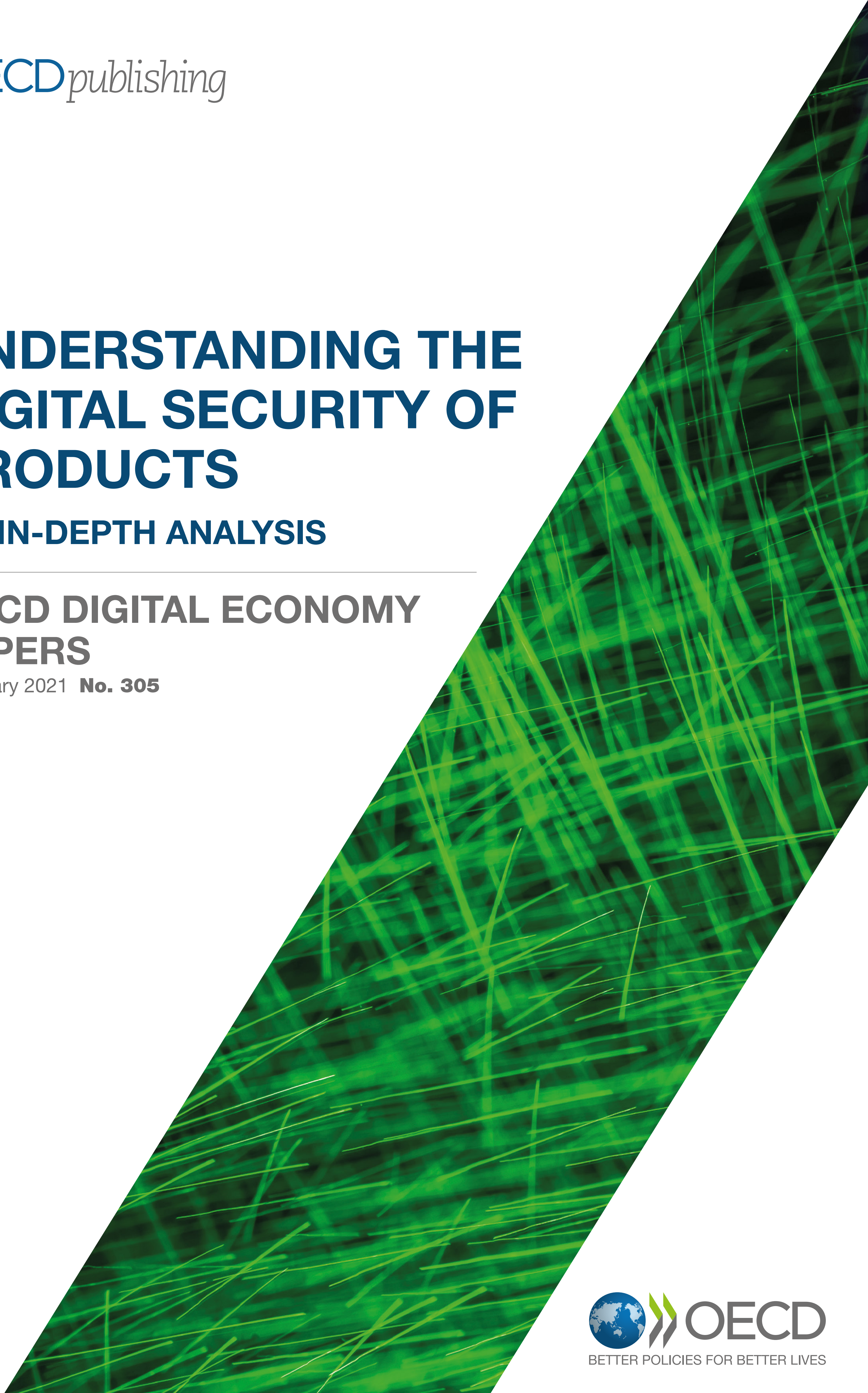
OECDpublishing

UNDERSTANDING THE DIGITAL SECURITY OF PRODUCTS

AN IN-DEPTH ANALYSIS

OECD DIGITAL ECONOMY PAPERS

February 2021 **No. 305**



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]). The analysis provided in this report has been used to develop a separate report on "enhancing the digital security of products: a policy discussion" (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 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)10/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.

Table of contents

Tables

Figures

Boxes

Executive Summary

This report provides a detailed discussion of key concepts, approaches and challenges associated with the digital security of products. It contains an in-depth analysis of the dynamics that shape the digital security of products in various markets, from smartphones and desktop computers to consumer IoT products and cloud services.

Code is everywhere

This report focuses on "smart products", i.e. products that contain code and can connect. They include "pure" software, "traditional" IT products such as laptops and smartphones, and products associated with emerging technologies, such as Internet of Things (IoT) devices. Governments, businesses and consumers are increasingly dependent upon smart products. In 2019, 60% of large companies in OECD countries used cloud computing services and 68% of individuals used online banking. According to a survey by Consumers International, 69% of individuals own at least one connected device.

The COVID-19 crisis accelerated the digital transformation and highlighted our increasing reliance on such products. As governments across OECD countries imposed lockdown measures to contain the pandemic, the workforce in many sectors massively shifted to teleworking, sometimes almost overnight. To ensure business continuity in an unprecedented situation, public and private organisations quickly adopted or extended their use of virtual private networks (VPNs) and video conferencing tools.

Code is vulnerable

Because all smart products contain code, they are all, to some extent, vulnerable. In fact, code almost always contains vulnerabilities, which can be exploited by malicious actors. Between 2017 and 2020, an average of 40 new vulnerabilities in widely used products such as Android, iOS or Windows were publicly disclosed every day – and probably many more were discovered but undisclosed.

The exploitation of vulnerabilities in smart products can have severe economic and social consequences. In 2017, the WannaCry and NotPetya digital security attacks affected thousands of small and large organisations in OECD countries, including Renault, Honda, Boeing, Merck, Maersk and the UK's National Health Service. They showed that the successful exploitation of a vulnerability in a single product can paralyse global firms and lead to billions of dollars of damages.

