends to enable supply-side actors to "lessen the efforts needed by customers" to manage digital security risk

In the UK, the government has developed a Code of Practice for Consumer IoT (DCMS, 2018[44]) that proposes thirteen outcomes-oriented guidelines for stakeholders, in particular for producers of IoT devices. These guidelines address many aspects of the digital security of products, from access control and authentication to data protection and security updates. On the basis of this framework, ETSI has developed a technical specification, TS 103 645 on "Cyber Security for Consumer Internet of Things" (2019[32]), and a European standard, EN 303 645 on "Cyber Security for Consumer Internet of Things: Baseline Requirements" (2020[19]).

As these frameworks were developed recently, there is need to schedule regular review of their uptake by relevant stakeholders, in order to assess their effectiveness. In the absence of significant uptake, there may be a need to develop other policy tools such as *ex ante* requirements and *ex post* mechanisms.

Promoting certification and conformity assessment

Policy makers can promote certification and conformity assessments to reduce information asymmetries and realign market incentives. In the United States, a report recently recommended the creation of a "National Cybersecurity Certification and Labelling Authority, empowered to establish and manage a program on security certifications and labelling of ICT products" (Cyberspace Solarium Commission, 2020[12]).

The definitions of certification and conformity assessments vary across sectors and across OECD countries. Conformity assessments can be defined as mechanisms to evaluate whether products, processes or organisations meet specific requirements, which can be defined through voluntary guidance or technical standards (see section 4.5). Certification can be defined as a mechanism to assess with certainty, through the evaluation of an independent third-party, whether products, processes or organisations meet a certain level in a specific area, e.g. digital security.

In that regard, some experts consider that certification is one way of assessing conformity, through the evaluation of an independent third-party (as opposed to self-assessment). Alternatively, other experts consider that certification does not necessarily need to rely on a conformity assessment: for instance, a penetration testing may be used to certify that a product or organisation meets a certain level of maturity regarding digital security, while not relying on technical standards.

Benefits, risks and limits

Certification and conformity assessments are effective tools to build trust, increase transparency (see section 3.1), ensure the duty of care of supply-side actors (see section 3.3) and promote innovation and competition (see section 3.5). They also fuel co-operation (see section 3.4) as they enable stakeholders to verify products' quality and connect the technical state of the art (standards) with the market.

For producers, however, conformity assessments are associated with significant costs, depending on each model (e.g. certification, self-assessment…). Therefore, the use of certification and conformity assessment should be proportionate to the risk (see section 3.6). For the demand-side, the impact of certification conformity assessments can be high for advanced users, which may be familiar with voluntary frameworks and technical standards. However, for mainstream users, their impact without accessible labels (see section 4.7) will likely be limited.

Policy makers can promote certification and conformity assessments through other policy tools such as public procurement, labels, *ex ante* regulatory requirements and *ex post* mechanisms (see sections 4.3, 4.5, 4.7, 4.8 and 4.8). The risks and limits associated with conformity assessment depend on the other policy tools used to promote them.

Categories of conformity assessments

Conformity assessments rely on three main components:

- Products (goods and services), processes or organisations.
- Standards (e.g. ISO), which can be specified through technical specifications. They describe the requirements that the products, processes or organisations shall meet. Alternatively, certification may not rely on standards, but rather on assessing a maturity level for digital security.
- The conformity assessment process, which evaluates whether the products, organisations or processes are aligned with the standards or with the objectives and maturity level.

Quality assurance processes can be considered as a form of conformity assessment, even though they involve requirements that are defined internally, as opposed to requirements set in standards or technical specifications. The use of robust quality assurance processes can be one of the criteria used to assess conformity with standards.

Whether the conformity assessment targets products, processes or organisations, three elements are important: their nature, structure and timeframe.

Nature

Conformity assessments can be mandatory or voluntary:

- Mandatory: in the EU, a product manufacturer can only place a product on the market if it meets all the applicable requirements (e.g. electrical products, food, etc.). Conformity assessments are usually mandatory if consumer safety, health or critical activities are at stake.
- Voluntary: product manufacturers may assess the conformity of their products to reduce information asymmetries, and use the assessment as a market differentiator and to build trust with customers and public authorities.

Structure

Conformity assessment can rely on self-assessment or third-party certification:

- Self-assessment is often used in low-risk situations. Manufacturers have the responsibility to test the quality of their products internally and can then assess the compliance themselves (it is usually the case for certain consumer products in the European Economic Area (EEA) with the mark “CE”, e.g. light bulbs). Self-assessment usually entails the liability of the manufacturer, and therefore has to be associated with strong *ex post* mechanisms to be effective.
- Third-party certification is often used in medium and high-risk situations. The products are then certified by an authorised (or accredited) third-party. In this case, the costs of conformity

assessments are higher. Compliance rates are also usually higher when third-party certification is involved.

Timeframe

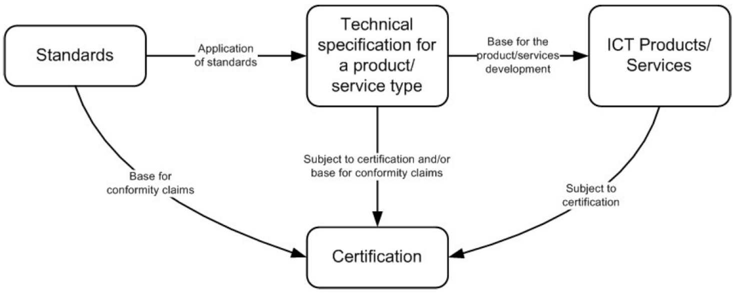
Conformity assessments can be carried out once, before the product is released, or on a continuous basis, through audits for instance.

- One-time assessment: this methodology is more common for goods, which are tested once, before their release on the market (*ex ante*). In addition, testing may be possible *ex post*, for instance through market surveillance. In this case, the costs of control are borne by society (i.e. the regulatory authorities).
- Continuous assessment: this methodology is more common for organisations, whose conformity can be assessed on a regular basis, e.g. several times a year.

As digital security risk is dynamic by nature, it is more and more common for third-party certification companies to adapt their assessment methodology and to implement continuous assessment, e.g. testing the product after it has been released and modified through updates.

Figure A B.2 provides an example of a conformity assessment framework. In this example, the conformity assessment is undertaken by a third-party (certification process).

Figure A B.2. The certification process for ICT products in the EU.

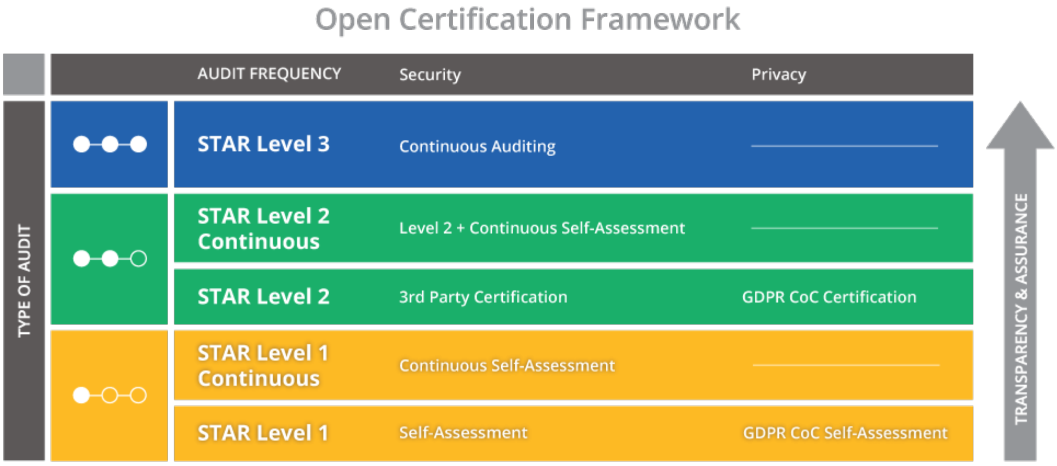

Standards
Application of standards
Technical specification for a product/ service type
Base for the product/services development
ICT Products/ Services
Base for conformity claims
Subject to certification and/or base for conformity claims
Subject to certification
Certification

Source: (ENISA, 2019[59]).