Economic factors play an important role in the digital security of products

To understand why code is vulnerable, **the report develops an analytical framework based on smart products' lifecycle and value chain, and applies it** to three case-studies: *i)* smartphones and desktop computers; *ii)* consumer IoT; and, *iii)* cloud services.

The case studies highlight that technical measures such as multi-factor authentication (MFA) or automatic security updates are key to enhance the digital security of products. However, **the broad adoption of effective technical measures by supply-side and demand-side actors is often hindered by economic factors**, as **market incentives on their own are often not sufficient to drive optimal behaviours**.

Significant information asymmetries often prevent end-users, in particular mainstream users such as SMEs and consumers, to make informed decisions about the products they purchase. The massive switch to teleworking tools during the COVID-19 pandemic provided a large-scale example of this lack of transparency.

In addition, **significant externalities** often lead the producers and users of smart products to neglect digital security risk management, enabling malicious actors to develop botnets and launch distributed denial-of-service (DDoS) attacks, often across borders. The Mirai malware, which managed to enrol millions of IoT devices into a botnet in 2016, illustrated the key role of negative externalities and their impact on the digital security of products.

More broadly, **there is a misperception of digital security risk, and a misalignment of market incentives**. The WannaCry attack highlighted that too many products continue to be used after their "end-of-life" (EOL), i.e. the end of security support. For supply-side actors, the gap between EOL and the end-of-use can be closed by incentivising end-users to buy new products – which may have stronger digital security features or architectures –, while end-users often prefer to continue using older products, unaware of the risk.

In addition, it can be **difficult to allocate responsibility for digital security gaps**. The value chains of smart products are global, complex and opaque. In 2018, the discovery of the Spectre and Meltdown vulnerabilities in microprocessors showed how vulnerabilities in components may affect a wide range of final products.

Key insights for policy makers

Overall, the main findings of the case studies are the following:

- Consumer IoT products have the most significant digital security gaps, at each stage of the product lifecycle.
- Across all case studies, the gaps that emerge during the product's commercial life (misconfigurations or limited deployment of security updates) are the most significant.
- The EOL gap is highly significant for goods such as IoT products and smartphones, less so for services such as cloud offers.
- Gaps during design and development are particularly significant in emerging and fragmented markets such as the IoT, where guidelines and technical standards for "security-by-design" and "security-by-default" are widely available, but not widely used. These gaps are less common in more mature and concentrated markets (e.g. for smartphones and computers).

Throughout the analysis, the report also sheds light on some key insights for policy makers:

- The digital security of products should be approached in terms of levels and as a continuum rather than as a binary concept. A product is not either secure or insecure, but may be "secure enough" for a given context of use, while its level of digital security may be considered suboptimal in other situations.
- Managing the digital security of products goes beyond technical aspects: many economic factors are at play, and market incentives on their own are unlikely to fix digital security gaps.

- Digital security is a dynamic area. Beyond security-by-design, smart products need to be maintained by security updates throughout their lifecycle.
- Supply-side actors could be incentivised to treat vulnerabilities more effectively, e.g. by adopting vulnerability disclosure policies and providing automatic security updates.
- There is no one-size-fits-all solution nor panacea. Digital security of products is complex, spanning across many sectors, markets, product categories and policy areas.

An informed policy discussion involving all relevant stakeholders is needed to address these challenges. Potential principles and tools are further discussed in the policy discussion report (OECD, 2021[2]).

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

Introduction

This brief historical overview shows that the risks associated with smart products are reaching a new scale, and that the digital security of products is evolving from a technical field to a policy challenge.

When digital technologies first reached mainstream consumers and businesses in the 1980s (e.g. personal computers, productivity software), the Internet was still in its infancy, and primarily used by academics. As there was limited interconnection of computers, mostly via internal enterprise networks, the likelihood of threats exploiting vulnerabilities was low and dependent on physical access. Similarly, information systems had a limited role in economic and social activities, which kept the potential impact of security incidents relatively low. Therefore, developers and software engineers did not develop their products and protocols with security in mind (Schneier, 2018[6]): vulnerabilities were widespread, but they were essentially associated with a low level of risk because they could barely be exploited.

Twenty years later, in the 2000s, the Internet became mainstream, and computers more widespread and interconnected, hence vulnerable to remote attacks. In 2000, the virus "ILOVEYOU", or "Love letter", spread through emails exploiting vulnerabilities in Microsoft Windows operating system and Outlook e-mail application. It was sent automatically to Outlook's contact list upon opening the infected email's attachment. While its consequences were not particularly severe, mostly amounting to spam, ILOVEYOU demonstrated how widespread vulnerabilities were and how quickly viruses could spread. The development of the Internet is also associated with that of the "patching culture": as products could be updated remotely, bugs and vulnerabilities could be fixed at a later stage. In the software industry, where time-to-market is a key success factor, "build first, patch later" naturally became the norm (Schneier, 2018[6]).

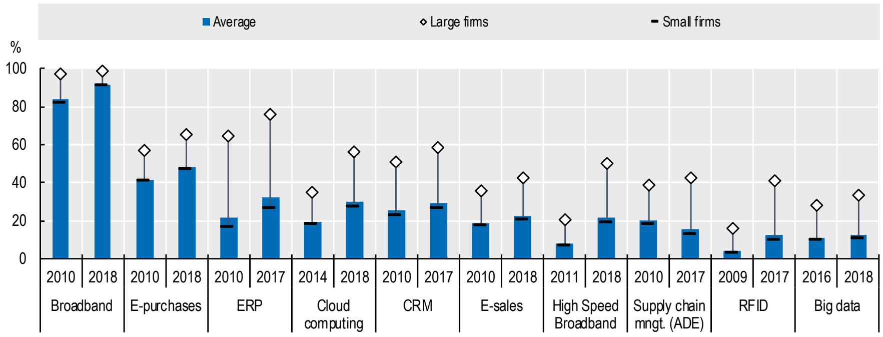
In the 2000s, however, some companies adapted their product development process to build security "by design". Smartphones, which became mainstream in the 2010s, benefitted from enhanced awareness of security issues, including for system design (e.g. application stores impose additional security requirements to developers; smartphones' operating systems usually use sandboxing, which enables only limited memory access for applications). Nonetheless, malicious actors also learned to adapt their techniques and use new attack vectors, as shown with the continuous increase of malware targeting mobile devices (McAfee, 2017[7]).