The Cloud Security Alliance (CSA)'s STAR program provides a layered approach to certify cloud service providers, from self-assessment in low risk environments to continuous assessment and auditing in high risk environments (Figure A B.3). In this framework, two variables are used to adapt the conformity assessment to the level of risk:

- The structure of the assessment: self-assessment v. third-party certification.
- The timeframe of control: one-time testing v. continuous auditing.

Figure A B.3. Cloud Security Alliance (CSA)'s Security Trust Assurance and Risk (STAR) Program



Open Certification Framework

	AUDIT FREQUENCY	Security	Privacy
●●●	STAR Level 3	Continuous Auditing	—
●●○	STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment	—
	STAR Level 2	3rd Party Certification	GDPR CoC Certification
●○○	STAR Level 1 Continuous	Continuous Self-Assessment	—
	STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment

Note: This conformity assessment program is designed specifically for cloud service providers.
Source: https://cloudsecurityalliance.org/star

The challenges of conformity assessment

While conformity assessments have many benefits, they also raise certain challenges:

- For the self-assessment model, there is a risk of non-compliance or poor implementation. For instance, some studies have found that in the EU, between 5% and 40% of electrical products were for sale without the energy label or with an incorrect implementation, with an overall non-compliance rate of 20% (Blythe and Johnson, 2018[68]).
- For the third-party certification model, assessing conformity usually incurs significant costs for the manufacturers. There are both direct costs (e.g. purchasing a service from a company authorised to certify) and indirect costs (e.g. increased time-to-market). Some experts consider that with the number of connected devices expected to reach 20 billion in 2020, the third-party certification model may not be scalable to all smart products (Blythe and Johnson, 2018[68]) but should be rather targeted at medium or high risk products.

In addition, while conformity assessments on their own may help advanced users to make better purchasing decisions, they would likely not have the same impact on mainstream users. In the absence of clear and simple information that allows for comparability (e.g. labels, see section 4.7), mainstream users are often unable to leverage other information such as conformity assessments (e.g. ISO 27001 certification).

Furthermore, certification schemes are usually only valid within a specific jurisdiction. A company would therefore have to undergo new certification processes for every new market they intend to target, which may incur significant additional costs. The challenges associated with the proliferation and fragmentation of norms across countries, including for conformity assessments, are further discussed in section 4.9.

Finally, the digital transformation significantly challenges the nature and scope of certification. In many OECD countries, certifications are only valid for a finished and tangible product, whereas more and more products contain intangible code, and can be updated in the course of their commercial life. If an update modifies their code, their conformity assessments may no longer be valid (Schmitt, 2019[49]). When such certification is mandatory, it can become an obstacle to the implementation of security updates, an issue pointed out as "insecurity-by-compliance" (OECD, 2019[1]).

Addressing the challenges associated with conformity assessment

The various models of conformity assessments enable policy makers to take these challenges into account and adapt requirements to the level of risk, in line with the “proportionality” principle. Low-risk situations may call for voluntary self-assessments while high-risk situations may call for mandatory and continuous third-party certifications. A multi-layered approach may be the most effective, with self-assessment being favoured as a baseline, and certifications required for higher risk products.

To adapt to smart products, certification methodologies are evolving. Some companies increasingly rely on continuous auditing rather than one-time testing, and include certifying processes and organisations, rather than just a product. For instance, certifications can assess a product’s features (e.g. an update mechanism) as well as the vendor’s organisational and technical capabilities (e.g. team in charge of maintaining the product’s security, vulnerability disclosure policy, time between the discovery of a vulnerability and the issuance of a security update, EOL policy, etc.).

In the US, for instance, the Food and Drug Administration (FDA) had to take action to adjust existing policies with new challenges related to IoT. In 2016, the FDA (2016[69]) established guidelines for medical devices that decouple basic security updates from existing product certification regimes.

To address the proliferation and fragmentation of norms, policy makers can promote interoperability between legal frameworks (see section 4.9.7). In the European Union, the Cybersecurity Act (EU, 2019[48])aims to facilitate cross-border recognition of certifications across the European Union. Cross-border recognition can support the “business case” for certification, as companies would need to go through only one process to obtain a certification that would be valid for a significant market. However, cross-border recognition also raises concerns regarding the consistency and equivalence of evaluation methods as well as the enforceability of certificates (PETRAS, 2018[70]). To address this issue, the Cybersecurity Act introduced peer-review mechanisms to evaluate the consistency of national certifications.

What role for policy makers?

Certification and conformity assessments are widely used in some sectors (e.g. food, energy, industry) to reduce information asymmetries and ensure that products meet a certain level of quality or safety. However, to maximise the impact of conformity assessments, policy makers need to leverage other policy tools.

First, policy makers can develop their own frameworks (see section 4.5), and incentivise producers and other stakeholders to use those frameworks on a voluntary basis. Such incentives include awareness-raising campaigns and public procurement (see sections 4.1 and 4.3). These voluntary frameworks can build upon existing international standards. Alternatively, some international standards (ETSI, 2019[32]; ETSI, 2020[19]) were built upon existing governmental frameworks (DCMS, 2018[44]). Secondly, policy makers can develop labels. Certain labels require producers and/or products to be certified to be awarded. This area is further discussed in section 4.7.

Furthermore, policy makers can leverage *ex ante* mandatory requirements to impose conformity assessments on producers. While this tool is the most effective, it also comes with risks and challenges (see section 4.9.3).

Finally, policy makers can use *ex post* mechanisms (see section 4.8), e.g. liability regimes and insurance, to incentivise producers to use conformity assessments. For instance, producers that had their products certified by a third-party could be exempted from certain liability risks, while such waivers would not be granted to products that did not go through conformity assessments or whose conformity was only self-assessed.

Promoting labels

Policy makers can promote labels for the digital security of products. Labels can be effective at reducing information asymmetries, supporting innovation and competition, realigning market incentives and enabling stakeholders to better perceive risks.

As of November 2020, at least three OECD countries are considering launching, or have launched already, labelling schemes for the digital security of products: Finland, Germany and Japan. A draft label that could be associated with the candidate EU cybersecurity certification scheme is also discussed in the EU. These initiatives are further detailed below.

In the United States, a report recently suggested that the "government should convene industry, civil society, and government stakeholders in a multi-stakeholder process to explore requirements for a viable labelling approach", "so security-conscious consumers can make informed choices and create market incentives for secure-by-design product development" (DHS and DoC, 2018[7]). More recently, another report recommended the creation of a "National Cybersecurity Certification and Labelling Authority, empowered to establish and manage a program on security certifications and labelling of ICT products" (Cyberspace Solarium Commission, 2020[12]).

Definition

Labels are typically present on the product's package or on the producers or vendors' website or application. They can help to achieve three objectives:

- Demonstrate to customers that the product meets a certain level of quality;
- Communicate objective information about a product to customers, in a clear and simple manner;
- Enable customers to compare products and make purchasing decisions that are more informed.

However, labels do not form a homogenous category. Their characteristics can vary greatly, as they can be:

- Mandatory (e.g. energy labels for refrigerators in the EU) or voluntary (e.g. "organic" labels for food);
- Awarded by public authorities or by industry-led associations;
- Associated with a level of quality (e.g. certifications), or simply providing information about a product (e.g. a list components or of characteristics of a product with by spider diagrams);
- Based on self-assessment and declarations (e.g. energy labels) or requiring validation by a third-party (see section 4.5).

Benefits, risks and limits

Labels are an important policy tool to increase transparency, and make stakeholders more aware and empowered. They are effective at reducing information asymmetries and realigning market incentives.

Labels are often considered as a balanced tool, which has a positive impact on market dynamics while not imposing disproportionate obligations or costs on producers. They are even considered by some as "low-hanging fruit", i.e. a policy tool that would be easy to develop and bring quick and tangible benefits, with a low risk of negatives consequences.

However, these perceptions may underestimate the complexity of developing labelling policies, and some of the risks that they carry. Certain flaws often limit the effectiveness of labelling schemes (e.g. lack of comparability and lack of uptake by the industry). In case international co-operation is limited, there is also a significant risk of label proliferation that may be detrimental to both producers (raising their costs) and customers, in particular mainstream users (e.g. fuelling consumer fatigue and complexity).

There is therefore a need for governments to approach labels with the principles of smart regulation (see section 4.1) in mind, in order to ensure that labelling schemes are proportionate and consistent across sectors and countries, and with other policy instruments. First, policy makers should consider which type of label is the more adapted to their objectives (mandatory or voluntary, binary or multi-layered, etc.). Second, policy makers should consider the scope of the label: will it apply to all smart products, or only to specific verticals (e.g. consumer IoT, routers…). While the former may be beneficial to increase the simplicity and universality of the labelling scheme – two key factors for its effectiveness –, it may also be difficult to implement as the digital security challenges and best practices may vary across sectors, for which various technical standards may be available. While it may seem easier to implement binary voluntary labels on specific market segments, the use of mandatory labels that rely on a tiered approach (e.g. a graded scheme) is more likely to have wide-ranging effects on market dynamics.

To conclude, while labels are promising, they should not be considered as a "silver bullet" to enhance the digital security of products. In 2019, the UK government has considered developing a voluntary label for IoT security. However, the government decided to rather resort to a regulatory approach after a public consultation highlighted important gaps that may not be addressed by the development of labels only. In particular, the public consultation indicated that consumers expected minimum requirements to be in place through regulations, and would not consider the absence of label as a sign of increased risks. Labels could be useful to help consumers decide between products with a reasonable level of digital security but would be insufficient to impose a minimum level of digital security for all products.

Opportunities and challenges

For governments, labels present three advantages:

- They enable consumer to better assess the quality of the product they purchase - that would otherwise be difficult to discern. Ultimately, the goal is to incentivise consumers to make better choices by enabling them to compare products on the basis on an objective assessment.
- They can act as a lever to encourage supply-side actors to value digital security more. Labels also enable stakeholders to hold product manufacturers accountable, as they allow market surveillance authorities to assess compliance in a more consistent and accessible manner.
- They allow government to promote better behaviour, reduce information asymmetries and realign incentives without stringent requirements or limiting rights to entrepreneurship, or "the industry's freedom to develop the products of their choice" (Blythe and Johnson, 2018[68]).

Labels are usually effective in reducing information asymmetries. Recent studies on the effects of nutrition labels in the EU have found that they increase healthy product choice by 18%, indicating that they do empower consumers to choose healthier food (Blythe and Johnson, 2018[68]). Other research on energy labels in the EU demonstrated that consumers are willing to pay more for energy efficient products as rated by labelling schemes and that around 50% of European citizens opt for Energy Labels as a key source of information to support purchasing decision making (Blythe and Johnson, 2018[68]). Some other studies also show a positive impact of labels on consumer behaviour: almost 80% of consumers pay attention to information about security features when purchasing new products and would perceive a digital security label as a positive factor when choosing a product (Traficom, 2019[71]).

According to recent research, the following aspects are important factors for labelling schemes:

- **Simplicity**. In the EU, the introduction of A+ to A+++ in energy labels has undermined the efficacy of the label as consumers do not perceive the difference between A+ to A+++ as the same as A to G. Consumers want a less time consuming, clear and simplistic alternative to the current implementation of the energy label. Similarly, traffic light nutrition labels have proven less effective than binary labels or scoring nutrition labels to drive better consumer choice (Blythe and Johnson, 2018[68]).

- **Universality**. The more often consumers are exposed to a label, the more they understand it and the more likely they are to be positively influenced by the label (Blythe and Johnson, 2018[68]). For instance, the study of binary health logos for food products has shown that consumers may not detect that it is absent and understand what this absence means. Unless the label is ubiquitous and mandatory on all products (e.g. nutrition scores), its absence is not considered by consumers as a sign of increased risk.
- **Comparability**: effective labels enable consumers to easily compare between products of the same category, and acknowledge various levels of maturity or conformity (as opposed to binary models).
- **Tiered approach**: the graded schemes labels, or the layered "seal of approval" labels seem the most effective to reduce information asymmetries as they enable an easy comparison between products and go beyond a binary approach (see Figure A B.3). From another perspective, labels with different tiers could also present various degrees of information. For instance, a first tier could provide basic information for mainstream users, on the package, while another tier (accessible through a QR code for instance) could provide more detailed technical information for more advanced users (see section 3.2).

Alternatively, the following risks must be taken into account when designing labels:

- **Consumer fatigue**: when exposed to too many labels, or to labels whose meaning is not clear, consumers are likely to not understand them or not take them into account in their purchasing decisions (Blythe and Johnson, 2018[68]).
- **Lack of uptake by the industry**: if the labels are introduced in a voluntary framework, there is a risk that not enough companies adopt the label. If the label is not visible enough to consumers, its impact will likely be limited.
- **Simplification of a complex issue**: while labels aim to facilitate consumers' understanding, they may also oversimplify an issue and disincentivise stakeholders to go beyond the label requirements if a tiered approach is not used (risk of a "race to the bottom"). In addition, labels could be misunderstood by mainstream users as a guarantee of full digital security, even though they only signal that the product fulfils certain requirements.

Examples of labels in other sectors

This section explores existing labelling initiatives in two sectors: food and energy.

In the food sector, there are at least three types of front-of-package (FOP) labels that a consumer may be exposed to (Figure A B.4).

- The first type are Guideline Daily Amount (GDA) schemes that display the calories and information relating to the key risk nutrients and their relative percentage contribution to daily adult requirements. They provide objective information but do not allow for product comparability.
- The second are traffic light schemes. These also communicate information on nutrients. In addition, they add traffic light colouring to help the consumer interpret the data more easily. It allows for a certain degree of product comparability, even though in real life such comparison is often difficult.
- The third type are health logos which are "seals of approval" (Blythe and Johnson, 2018[68]). They do not provide specific information about a product, but suggest a certain level of quality.

Figure A B.4. Examples of food labels

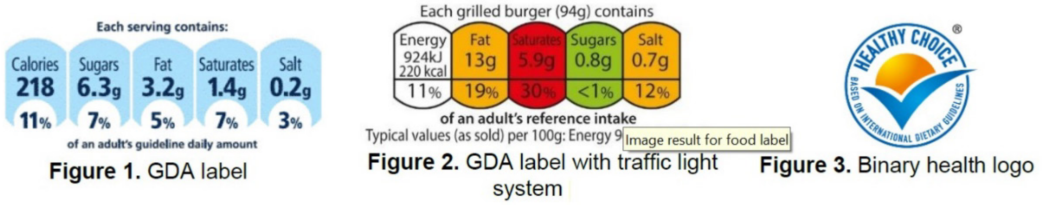
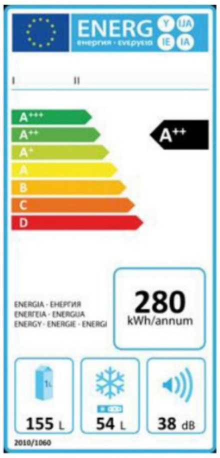

Each serving contains:
Calories 218 11%
Sugars 6.3g 7%
Fat 3.2g 5%
Saturates 1.4g 7%
Salt 0.2g 3%
of an adult's guideline daily amount
Each grilled burger (94g) contains
Energy 924kJ 220 kcal 11%
Fat 13g 19%
Saturates 5.9g 30%
Sugars 0.8g <1%
Salt 0.7g 12%
of an adult's reference intake
Typical values (as sold) per 100g: Energy 9
Image result for food label
HEALTHY CHOICE
BASED ON INTERNATIONAL DIETARY GUIDELINES

Figure 1. GDA label **Figure 2.** GDA label with traffic light system **Figure 3.** Binary health logo

Source: PETRAS

In the energy sector, EU consumers are exposed to a graded scheme for energy efficiency (Figure A B.5). This scheme was introduced by the EU Directive 92/75/EC, which was updated as Directive 2010/30/EU. It rates the energy efficiency of a product from A to G, with A being most efficient and G being least efficient. These markers are paired with a colour to indicate performance with greener products (e.g. A) indicative of greater performance then red (e.g. F). In 2010, A+, A++ and A+++ grades were introduced to keep up with advances in energy efficiency standards. The energy efficiency is rated according to a specific product category covering a range of products including washing machines, refrigerators and light bulbs. Failure by a producer or vendor to comply with the regulation or intentional provision of misleading information is an offence that can lead to financial sanctions. Compliance with the regulation lies with both the producer and the vendor.

Figure A B.5. Example of an energy label



Energy Efficiency label

Source: PETRAS

Labelling models

Based on the examples from other sectors, at least four labelling formats can be distinguished and could be envisioned for communicating information about a product's digital security (Blythe and Johnson, 2018[68]):

- A **descriptive information label** that would provide a list of components or information regarding digital security, such as the product's expected EOL. This format is closer to the "Software Bill of Materials" (SBOM) scheme proposed by NTIA.