In 2020, products are increasingly digital-intensive and entire sectors are digitally dependent. Digital transformation increases the dependency on smart products and the risks associated with digital security incidents (Dutch Government, 2018[8]).

On the consumer side, "traditional" goods are increasingly becoming "smart", i.e. contain code and can interconnect (e.g. connected cars and home appliances). Some consider that "everything is becoming a computer": the number of connected devices is expected to reach 20 billion globally in 2020 (Schneier, 2018[6]). On the business side, companies increasingly use software to perform core functions such as production and distribution – "software is eating the world" (Andreessen, 2011[9]) –, making the products they rely on mission-critical, while they used to be considered as a mere support function. The development of cloud computing and subscription-based models for software also changed the dynamics of the Internet ecosystem. For instance, around 60% of large firms in OECD countries rely on cloud computing and on Customer Relationship Management (CRM) tools for their daily operations, according to 2018 and 2017 data respectively (Figure 1).

Figure 1. Diffusion of ICT tools in businesses, OECD countries, 2010 and 2018.

As a percentage of enterprises with ten or more persons employed.



Source: OECD, ICT Access and Usage by Businesses Database, http://oe.cd/bus, January 2019.

With digital transformation, Information and Communication Tools (ICTs) are used to re-engineer business processes entirely through new and innovative business models, rather than only automate them as was the case since the early 1980s. This so-called digital transformation is a source of important disruptions and has profound crosscutting policy implications, the analysis of which is at the core of the OECD Going Digital project (OECD, 2019[10]). Dependence on code and connectivity to achieve economic and social objectives has become significant. With digital-physical convergence and the rise of Internet of Things (IoT) products, the consequences of a security incident are more likely to be tangible and, in some cases, can threaten the physical safety of users. The likelihood of security incidents resulting from vulnerabilities in products has increased, and so have the level of sophistication of attacks and their potential impact. The consequences of digital security incidents are no longer only spam emails sent to a contact list, but now include the disruption of production lines and the paralysis of entire sectors.

In particular, the digital security of IoT has drawn the attention of policy makers across OECD countries in recent years. While the scope of this report is not limited to IoT products – which is only one category of smart products, see chapter 1 –, it provides a case study focusing on consumer IoT.

The objective of this report is to raise awareness and provide analytical background information through:

- Exploring the complex dynamics that shape the digital security of products, in particular the economic factors that determine the behaviour of stakeholders;
- Developing an analytical framework that approaches the digital security of products in a holistic manner, taking into account the product's lifecycle and value chain;
- Applying this framework to three case-studies to test its main hypotheses.

The policy discussion report (OECD, 2021[2]) explores avenues for policy makers to address these issues.

This report explores the economic hurdles that prevent smart products from reaching an optimal level of digital security. It is structured in four chapters:

- Chapter 1 recalls the scope of this work stream.
- Chapter 2 discusses key concepts for understanding the digital security of products.

- Chapter 3 provides an analytical framework to identify digital security gaps, building on the lifecycle and value chain approaches.
- Chapter 4 summarises the main findings of the application of the framework to three case studies on *i)* smartphones and desktop computers; *ii)* consumer IoT products and *iii)* cloud services.

Annex A provides a detailed version of the case studies and Annex B explores areas for future research.

1 Scope

This chapter intends to clarify the scope of this report, in particular regarding the OECD's approach to digital security (Section 1.1) and the definition of products retained for this work (Section 1.2).

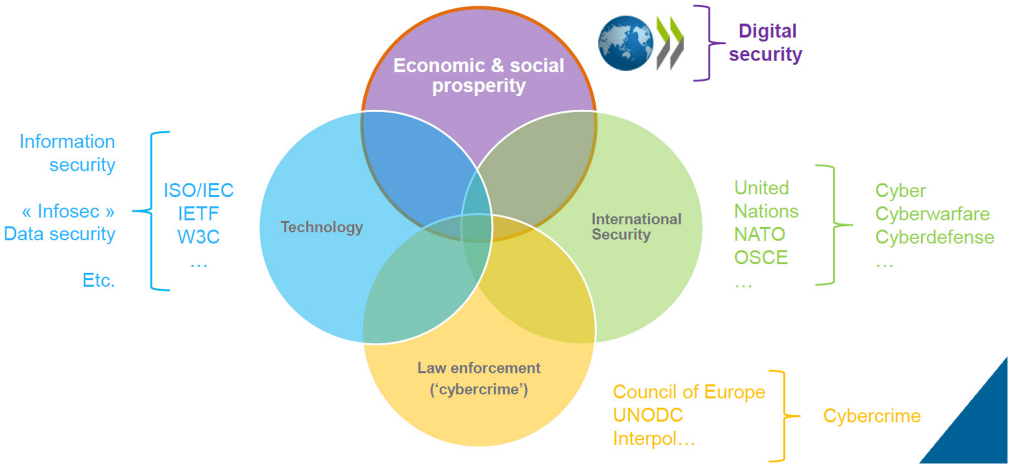
1.1. OECD's mandate is focused on economic and social prosperity

The scope of this report is consistent with OECD's mandate, which focuses on economic and social prosperity. OECD's mandate does not include other areas such as criminal law enforcement, national and international security, or technical standards setting (Figure 1.1), which are discussed in other international fora.