- A **traffic light label** that would add to each layer of information a colour, indicating the relative performance of the product for that specific field. For instance, a product may have a green light for its design but a red light for the EOL policy.
- A **"seal of approval" label**. This type of label usually indicates that a product meets a certain level of quality, and relies on conformity assessments (see section 4.5). It does not contain further information on the package (even though more information may be available on the label's website, or upon scanning the label's QR code for instance).
- A **graded scheme** that allows more nuanced comparisons of digital security between products.

Each format has specific upsides and downsides:

- The descriptive information label is easy to implement, but may not be directly useful in informing mainstream users. Consumers usually do not have the means to understand technical details or to compare the products on the basis of such information. However, the information provided may be used by other stakeholders, such as advanced users, to develop more user-friendly types of labels. For instance, in the food sector, stakeholders have developed applications that provide graded schemes on the basis of the information provided on products' packages.
- The traffic light label may help in providing more context and nuanced information about a product's quality. However, the accumulation of information and colours may also lead to consumer's confusion and not lead to better choices when purchasing products (Blythe and Johnson, 2018[68]).
- The "seal of approval" label is usually effective in driving better consumer choices, as it is simple and easily understandable by consumers. However, its absence does not necessarily lead consumers to assess the product's level of quality as insufficient (Blythe and Johnson, 2018[68]). In addition, if the bar set to award the label is too high, there will be limited uptake by the private sector. If the bar is too low, it may disincentivise companies to go beyond the requirements of the label, as this type of label does not enable nuanced evaluations of a product's quality. Companies that provide additional security features would not be able, for instance, to use them as a market differentiator, which may ultimately lead to a "race to the bottom". To address this risk, some countries have favoured a tiered approach, which integrates several levels in the "seal of approval" label (e.g. labelling initiative in Japan, see Figure 4.5).
- The graded scheme may be the most comprehensive type of label (Blythe and Johnson, 2018[68]) as it enables consumers to easily compare products on the basis of their objective characteristics in a simple and intuitive manner. However, this scheme is mostly effective if all products are required to have the label. In a voluntary scheme, companies that would not rank well would likely not volunteer to be part of the label.

Digital security labelling schemes developed in OECD countries

This section provides an overview of the digital security labelling schemes developed in OECD countries, as well as a comparison of the scope, type of labelling and criteria retained for these initiatives.

Finland

In November 2019, the Finnish Transport and Communications Agency (Traficom) launched an "information security" label for IoT devices. The label will be awarded to IoT products if they meet certain certification criteria, based on the ETSI technical specification on Cyber Security for Consumer IoT (2019[32]).

The initiative results from a private-public partnership between the National Cyber Security Centre Finland (NCSC-FI) at Traficom and the following companies: Cozify Oy, DNA Plc and Polar Electro Oy. The label's website (Traficom, 2019[51]) references the products that have been awarded the label and publishes information about the label. In addition, the website provides information to businesses on how they can apply for the label.

The label is awarded if the products meet the following criteria:

- **Certification** of the product by recognised organisations (e.g. STAR certification from the Cloud Security Alliance).
- **Support period:** An EOL policy shall be published that explicitly states the minimum length of time for which the product will receive software updates. For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable. The period of hardware replacement support and an EOL policy should be published.
- **Authentication / Access:** All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.
- **Updatability:** All software components in the product should be securely updatable. The consumer should be informed that an update is required. Updates shall be timely. The need for each update should be made clear to consumers and an update should be easy to implement.
- **Vulnerability disclosure policy**: The vendor 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.
- **Timely updates:** Typical update cycles range from 30 to 90 days, though this may vary greatly depending on the nature of the product.
- **Privacy protection:** Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third-parties that can be involved, including advertisers.
- **Encryption:** Security-sensitive data, including any remote management and control, should be encrypted in transit, with such encryption appropriate to the properties of the technology and usage. All keys should be managed securely. Credentials and security-sensitive data shall be stored securely within services and on devices.
- **Attack surface minimisation:** Unused software and network ports should be closed. Software should run with least necessary privileges, taking account of both security and functionality. Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

Japan

In Japan, the Connected Consumer Device Security Council (CCDS), a business association to improve the security of consumer devices including IoT devices, started a voluntary labelling program for IoT devices in October 2019. The labelling program relies on the certification of products. In this certification program, the level of security measures for IoT devices is classified into a three-layer model as shown in Figure 4.5.

The level 1 certification is based on the regulatory requirements set by the regulator's Amendment of the Technical Standards of Terminal Equipment for IoT security. This regulation makes the following elements mandatory for the provision of IoT devices: access control function; feature to encourage users to change the default IDs/passwords; firmware update feature for the future security fixes.

The level 2 certification will be developed within specific sectors (e.g. banking, industry) while the level 3 certification will be developed for product safety.

Germany

In Germany, the agency in charge of digital security (BSI) partnered with the industry to launch in 2020 a voluntary labelling scheme, “IT Security”. The labelling scheme would be available for all IT products, even though the criteria used to award the labels would be adapted for each category of products (e.g. routers, meters…).

For the government, the objective of the label is to supplement existing statements by product manufacturers, which often lack visibility, relevance and comparability between products. In comparison, the IT security label is standardised, easily understandable by customers and up-to-date.

The label takes the form of a QR code present in the product’s package, which, upon scanning, presents two sets of information to the customer: the manufacturer’s self-declaration and the BSI security information (Figure 4.4). The latter is intended to inform the consumer about security gaps or other security-relevant IT characteristics, while the manufacturer’s declaration assures that the product has certain IT security characteristics.

Comparing digital security labels across three OECD countries.

Figure A B.6 compares the types of labels proposed in three OECD countries.

Figure A B.6. Comparing security labelling schemes in three OECD countries

	Germany	Japan (Level 1)	Finland
	Scope		
Public private partnership	✓	✓	✓
Voluntary	✓	✓	✓
Mandatory			
IT products	✓		
IoT products	✓	✓	✓
Subcategory of IoT products	✓		
	Type of conformity assessment		
Self-declaration	✓	✓	✓
Validation by public authority	✓	✓	✓
Third-party certification		✓	✓
	Type of label		
Information label	✓	✓	✓
Traffic light label	✓		
Seal of approval label		✓	✓
Tiered label		✓	
Graded scheme			

Note: Based on available information as of November 2020.
Source: OECD.

Figure A B.7 compares the substantial criteria used to award these labels.

Figure A B.7. Criteria used to award digital security labels in three OECD countries

	Germany	Japan (Level 1)	Finland
		Criteria	
Strong Authentication	✓	✓	✓
Remote access control		✓	
Updatability	✓	✓	✓
Vulnerability disclosure policy			✓
Attack surface minimisation		✓	✓
Privacy			✓
Encryption	✓		✓
Timely updates	✓		✓
EOL Policy	✓		✓

Note: Based on information available in November 2020.
Source: OECD.

Other tools to increase product transparency comparability

Other policy tools, similar to labels, could be used by governments to increase product transparency and comparability. Such tools are effective to reduce information asymmetries and realign market incentives. For instance, some governments have developed, in other areas (e.g. climate change), the following mechanisms:

"Name & shame" lists to disincentivise consumers to purchase the products of certain producers and vendors. For the digital security of products, this could include actors that are not transparent regarding their EOL policies, that do not provide a software bill of materials or that do not have a vulnerability disclosure policy.

Ratings, on the model of credit rating agencies or of applications rating the health impact of food products. To enable such mechanisms to develop, governments need to impose mandatory transparency requirements on producers (see section 4.8).

Ex post mechanisms

Ex post mechanisms include liability regimes (e.g. strict liability, negligence…), consumer protection (e.g. against unfair and deceptive practices), contract law, insurance and guarantees. They can be defined as policy instruments that enable stakeholders to claim compensations in case of defects or incidents, *after* their occurrence. They often rely on assessing the alignment of a product's quality, or of an organisation's responsibility (e.g. producers and vendors) with what could be reasonably expected. In case of misalignment, *ex post* mechanisms sanction the responsible actors (e.g. with fines). Such controls take place after the product has been released on the market, and may use conformity assessments with applicable standards and norms as a way to determine the responsibility of each actor.