Consequently, while they may be considered important when addressing the digital security of products in a holistic manner, policy challenges related specifically to law enforcement (e.g. attack attribution, cybercrime legislation) and national and international security (e.g. the role of State-sponsored attacks, cyber-espionage and cyber warfare)are not directly in the scope of this report.[1] Similarly, while the work of organisations specialised in technical standard setting (e.g. ISO, ETSI, IETF…) is taken into account, this report focuses on the policy level and intends to remain technology-neutral.

The use of "digital security" by the OECD, instead of "cyber security", highlights that its analytical work focuses on economic and social aspects (e.g. digital economy, digital transformation), rather than on crime or national security.

Figure 1.1. The OECD approach to digital security



Source: OECD.

1.2. A wide scope for products

The concept of "product" is relatively new in digital security policy. Since the 1990s, policy attention in this area has focused on the digital security of organisations' information systems,[2] which can be defined as "a collection of digital components that are connected using communication technologies to perform a business function" (NCSC, 2020[11]). More recently, policy makers have started to investigate how to enhance the digital security of specific categories of products such as smartphones (FTC, 2018[12]) and IoT products (DCMS, 2018[13]).

This report addresses the digital security of products in a holistic manner, encompassing all products for which there are digital security risks.

In this report, the term "products" therefore refers to "smart" products, i.e. products that contain code and can interconnect.[3] Code[4] can be defined as programmable logic or instructions that can be executed by a processor. If a product contains code, it also contains vulnerabilities.[5] A common estimate (Dean, 2018[14]) states that there are between 20 and 100 vulnerabilities every 2000 lines of code. If a product is able to interconnect (i.e. send and receive bits),[6] then these vulnerabilities are likely to be exploitable[7] by threat actors.

These "smart" products can be goods or services, tangible or intangible, hardware and/or software (for a more detailed discussion, see section 2.3), rely on open source or proprietary technologies, and can be "developed for sale or be offered for free" (ISO, 2014[15]). They include, inter alia:

- Software-only products, such as operating systems, applications or websites;
- Internet of Things (IoT) products such as connected home devices, connected cars, connected cameras, etc.;
- "Traditional" IT products (OECD, 2018[16]) such as computers, smartphones, routers and other network equipment;
- Services such as cloud offerings.

2 Key concepts

This chapter explores key concepts to understand the dynamics of the digital security of products.

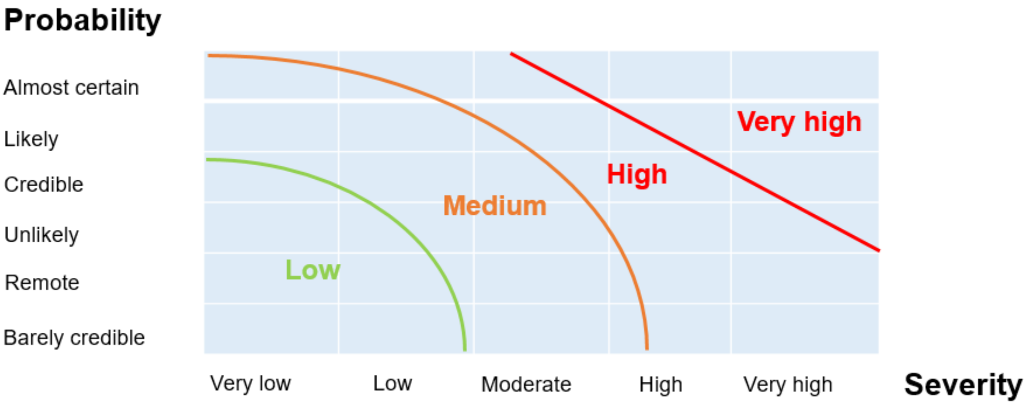
2.1. Risk management

The OECD approaches digital security through the framework of risk management. Risk can be defined as “*the effect of uncertainties on objectives*” (OECD, 2015[17]; ISO, 2018[18]) and should be distinguished from its causes – risk factors.

2.1.1. Risk assessment and treatment

All economic and social activities face some uncertainties and carry a certain level of risk (e.g. eating at a restaurant, driving, taking the plane…). Risk cannot be eliminated completely other than by entirely stopping related economic and social activities. However, it can be managed and reduced to an acceptable level. This is why risk is usually analysed as a combination of likelihood and impact severity, and categorised within ranges such as low, medium or high. Figure 2.1 provides an example of a risk assessment matrix.

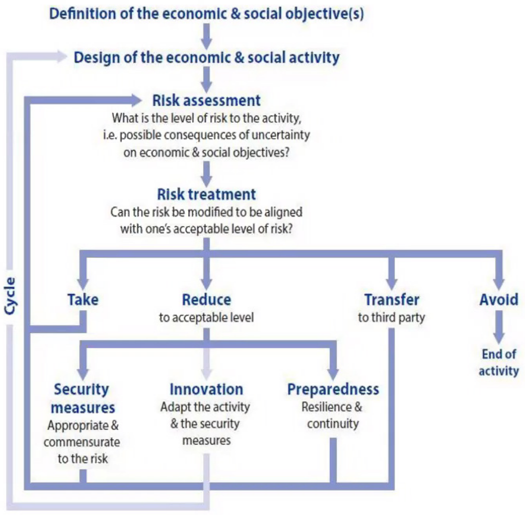
Figure 2.1. Example of a risk assessment matrix



Note: For illustrative purposes only. Thresholds may vary according to the context and to each economic agent.
Source: OECD.

Economic agents adapt their behaviour accordingly, and can decide to accept, mitigate, transfer or avoid the risk. Thresholds depend on each economic agent’s context and risk appetite. Figure 2.2 provides an example of a framework that organisations may use to assess and treat risks on the basis of their economic and social objectives.