Benefits, risks and limits

Ex post mechanisms are an important policy tool to ensure responsibility and duty of care. They are affective at incentivising stakeholders along the value chain to provide higher standards of security for their products (Dean, 2018[9]). They have been implemented in other policy areas (e.g. product safety), usually in combination with other tools such as *ex ante* requirements, certification and conformity assessments.

The main advantage of *ex post* mechanisms is that they can incentivise stakeholders to act more responsibly without prescribing wide-ranging, horizontal norms, as they rather let stakeholders determine what is optimal in each specific context (e.g. certain markets or product categories). This flexibility is important to address the issue of complexity inherent to smart products (see section 2.1.1).

However, the application of *ex post* mechanisms to smart products raises a number of challenges. These mechanisms take time to adapt to new products and technological change, and to result in effective changes on market dynamics and stakeholder behaviour. Relying exclusively on such mechanisms to address the challenges identified in chapter 2 of this report would be likely insufficient.

In addition, recent research suggests that current norms and regulations need to be adapted to facilitate the application of *ex post* mechanisms to smart products (EU Expert Group on Liability and New Technologies, 2019[33]). In the United States, a recent report recommended to “pass a law establishing that final goods assemblers of software, hardware and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities for as long as they support a product or service” (Cyberspace Solarium Commission, 2020[12]). More broadly, there may be a need for policy makers to review existing legal regimes that support *ex post* mechanisms, to examine their effectiveness for smart products, and to explore solutions to bridge potential gaps. Defining clear roles and responsibilities for all relevant stakeholders (e.g. supply-side actors, network operators, end-users and other code owners) is key to enable *ex post* mechanisms to be effective. Similarly, the development of cyber insurance is limited due to the lack of available data to define and set the price of coverage in an optimal manner. The use of other policy tools (e.g. multi-stakeholder partnerships) could be effective to enable more information sharing between insurance companies and other relevant parties.

The application of liability regimes is often complex

Liability legislation enables users to claim compensation for damages. In theory, it could therefore be a powerful tool to incentivise producers to enhance the digital security of products. An irresponsible behaviour from actors on the supply-side will likely trigger compensation claims on the demand-side, therefore incentivising suppliers to internalise these future costs and invest more in security. A common storyline states that with time, the digital security of products will get better “by itself”, through common law court cases and the application of liability legislation.

Some experts consider that the development and enforcement of personal data protection laws (e.g. GDPR in the EU) will have a positive effect on the digital security of products. In fact, these laws often make data controllers and processors (whether they are legal or natural persons) liable for a breach of personal data affecting other data subjects. As one potential consequence of a digital security attack is a personal data breach, such laws may incentivise, through *ex post* mechanisms, stakeholders (including producers) to put in place adequate digital security measures.

However, the application of liability law is challenging. Investigations are often necessary to determine which actor(s) is (are) responsible for the specific defects that caused harm, as they can originate from the product’s design, its manufacturing, its operation or from the absence of appropriate warnings regarding its use.

When a product is defective, customers usually turn to the final vendor (or reseller) for redress, even though they may not be directly responsible for the defect. In fact, in many OECD countries, the act of sale comes with guarantees and legal responsibility for the vendor. The final vendor may then turn to the previous vendors, i.e. manufacturers and suppliers, to claim compensation for the defect. In a way, all suppliers can therefore be considered vendors of components, resulting in a sometimes complex chain of vendors. While the allocation of responsibility will depend on each specific case, it often lies with the producer and/or the vendor, as they are legally responsible for the product they circulate on the market.

This complexity is exacerbated with smart products

For smart products, the complexity and opacity of the value chain tend to reduce the effectiveness of redress mechanisms, as plaintiffs often do not know to which actor of the value chain they should turn to in case of a digital security incident.

In many OECD countries, the liability of code owners is very limited (Schneier, 2018[10]). Most provisions in software licenses and contracts for services such as cloud offers largely relieve vendors from liability for damages resulting from the exploitation of vulnerabilities. For strict product liability to apply, the consequences have to be particularly severe and involve harm, death or property damage (Dean, 2018[9]), which is often not the case for digital security incidents.

In a recent report (2019[33]), the European Union's Expert group on Liability and New Technologies considered that "liability regimes in force in the EU Member States ensure at least basic protection of victims whose damage is caused by the operation of new technologies" such as AI and the IoT. However, it also noted that with the development of such technologies, "the allocation of liability [may be] unfair or inefficient" and that "the specific characteristics of these technologies", in particular their complexity, opacity, openness, autonomy and "data-drivenness", "may make it more difficult to offer these victims a claim for compensation in all cases where this seems justified".

In particular, the report noted that products containing code do not easily fit in a traditional value chain model based on the distinction between "producers" and "consumers". In many cases, supply-side actors continue to be "operators" of the product after the purchase, for instance to provide updates, and they often have a "higher degree of control than the owner or user" over the product. Consequently, these operators should also have a higher level of responsibility and of liability in case of incidents. The report also noted that products relying on these technologies pose a number of challenges regarding the application of current liability regimes, in particular for:

- Defining what constitutes a "damage", the prerequisite for which victims can claim compensation. "While there is unanimous accord that injuries to a person or to physical property can trigger tortious liability this is not universally accepted for pure economic loss". As a result, the loss of data, for instance, may not be considered as "damage" and therefore may not be compensated in some OECD jurisdictions.
- Demonstrating causation: "one of the most essential requirements for establishing liability is a causal link between the victim's harm and the defendant's sphere", and the burden of proof usually lies on the plaintiff, or end-user. However, it's often difficult to prove that a damage results from a weakness in a product's code (i.e. a vulnerability), especially since the product manufacturer may argue that the damage resulted from negligence on the plaintiff' side (e.g. a misconfiguration).
- Similarly, it is difficult to determine wrongfulness and fault for code weaknesses. Courts may rather associate the fault with the threat (e.g. malicious actors) rather than with the product manufacturer or the vulnerability itself.

Because of these challenges, the report (2019[33]) considered that the adequacy of existing liability rules may be questionable, and that to rectify this, certain adjustments may be needed for national liability regimes. Such adjustments could include the inclusion of hardware manufacturers and software designers in the scope of product liability and safety laws (product security laws, EU Directive 85/374/EEC).

The debate on updating liability laws is also gaining momentum in other OECD countries. For instance, in the United States, a recent report recommended to “pass a law establishing that final goods assemblers of software, hardware and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities for as long as they support a product or service” (Cyberspace Solarium Commission, 2020[12]). However, such requirements should take into account the complexity of the value chain, including potential code owners other than the final assemblers, as well as the role of other actors such as network operators and end-users.

Contract law and consumer protection

Beyond liability regimes, contract law and consumer protection law (e.g. against unfair and deceptive practices) are important mechanisms to realign market incentives. However, in many OECD countries, the application of such laws to the producers and vendors of smart products raises a number of challenges, similar to those raised with the application of liability regimes.

Historically, the responsibility of software designers has been very limited (Dean, 2018[9]) (Schneier, 2018[10]), as the damages caused by code weaknesses have been considered minor and as it has been difficult to associate causation and fault with the producers and vendors. In addition, judges and legislators have considered that software liability needed to be limited in order to support innovation.

The terms of services and end-users’ agreements, in particular for services such as cloud offers, largely relieve producers and vendors of any responsibility in case of digital security incidents. While laws and regulations usually supersede contracts, there is often a gap for the digital security of products, resulting from the difficult application of relevant liability law to smart products.

Insurance

From a risk management perspective, cyber insurance can be described as a tool to transfer risk. While the use of insurance does not reduce the risk level, it can help to mainstream best practices. In fact, insurance providers often impose premiums on actors that do not behave responsibly (e.g. drivers who get fined for driving too fast). Alternatively, they may offer rates that are more favourable to actors that can demonstrate commitment to best practices (e.g. international standards). In a way, incentivising stakeholders to buy insurance policies for digital security may result in a virtuous circle. As insurance companies gain more experience and the market matures, the pricing of policies could incentivise companies to act more responsibly.

However, the effect of insurance on the digital security of smart products is uncertain. Insurance policies are usually bought by actors from the demand-side, in particular corporations, not by the actors from the supply-side. Even though buying insurance could indirectly encourage end-users to choose products with a higher level of digital security (e.g., these products could enable them to obtain better rates), this effect would be indirect, and its impact on the supply-side would probably be limited, in particular on consumer markets. In addition, more transparency would be needed to enable insurance companies to recommend certain products, e.g. conformity assessments and labels (see sections 4.5 and 4.7). While the use of liability insurance by actors on the supply-side is uncommon, some experts have argued that “compulsory liability insurance could give victims better access to compensation and protect potential tortfeasors against the risk of liability” (EU Expert Group on Liability and New Technologies, 2019[33]).

Recent research suggests that despite a growth in take-up, the digital security insurance market remains small relative to other commercial insurance business lines (OECD, 2020[72]). Some obstacles limit the effectiveness of insurance coverages for enhancing the digital security of products. In particular, there is a general lack of data, and limited information sharing between insurance providers, which hinders their ability to provide adequate coverages and incentives. The inability to adequately quantify exposure to digital security risks limits both insurance buyers' understanding of their insurance needs and insurance companies' willingness to extend significant coverage for digital security risk (OECD, 2020[72]).

In addition, there is a lack of clarity regarding the nature and scope of insurance coverage for digital security (OECD, 2020[73]). There is often an overlap, and sometimes confusion, between traditional coverage (e.g. for theft or damages on property) and standalone digital security coverage. For instance, should a ransomware paralysing a company's information system be considered as a damage on property? Should an attack through a web server resulting in the breach of a corporation's intellectual property be considered theft? These questions are still largely unanswered and depend on each specific case and insurance company. Such complexity is exacerbated when digital security, as it often does, collides with privacy and international security (e.g. should a digital security insurance cover a GDPR fine in case of a data breach, or be applicable in case of an attack that could be considered as an act of war? (Voreacos, Chiglinsky and Griffen, 2019[74])).

Despite these challenges, the development of insurance could be an important factor to incentivise stakeholders to better manage digital security risk. A recent report in the United States recommended to place "a cap, via standards or certifications of insurance products, on insurance pay-outs for incident that involve unpatched systems" (Cyberspace Solarium Commission, 2020[12]). For instance, the pay-outs could not be issued if the incident involved the exploitation of vulnerabilities for which a patch was available for more than three weeks.

Guarantees

As noted by Akerlof (1970[75]), guarantees are a contractual remedy that is effective at countering information asymmetries: "most consumer durables carry guarantees to ensure the buyer of some normal expected quality. One natural result of our model is that the risk is borne by the seller rather than by the buyer". In fact, guarantees can be considered as another tool to transfer risk, where end-users transfer the risk back to supply-side actors

However, it is unclear how guarantees apply to digital security risk. In most cases, guarantees cover defects that result from the product's design or manufacturing, and exclude damages that are caused by a third-party (e.g. a malicious actor). Unlike insurances, guarantees' coverage is usually limited to the value of the product itself, or to the costs of repairing it, and does not include the economic and social consequences that a digital security incident could result in.

Recent exploratory research (Woods and Moore, 2020[76]) in this area suggests that product guarantees rarely cover digital security risk. In the few cases where they do, many obligations ("what the buyer must do for the warrantee to be valid") and exclusions ("which circumstances invalidate" the guarantee), and the lack of standards across the industry, limit the effectiveness of this tool to reduce information asymmetries. Some of these guarantees, for instance, are only valid in case the digital security incident results from the exploitation of a known vulnerability, and would not cover cases where a zero-day vulnerability is exploited. In some other cases, the guarantee would be invalid if the end-user does not deploy available security patches in a timely manner. This category of exclusion clauses could prove useful to incentivise stakeholders to better manage digital security risk, for instance through effective patch management strategies.

This area could be further explored, in particular regarding the following questions: what is the uptake of guarantees in the markets for smart products? Do guarantees cover digital security risk? Should end-users be more incentivised to adhere to guarantees? Should vendors and providers of smart products be required to provide guarantees for a minimum period?

Annex C. **Car safety in the 1960s and IoT security today: same challenges, same solutions?**

The situation of the booming IoT market of the 2020s is often compared with that of the automobile industry in the United States[34] in the second half of the 20th century (Dean, 2018[9]). Just as cars in the 20th century, the argument goes, IoT products are becoming pervasive and bring tremendous economic and social benefits. However, their massive adoption is associated with new and significant risks. In both cases, the speed of innovation is such that regulation often lags behind, leaving consumers with the burden of coping with risks they cannot fully perceive, assess or mitigate. In order to not repeat the mistakes of the past, and leverage the lessons learned, the argument continues, policy makers should act proactively and regulate the IoT market. Such diligence will likely save time, money and, potentially, lives. While the analogy has its merits, it also has, like any comparison, its limits. This short section analyses the important lessons learned from the automobile industry in the 20th century, explores its relevance towards the booming IoT market, and highlights important differences that policy makers should keep in mind.

From road safety to car safety

For most of the 20th century, deaths by car accidents were considered ineluctable, and reckless drivers were usually blamed for any tragic outcome. The primary policy responses to address those deaths was the enactment and enforcement of rules of the road, such as speed limits, as well as educational programs and awareness-raising campaigns.

In the 1950s, however, the “second collision” doctrine started to gain traction. According to this new school of thought, the cause of death by car accidents was not so much the first collision (i.e. between the car and an obstacle) but rather the second collision (i.e. between the individual in the car, and the car itself). Appropriate technical measures to mitigate the impact of the second collision (e.g. seat belts, and later on, airbags) could therefore be developed, and would later be considered instrumental in saving lives.

Nonetheless, as described by consumer advocate Ralph Nader in his best seller book *Unsafe at any speed* (1965[77]), the implementation of such measures did not take off in the 50s, and were lobbied against by car manufacturers, for which they represented significant costs. Drivers themselves were not particularly eager to pay more for safety, as they rather valued a lower price, comfort and speed. Only a wave of civil lawsuits in the 1960s led most American States to enact regulations that required carmakers to build in safety checks for their products – the equivalent of “security-by-design” requirements for IoT products. For instance, before the 1960s, seat belts were usually optional: they often needed to be purchased for an additional fee, and sometimes had to be installed directly by the customer. In 1966, the US Congress enacted the *National Traffic and Motor Vehicle Safety Act,* which enabled the federal government to impose nation-wide safety standards for motor vehicles. Car safety, often overlooked before the 1960s, had become a building block of road safety.

The introduction of mandatory safety requirements for car manufacturers and vendors significantly contributed to improve car safety, and thus road safety, in the following decades. In the United States, the rate of deaths by motor vehicle accidents per 100 000 inhabitants dropped from 23 in 1950 to 11.3 in 2010, and the rate per 10 000 registered motor vehicles dropped from 7.07 in 1950 to 1.41 in 2010 (Injury Facts, 2011[78]). Other important factors, such as product innovation, the increased investment in and effectiveness of awareness-raising campaigns, and the development of car insurance also significantly contributed to these positive results.

Lessons learned for the IoT market

Important lessons can be learned from how car safety was enhanced in the United States in the second half of the 20th century:

- When many factors and actors are involved, there is no silver bullet or panacea. Policy makers need to approach such issues holistically to design and implement successful strategies.
- Policy responses should not focus only on the demand-side, e.g. with awareness raising campaigns targeting drivers. While user behaviour is important, ensuring that actors within the supply-side take their fair share of responsibility is also paramount.
- Liability laws can have a positive impact. However, their application is often challenging, takes time and incurs significant private and social costs (lawsuits, accidents…).
- Innovation and voluntary measures can prove useful, but are unlikely to raise the minimum level of safety horizontally.
- Alternatively, minimum mandatory requirements have an effective and quick impact on raising the minimum level of safety.

There are many similarities between the policy challenges related to car and road safety in the 1960s and the current policy debate around the digital security of the IoT. This suggests that some of the lessons learned from the former could apply to the latter:

- Misaligned market incentives: for cars as well as for IoT, producers may value cost-effectiveness and usability over security.
- Misperception of risks: before a car accident or a digital security incident strikes a relative, most individuals believe it only happens to others.
- Information asymmetries: both cars and IoT devices are complex technical products, and most consumers are not empowered to evaluate their level of security or safety accurately.
- Complex ecosystems: for both products, many actors are involved, which makes the attribution of responsibility more difficult. The responsibility for car accidents and data breaches is often attributed to the customer who drove recklessly or clicked on the wrong link (Schneier, 2016[79]).