Figure 2.2. Digital security risk assessment and treatment cycle


Definition of the economic & social objective(s)
Design of the economic & social activity
Risk assessment
What is the level of risk to the activity, i.e. possible consequences of uncertainty on economic & social objectives?
Risk treatment
Can the risk be modified to be aligned with one's acceptable level of risk?
Cycle
Take
Reduce
to acceptable level
Transfer
to third party
Avoid
End of activity
Security measures
Appropriate & commensurate to the risk
Innovation
Adapt the activity & the security measures
Preparedness
Resilience & continuity

Source: (OECD, 2015[19]).

2.1.2. Digital security risk

Digital security risk is a category of risk "related to the use, development and management of the digital environment in the course of any social and economic activity" (OECD, 2015[19]). The level of digital security risk faced by an economic agent depends on several factors. These factors include:

- The level of digital security of the product: a poorly secured product will likely be more vulnerable to attacks.
- The context of use: the smartphone or the email service of a CEO will be likely targeted by more sophisticated actors than those of a high-school student. Similarly, an attack on a processor used in an industrial system will likely have a more severe impact than an attack on the same processor used in a video game console.

As a result, digital security should not be understood as binary (e.g. a product would be either secure or not) but rather as a continuum: products have a certain level of security. Furthermore, the same product may be "secure enough" for a given context of use, while its level of digital security may be considered suboptimal in other situations. Therefore, this report considers levels of security, in particular against what would be an optimum, or optimal level of digital security (Dutch Government, 2018[8]; Kopp, Kaffenberger and Wilson, 2017[20]). This concept is analogous to the concept of optimal allocation of resources (Pareto's optimum), which is a situation of economic efficiency, where no factor can be improved without negatively affecting another factor. Similarly, the optimal level of digital security would be reached if, taking into account all the other factors of the product (e.g. price, usability, utility…), the level of digital security is at its highest, i.e. a higher level could only be reached by decreasing economic agents' satisfaction with other factors.

Importantly, the optimal level of digital security is therefore not absolute but acceptable security, relative to other factors. The optimal level of digital security will also vary according to the context of use and the economic agent's preferences and risk appetite. At the societal level, an optimal level would enable all economic agents to carry the level of risk of their choice, within the constraints of all other factors. While an optimal level of digital security may be difficult to precisely determine, this concept is useful in order to identify gaps and suboptimal situations.

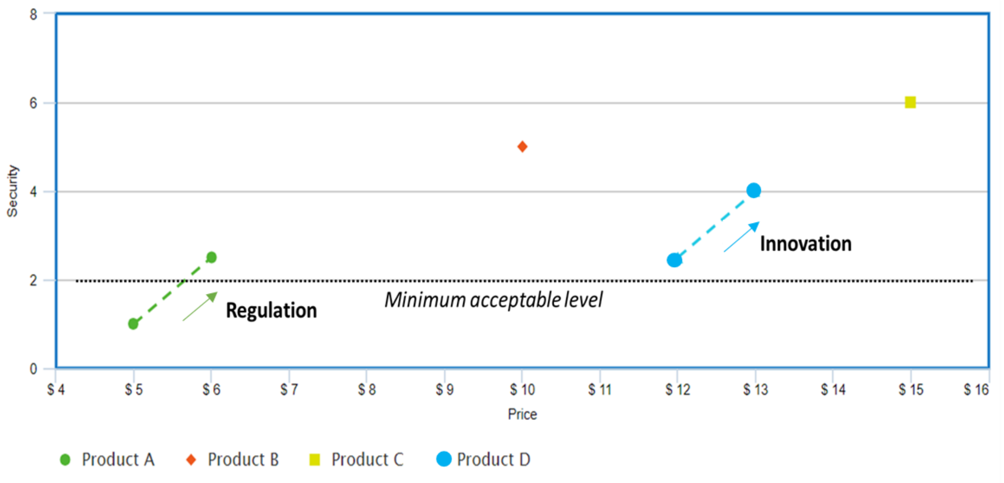
2.1.3. Risk management for products

For products, at least two categories of economic agents are involved in the risk management decision-making process: supply-side actors (vendors and manufacturers) and customers. When customers purchase a product, they trust that it does not expose them to unreasonable risks, and corresponds to what they perceive as an acceptable level of risk.[8] Moral hazard and misallocation of responsibility are further discussed in section 3.2.

Reducing risk usually affects other factors (e.g. a product's price, economic utility or usability), for which economic agents may have to make a trade-off. For instance, a car manufacturer could make its products more secure by adding high quality brakes and airbags, but it would likely increase development costs and therefore the car's price, which could negatively affect demand. An organisation may decide to isolate, or "air-gap" (physically separate from the Internet), a network in a high-risk environment such as the Industrial Control Systems (ICS) of a nuclear power plant. However, this solution would come with significant downsides in terms of usability, functionality, and, potentially, digital security (e.g., the deployment of updates would be difficult if not impossible).[9]

Such potential trade-offs are illustrated by Figure 2.3, based on a two-variable model. Depending on their risk appetite and how they value the other factor (e.g., price), customers may prefer to purchase one product or another. Innovation (product D) may significantly increase a product's level of digital security. Regulation can also be used to impose minimum requirements (product A). Without regulation, products could be marketed even though their level of digital security is not acceptable from the regulator's point of view.

Figure 2.3. Two-variable model: potential trade-offs between security and price



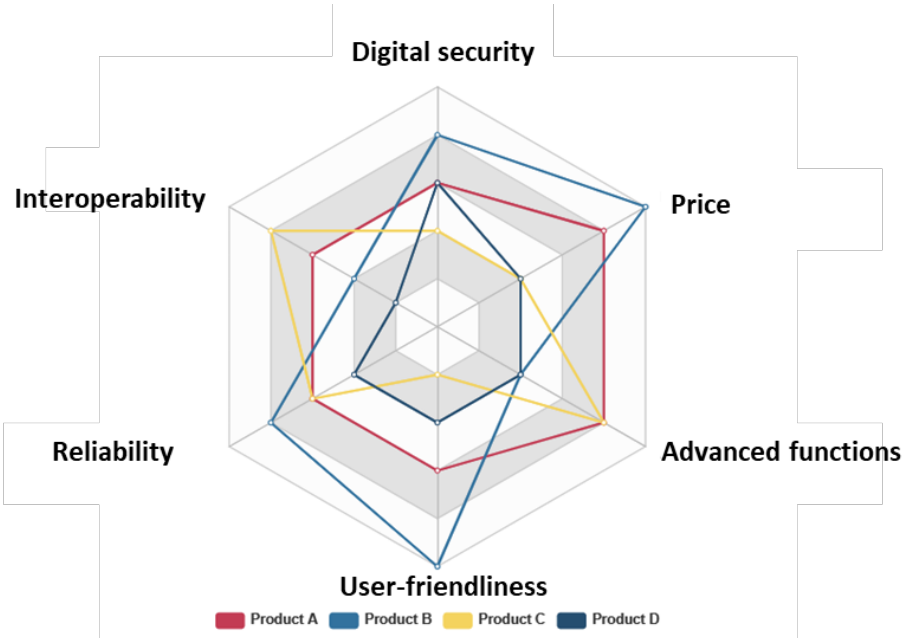
Source: OECD.

However, this two-variable model has many limits. In real life, the choice to purchase a product often depends on multiple variables, as shown in Figure 2.4. However, it is often difficult for customers to take into account all these variables, and even more difficult to compare them in a normalised way. Except for price, quantifying and measuring these variables is often difficult, if not impossible. The customer's judgement therefore relies on other input such as ratings on online marketplaces and marketing materials associated with the product's brand.

In addition, for many customers, the decision-making process to purchase smart products is constrained by limited financial resources. They include consumers with low purchasing power, and organisations with limited resources dedicated to information technology and digital security. These organisations may be

SMEs, institutions in the healthcare or education sectors, as well as large organisations that do not consider digital security as a strategic priority. Often, resources-constrained customers do not take into consideration variables other than price and functionality. These challenges are further discussed in section 3.3. Policy remedies to enable customers to better understand digital security risk associated with smart products, such as labels, are further discussed in the policy discussion report (OECD, 2021[2]).

Figure 2.4. Multiple-variable model: potential trade-offs between security and other factors



Source: OECD.

2.2. Digital security risk

Digital security risk results from the combination of threats and vulnerabilities, which leads to incidents that impact the confidentiality, integrity and availability of data, products or networks. Digital security incidents have a technical impact, which can lead to economic and social consequences. This section provides an overview of these concepts,[10] and explores the relationship between digital security and other approaches such as consumer product safety. In the context of smart products, vulnerabilities can be considered as the "internal" cause of a digital security incident, and threats as the "external" cause. In fact, vulnerabilities are inherent to the product's code, design or implementation, while threats exist independently and are directly not related to the product.

2.2.1. Weaknesses, vulnerabilities and misconfigurations

This report focuses on two types of vulnerabilities contained in smart products: code vulnerabilities and misconfigurations[11].

Code vulnerabilities (hereafter, "vulnerabilities") are generally defined as weaknesses contained in the code embedded in a product, which can be exploited by a threat and cause damages.

While vulnerabilities usually result from flaws in the product's code, they can also result from the product's design itself. Design vulnerabilities may be associated with a specific type of software architecture or with technical constraints that are specific to a product (e.g., low memory). Such vulnerabilities are less likely to be fixed by a security update, as it would require redesigning the product entirely.

For the purpose of this report, the term "vulnerability" will refer to a weakness in the product's code or design that can be exploited by a threat and lead to damages.

Misconfigurations can be defined as an "incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities[12]" (NIST, 2020[21]). Misconfigurations are associated with a specific context, while vulnerabilities are typically present in all the products that contain the vulnerable layer of code. A product's parameter may be optimal in one situation, and suboptimal (hence, a misconfiguration) in another context. Misconfigurations do not require a patch to be fixed, while vulnerabilities usually do. While fixing vulnerabilities often requires a patch, fixing a misconfiguration usually only requires a change of settings.

For the purpose of this report, a weakness in the product's operation or implementation will be referred to as a "misconfiguration".

Importantly, not all weaknesses in the product's code are exploitable vulnerabilities. Other types of product weaknesses are usually referred to as bugs, which cannot be exploited by threat actors and would not cause damages (e.g. the program does not behave as expected).

Similarly, all vulnerabilities are not "created equal". Not all vulnerabilities are critical, and many vulnerabilities are not easily exploitable. For instance, some vulnerabilities can be exploited remotely, through the network, while others would require adjacent presence (e.g. Bluetooth) or physical access (e.g. USB). In addition, the "exploitability" of a vulnerability is likely to increase over time. While initially, real-world exploitation may only be theoretical (e.g. a proof-of-concept), the development of a functional exploit code and the public availability of simple-to-use exploit kits would increase the "exploit maturity". Scoring systems have been developed to measure the severity of a vulnerability. For instance, the Common Vulnerability Scoring System (CVSS) provides a framework to enable stakeholders to rate vulnerabilities, with scores ranging from low (0 to 3.9) to medium (4.0 to 6.9), high (7.0 to 8.9) and critical (9.0 to 10) (FIRST, 2020[22]).

2.2.2. Threats, exploits and AIC

Threats can be intentional or unintentional (e.g. an employee's mistake, an outage or a flood). When threats are intentional, they are referred to as "malicious actors", which includes various categories such as "script kiddies", "hacktivists", cyber criminals or State-sponsored organisations. The objectives of malicious actors can vary extensively, and include financial gain, reputational gain, intellectual property theft, access to personal data or simply the desire to harm or retaliate for personal or ideological reasons.

Digital security incidents encompass both intentional and unintentional threats, while digital security attacks refer to incidents caused by intentional threats.

To take advantage of vulnerabilities, threat actors develop "exploits", i.e. programs designed specifically to leverage vulnerabilities in order to bypass security measures and policies.