Limits to the analogy and way forward

However, there are also limits to the analogy between car safety and the digital security of IoT. Because of these differences, the lessons learned from the automobile industry may not all be relevant for or applicable to the digital security of IoT.

First, the risk range is not the same for these two product categories, at least for now. While car accidents often result in deaths, digital security attacks associated[35] with the IoT have so far mostly resulted in data breaches and in the unavailability of online marketplaces for a few hours or a few days. In the absence of safety concerns, stakeholders are usually more reluctant to support stringent regulations that could significantly distort market dynamics. However, it can be argued that in the near future, digital security attacks associated with the IoT are likely to have more serious consequences, for instance in case autonomous vehicles or connected power plants are targeted (Schneier, 2018[10]).

Second, even though the risk range for IoT products is likely to evolve in the near future, it is unlikely that it will become as clear-cut as the risk range for cars. Cars all have the same function and form a homogenous product category. The IoT, on the other hand, encompasses a wide variety of products, which form a very heterogeneous product category. While the risk range is similar for all cars, it greatly varies across IoT product categories as well as within them, as their risk level heavily depends on the context of use. This makes “one-size-fits-all” approaches ill-suited to address the digital security of IoT.

In addition, the dynamics of code development make the digital security of IoT a challenge more complex than car safety. For the latter, the product needs to be safe upon purchase, while for the former, the producer’s priority is to accelerate time-to-market, as flaws can be dealt with at a later stage. In the fast-paced software industry, the culture is to “build first and patch later” (Schneier, 2018[10]). On one hand, this means that many IoT products are put on the market without appropriate penetration testing or “pen test” – the IoT equivalent of car crash tests –, and may be very vulnerable to digital security attacks. On the other hand, the “patching culture” holds the promise of making IoT products more secure over time, as their level of digital security may increase after their purchase, without the need for costly product recalls. However, this promise relies on the assumptions that IoT devices are all updatable, that all stakeholders update the products in a timely manner and that security updates are provided for a sufficient period.

These few examples illustrate how IoT devices, and smart products in general, raise challenges that are in a way more complex than those of the car industry in the 20th century. While the analogy proves useful to highlight some key issues and promising answers, it also suggests that a deeper analysis is warranted to fully understand the role policy makers can play in enhancing the digital security of products.

Glossary

This glossary provides simple explanations of terms and concepts used in this report. These definitions have been discussed more extensively in the in-depth analysis report (OECD, 2021[2])

Advanced users: Individuals and organisations with a higher level of digital security maturity. Usually includes security researchers and large corporations that invest significant resources in digital security risk management.

Availability: Characterises a product that is accessible and usable on demand by an authorised user. One of the three characteristics of products that can be affected by a digital security incident.

Cloud computing: Centrally-hosted and shared computing and storage resources, accessed as a service and on-demand, instead of hosted locally.

Code owners: Actors that have a responsibility in managing the digital security of a layer of code, for instance through designing and distributing security updates to patch a vulnerability.

Code vulnerabilities: A weakness in the product's code or design that could lead to vulnerabilities.

Confidentiality: Characterises a product, and associated data, which have not been accessed by an unauthorised user. One of the three characteristics of products that can be affected by a digital security incident.

DDoS attack: Distributed-Denial-of-Service; A type of attack that affects the availability of a system (e.g. a website) by flooding it with requests from a large number of IP addresses. Usually leverages a network of infected products (e.g. computers, IoT) called a botnet.

Designers: The organisations responsible for the development of intangible products (e.g. software).

Digital security attack: A digital security incident involving malicious actors.

Digital security incident: Any event negatively impacting the availability, confidentiality or integrity of the product (e.g. hardware, software, networks and data), and thus leading to damages (e.g. reputational or financial loss, intellectual property theft…). Results from the combination of a threat and a vulnerability.

Digital security risk: A category of risk "related to the use, development and management of the digital environment in the course of any social and economic activity".

End-users: The individual or the organisation using the product. Can be a mainstream user or an advanced user.

Externalities Characteristic of a market where the exploitation of vulnerabilities in products have consequences on third-parties that are not part of the product's value chain (e.g. a DDoS attack). The presence of externalities in a given market tends to limit the ability of market forces to result in optimal outcomes on their own.

Information asymmetries: Characteristic of a market where some actors (e.g. supply-side actors) have more information on a product (e.g. its level of digital security) than other stakeholders (e.g. end-users). The presence of information asymmetries in a given market tends to limit the ability of market forces to result in optimal outcomes on their own.

Integrity: Characterises a product that has not been altered by an unauthorised user. One of the three characteristics of products that can be affected by a digital security incident.

IoT products: Devices and objects whose state can be altered via the Internet, excluding "traditional" IT products such as computers, smartphones or routers. IoT products are part of the Internet of Things, which includes other layers such as networks, protocols and cloud services.

End-of-life (EOL): Stage of the lifecycle when the supply-side actors cease to support the product and to issue security updates. Can be misaligned with the EOU.

End-of-use (EOU): Stage of the lifecycle when the end-users cease to use the product. Can be misaligned with the EOL.

Exploits: Programs developed by threat actors to leverage vulnerabilities in products, in order to bypass digital security measures and policies.

Lifecycle: Approach that consists in identifying the main stages of the product's commercial life, including design & development, market release, commercial life and end-of-life (EOL).

Mainstream users: Individuals and organisations with a lower level of digital security maturity. Usually includes consumers and SMEs.

Malicious actors: Individuals and organisations that look for and exploit vulnerabilities in products, with the intention of causing harm through digital security attacks.

Manufacturers: The organisations responsible for the production of tangible products (e.g. hardware).

Market incentives Elements that influence the behaviour of economic agents towards a certain direction. They can be misaligned when the market favours behaviours that are detrimental to the optimal level of digital security.

Misconfigurations: A weakness in the product's operation or implementation that could lead to vulnerabilities.

Patch: A "repair job" for a piece of code, designed and distributed by code owners to fix a vulnerability. Also referred to as a "security update".

Producers: Encompass both designers and manufacturers.

Products: In this report, refers to any good or service that contains code and can connect (e.g. to the Internet). Also referred to as "smart products".

Risk: The effect of uncertainty on objectives.

Risk assessment: Process of evaluating the severity and probability of the risk.

Risk management: Process of identifying, assessing and treating risk in a systematic and cyclical manner.

Risk treatment: Process of accepting, mitigating, transferring or avoiding risk.

Security researchers: Individuals and organisations that discover vulnerabilities in products, without the intention of exploiting them and causing harm through digital security attacks.

Security update: A “repair job” for a piece of code, designed and distributed by code owners to fix a vulnerability. Also referred to as a “patch”.

Service providers: The organisations responsible for the delivery of services.

Suppliers: The organisations that supply components to producers.

Supply-side actors: Actors that have a role in developing, distributing and maintaining a product. Includes suppliers, manufacturers, designers, producers, vendors and service providers.

Threats: Individuals, organisations or events that may exploit a vulnerability. They are the “external cause” of digital security incidents, and can be intentional (malicious actors) or unintentional (e.g. an employee’s mistake, an outage or a flood).

Value chain: Approach that consists in mapping all actors that have a role in the product’s lifecycle and in managing its digital security, including supply-side actors and end-users.

Vendors: The customer-facing individuals or organisations responsible for the sale of the product.

Vulnerabilities: Any weakness that can be exploited by a threat and lead to a digital security incident. They are the “internal cause” of digital security incidents, and include code vulnerabilities and misconfigurations.

Zero-day: Vulnerabilities that have been discovered by some actors (e.g. a security researcher or a malicious actor) but are unknown to, and thus unaddressed by, the party that can mitigate them (i.e. the code owner has had “zero day” to develop a patch).

Notes

[1] Between 1992 and 2007, the size of Microsoft Windows increased from 2 million to 40 million lines of code (from Windows 3.1 to Windows 7). Today's typical new car includes 100 million lines of code, and a typical iPhone or Android application has tens of thousands of lines of code. Some experts consider that the size of software source code doubles every three and a half years (see the vulnerability treatment report (OECD, 2021[4])).

[2] In addition, only a fraction of users (advanced users) would possess the programming skills that would be required to analyse the source-code. Even when the code is accessible, its complexity and opacity often make it difficult for third-parties to evaluate its level of digital security. The strategy of "security by obscurity"[2], while overwhelmingly rejected by experts, is still widely used by some supply-side actors.