The technical impact of digital security incidents is usually categorised as affecting the availability, integrity and/or confidentiality of the product, data or network, often referred to as the "AIC" triad:

- Availability: the product, data or network is not accessible and usable on demand by an authorised entity. For instance, a DDoS attack aims to affect the availability of a website, without affecting integrity or confidentiality;
- Integrity: the product, data or network has been altered in an unauthorised manner. For instance, the product's code has been changed and leads the product to behave in an unexpected manner (however, the product is still available and there has been no breach of confidentiality);
- Confidentiality: data has been disclosed to unauthorised entities. For instance, a digital security attack can leak credentials or clients' personal data.

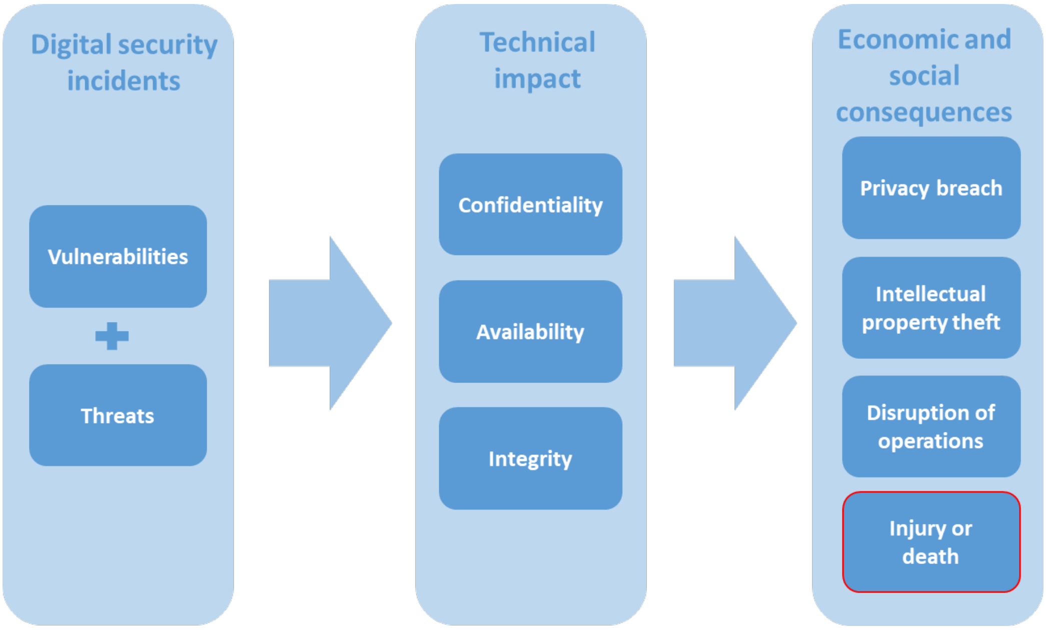
Digital security incidents also have economic and social consequences,[13] e.g. affecting business performance (e.g. lowering competitiveness), financial assets (e.g. loss of money, or increased security costs), physical assets (e.g. interrupted production lines or physical injuries) and intangible assets (e.g. breaching privacy, undermining reputation).

2.2.3. Digital security and consumer product safety

With the emergence of consumer IoT (e.g. connected cars, home appliances…), digital security incidents are more and more likely to impact consumer safety, i.e. pose unreasonable risks of serious injury or death. In fact, as illustrated in Figure 2.5, safety risk is becoming one of the possible economic and social consequences of digital security incidents, along with privacy breaches, intellectual property theft or disruption of operations (e.g. interruption of production lines), to name a few.

Figure 2.5. The economic and social consequences of digital security incidents

Consumer safety is a relatively new possible consequence of digital security incidents.



Note: For illustrative purposes only. The list of economic and social consequences is not exhaustive, and any category of technical impact can have various economic and social consequences. For instance, a breach of confidentiality could also, indirectly, affect consumer safety (e.g. revealing an individual’s location).
Source: OECD

As a result, there is a growing interest in exploring the relationship between digital security and consumer product safety (hereafter “product safety”). However, these two approaches rely on different conceptual frameworks, which raises certain challenges:

- **Intentionality**: consumer product safety usually focuses on unintentional causes (e.g. the user presses a button at the wrong time, but with no intention to cause harm). Alternatively, digital security attacks typically involve a malicious actor who will use his/her expertise to leverage any weakness in the product’s code, with the intention to harm. This means that traditional approaches to manage consumer safety risks, for instance in the automobile industry, may not be suitable for managing digital security risk, as they do not sufficiently take into account expert and intentional threats, for instance through threat modelling.[14] It also means that a product could be deemed safe until a malicious actor exploits a vulnerability. Unlike a defect, a vulnerability may not pose particular safety risks for consumers if it is not exploited by a malicious actor.

- **Focus of the conceptual framework**: the digital security culture is generally based on an operational approach focusing on the AIC triad, while the consumer safety culture is generally based on a legal approach focusing on liability for safety risk. Therefore, there is a need for dialogue between the two communities in order to clarify each approach and enable interoperability.
- **Acceptable level of risk**: when digital security attacks can have safety consequences, the risk appetite is likely to be much lower than in other circumstances. Therefore, the way digital security has been addressed so far in "traditional" consumer IT products may need to be reviewed, in light of the possible safety consequences of incidents affecting consumer IoT products.
- **Lifecycle**: the approach to digital security is dynamic, while the approach to product safety is more static as it is primarily tailored to address tangible products. Many latent digital security vulnerabilities are discovered after the product has been purchased, and products may become unsafe if vulnerabilities are intentionally or unintentionally added to the product through updates (hazardisation). This challenges the notion of pre-market quality testing, which is at the core of product safety.
- **Conformity assessments**: In many OECD countries, certain product safety certifications are only valid for a finished and tangible product. However, more and more products contain intangible code, and can be updated in the course of their commercial life. Therefore, managing digital security risk challenges traditional approaches to products' certification.
- **Product recalls and security updates**: when a product is deemed unsafe, the vendors and consumer safety authorities usually issue a recall. The costs of product recalls are usually borne by the vendors, and consumers are often entitled to a compensation. However, their implementation is not always optimal as it may sometimes be difficult to reach out to the consumers who have already bought the product. Security updates, which may be considered as "digital recalls", are more easily implementable in theory. They only require an internet connection, as opposed to requiring a technician to come, or shipping the product back to the vendor, and are easily scalable, as all products can be updated at the same time. However, security updates are usually not deployed optimally either, as they often require action by end-users. They do not entitle end-users to compensation, even though they may be considered as a way to transfer responsibility from the vendor to the end-user. Alternatively, a mechanism allowing for automatic security updates could be considered as a way to implement recalls optimally. Transparency mechanisms (e.g. reports or notifications) are also important tools to communicate relevant information to customers and inform them of the deployment of automatic security updates.