[3] For instance, Microsoft' Security Development Lifecycle (SDL), SAFECode's Fundamental Practices for Secure Software Development, the Open Web Application Security Project (OWASP) or ISO/IEC 27034 series for application security. More recently, national and international guidelines have been developed to address the specific challenges associated with the digital security of IoT products (DCMS, 2018[44]; NIST, 2020[18]; ETSI, 2020[19]).

[4] As described in Annex C, the role of regulation and innovation within the car industry over the last century provides an insightful example. Before the 1970s in the United States, belts had to be separately purchased and installed by the customer. A wave of civil lawsuits led American states to pass legislation imposing security requirements on car manufacturers, for instance installing belts. More recently, innovation such as the seat belt reminder, which produces noise if the car is moving while the seat belt is not on, shows how design can be used to further incentivize end-users to take safety into account.

[5] In the EU's GDPR, Article 32, "Security of processing", states that data processors should take into account the "state of the art" to "implement appropriate technical and organisational measures to ensure a level of security". It also states that "adherence to an approved certification mechanism may demonstrate compliance (GDPR, 2018[55]).

[6] For instance, the EU's GDPR states that data controllers and processors shall "implement appropriate technical and organisational measures" to "ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" and regularly "test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing" (Article 32 "Security of processing", (GDPR, 2018[55]))

[7] This would be in line with Microsoft's decision to release, in 2017, emergency security updates for products that reached their EOL such as Windows XP, in order to patch vulnerabilities that were exploited by the WannaCry and NotPetya malwares.

[8] Pure service providers such as cloud providers are able to terminate a product when they reach their EOL. The ability of vendors and manufacturers to do this for goods is more complex and could raise issues regarding consumer rights.

[9] Source code escrow is the deposit of a source code with a third-party escrow agent. Escrow is typically requested by a party licensing software (the licensee) to ensure maintenance of the software instead of abandonment or orphaning. The product's source code is released to the licensee in case the manufacturer or designer of the product files for bankruptcy or otherwise fails to maintain and update the software as promised in the license agreement.

[10] For instance, the development of an international registry of common weaknesses, on the model of CVE, or of a platform enabling the co-operation of national and regional registries, could be discussed.

[11] Economic agents tend to underestimate the cost of inaction in risk management, and consequently to overestimate the cost of mitigation or policy measures to manage risk. This is usually due to the fact that impact assessments often focus on the direct and short-term costs of certain measures (e.g. salaries paid for a digital security team, investment in an awareness-raising campaign), without fully integrating the long-term benefits of such measures, which can outweigh the initial cost.

[12] For instance, the impact assessment of a labelling initiative should integrate the potential costs for supply-side actors, as well as the potential benefits for customers and the long-term positive impact on information asymmetries.

[13] For instance, ETSI's European Standard on the digital security of consumer IoT (ETSI, 2020[19]), which lays out 13 provisions presented as "baseline requirements" for all consumer IoT products, notes that in certain cases, "constrained devices" may not be able to meet the requirements. The standard defines these products as a device "which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use" (e.g. power supply, battery life, processing power, physical access, limited memory or limited network bandwidth).

[14] From "script kiddie" jargon "pwn", i.e. to compromise or take control of another computer or application.

[15] Guidelines can focus on product features, such as "no default passwords" (ETSI, 2019[37]), on processes and policies, or "activities" (NIST, 2020[19]), or aim to increase transparency (e.g. recommending to develop a "bill of materials").

[16] Some experts consider that while it often takes time for stakeholders to adhere to standards, there is, however, a "natural" evolution of the market towards their adoption, as certain actors (e.g. large corporations) are likely to request adherence to such standards in their contracts with smaller companies. It may also be argued that for emerging markets such as the IoT, standards and guidelines have been developed quite recently. However, other experts consider that market incentives on their own are unlikely to foster the adoption of standards in an optimal manner. The analysis developed in the in-depth analysis report (OECD, 2021[2]) tends to confirm these views.

[17] The role of regulation and innovation within the car industry over the last century provides an insightful example. Before the 1970s in the United States, belts had to be separately purchased and installed by the customer. A wave of civil lawsuits led American states to pass legislation imposing security requirements on car manufacturers, for instance installing belts. More recently, innovation such as the seat belt reminder, which produces noise if the car is moving while the seat belt is not on, shows how the product's design can be used to further incentivize end-users to take safety into account.

[18] In the EU's GDPR, Article 32, "Security of processing", states that data processors should take into account the "state of the art" to "implement appropriate technical and organisational measures to ensure a level of security". It also states that "adherence to an approved code of conduct" or "an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements" (GDPR, 2018[55]).

[19] The technical solutions to achieve strong authentication may vary across industries and sectors, from multi-factor authentication (MFA) to biometrics (e.g. face recognition) and "password-less" authentication. Alternatively, some products may benefit when users do not need to be authenticated (e.g. web services for anonymous feedback).

[20] However, there could be exceptions to this feature. For instance, the hardware components of some products may have technical and physical constraints that make an update mechanism difficult to add (e.g. sensors for street lamps may be constrained by size, low memory or network capacity).

[21] For instance, a connected fridge or a connected coffee maker could be able to keep functioning even though the product is disconnected, and users should be able to disconnect their product if a connection is not necessary for the product to perform its main functions.

[22] For instance, the EU's GDPR states that data controllers and processors shall "implement appropriate technical and organisational measures" to "ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" and regularly "test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing" (Article 32 "Security of processing", (GDPR, 2018[55]))

[23] This would be in line with Microsoft's decision to release, in 2017, emergency security updates for products that reached their EOL such as Windows XP, in order to patch vulnerabilities that were exploited by the WannaCry and NotPetya malwares.

[24] Pure service providers such as cloud providers are able to terminate a product when they reach their EOL. The ability of vendors and manufacturers to do this for goods is more complex and could raise issues regarding consumer rights.

[25] Source code escrow is the deposit of the source code of a product with a third-party escrow agent. Escrow is typically requested by a party licensing software (the licensee) to ensure maintenance of the software instead of abandonment or orphaning. The product's source code is released to the licensee in case the manufacturer or designer of the product files for bankruptcy or otherwise fails to maintain and update the software as promised in the license agreement.

[26] For instance, the development of an international registry of common weaknesses, on the model of CVE, or of a platform enabling the co-operation of national and regional registries, could be discussed.

[27] Economic agents tend to underestimate the cost of inaction in risk management, and consequently to overestimate the cost of mitigation or policy measures to manage risk. This is usually due to the fact that impact assessments often focus on the direct and short-term costs of certain measures (e.g. salaries paid for a digital security team, investment in an awareness-raising campaign), without fully integrating the long-term benefits of such measures, which can outweigh the initial cost.

[28] For instance, the impact assessment of a labelling initiative should integrate the potential costs for supply-side actors, as well as the potential benefits for customers and the long-term positive impact on information asymmetries.

[29] For instance, ETSI's European Standard on the digital security of consumer IoT (ETSI, 2020[19]), which lays out 13 provisions presented as "baseline requirements" for all consumer IoT products, notes that in certain cases, "constrained devices" may not be able to meet the requirements. The standard defines these products as a device "which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use" (e.g. power supply, battery life, processing power, physical access, limited memory or limited network bandwidth).

[30] As of April 2020, ((n.a.), 2021[84])

[31] For a more thorough discussion on the application of the "tragedy of the commons" to open-source software, see the Annexes.

[32] Some experts consider that while it often takes time for stakeholders to adhere to standards, there is, however, a "natural" evolution of the market towards their adoption, as certain actors (e.g. large corporations) are likely to request adherence to such standards in their contracts with smaller companies. It may also be argued that for emerging markets such as the IoT, standards and guidelines have been developed quite recently. However, other experts consider that market incentives on their own are unlikely to foster the adoption of standards in an optimal manner. The analysis developed in the in-depth analysis report (OECD, 2021[2]) tends to confirm these views.

[33] However, ETSI's technical specification also focuses on processes and policies (e.g. VDPs).

[34] For practical reasons, this discussion focuses only on automobile industry and car safety regulation in the United States.

[35] Such attacks can either target IoT products directly (e.g. to extract sensitive data such as credentials or personal information) or leverage vulnerabilities in IoT products, in order to enrol them into a botnet and perpetrate DDoS attacks against other targets (e.g. social media and e-commerce platforms).