There are also commonalities between the digital security and product safety conceptual frameworks:

- **Proportionality**: in both frameworks, the goal is not to eliminate risk, but rather to keep it to a "reasonable", "proportionate" or "acceptable" level. However, as noted above, when there are safety risks, the risk appetite will typically be very low.
- **Complex value chains**: in both frameworks, the product value chain or ecosystem is often complex and requires the assessment of the responsibility of each actor (e.g. suppliers, manufacturers, vendors, end-users, etc.). Any incident will likely trigger an analysis of the causal chain that led to the event in order to determine the responsibility of each actor across the value chain (see section 3.2).

The relationship between digital security and product safety is therefore a key regulatory challenge. If not properly anticipated and managed, this might easily lead to overlap, contradictory recommendations for the industry or conflicts between institutions.

2.3. Products

Focusing on the concept of "product" is a relatively new trend in digital security policy. Digital security policy makers have traditionally focused on strengthening the digital security of organisations' information systems rather than products. It is therefore necessary to clarify the concept of product as used in this report.

From a broad perspective, products are the outputs organisations develop to satisfy customers' needs. They are usually delivered through a transaction (e.g. a sale), but may also be consumed for free, in particular in multi-sided markets (e.g. a search engine). The following sections explore approaches to products that are relevant from a digital security perspective.

2.3.1. Goods and services

While some businesses tend to differentiate between products and services (Google, 2020[23]), economists usually consider that services are a category of products, along with goods. Goods and services encompass all products.

Historically, goods have been characterised by their tangibility (e.g. a car) and by the transfer of property rights they entail when they are purchased. On the other hand, services usually consist of intangible activities (e.g. an appointment with a medical doctor) and entail no transfer of property rights, as they rather rely on the concept of an "access" limited in time. However, these categories are not necessarily discrete, and one may argue that there is a continuum between pure goods on one side (e.g. raw materials) and pure services on the other (e.g. a legal advice). In between, many products are hybrid (e.g. a smartphone) and the sale of a good is often associated with some services (e.g. guarantees, maintenance).

These distinctions have also been challenged by the digital transformation. For instance, some goods have become intangible (e.g. downloadable music and movies, also referred to as "digital content goods"). Software, on the other hand, has been traditionally categorised as a good, but is usually sold through licensing schemes whose characteristics are closer to those of a service. Licensing schemes often limit property rights (e.g. no access to source code, Digital Rights Management, etc.), rely on the concept of "access" rather than "property" and can be limited in time (e.g. based on a yearly subscription). Software is also increasingly downloaded, as opposed to sold through a physical medium, and cloud computing further enables the delivery of software as a service (SaaS). Alternatively, cloud computing could also be described as an access to physical / tangible infrastructure (e.g. infrastructure as a service).

From a digital security perspective, the distinction between goods and services is important. First, in most OECD countries, legal regimes for liability[15] apply mostly for goods (often defined as products that are both tangible and finished) and much less so for services, for which terms of services and contracts have greater influence. The application of a liability regime in these cases is complex because many products that incur digital security risk are hybrid, and can be considered as either a good or a service depending on the perspective. Second, the digital security challenges faced by goods and services can be different. For instance, a "pure" service relies exclusively on the notion of "access" and not on the notion of "property". As a result, the EOL gap (when a product continues to be used even though there is no more support provided by the vendor, see sections 3.1.3 and 4.4.2), could be less of an issue for services that can be terminated instantly by revoking the "access" rights.

2.3.2. Hardware and software

A typical dichotomy in the area of digital security is the distinction between hardware and software. Hardware refers to the physical components of a product, such as a device or a microprocessor, while software refers to intangible code. Historically, digital security experts have focused more on software than hardware.

However, this distinction should be nuanced. To function, hardware relies on deeply embedded code, usually referred to as "firmware". Because hardware contains code, it can also contain vulnerabilities. While most vulnerabilities are usually software vulnerabilities, more and more hardware vulnerabilities are discovered. They raise specific challenges, as they may not always be fixed through a security update. In 2017, two vulnerabilities – Spectre and Meltdown – were discovered in modern Central Processing Units (CPUs). They allowed attackers to bypass system protections on almost all recent computers and smartphones, and access sensitive information such as credentials.

Many products combine hardware and software components (e.g. a smartphone). Even though the hardware component might not be part of the product itself (if the product is an application for instance), there is a functional interdependency between hardware and software: bits cannot be processed without atoms. Whether the product is software, hardware, or a combination thereof, it can be exposed to digital security risk because one or more of its components contain code.

2.3.3. Components, ecosystems and context

Some experts such as Bruce Schneier consider that "everything is becoming a computer" (2018[6]). Without going as far, it is reasonable to say that with the digital transformation, more and more products contain digital components (e.g. hardware or software). Between purely intangible (i.e. code-only) "digital" products (e.g. a software, an application, an operating system) and purely tangible "non-digital" products (e.g. crops), there is a wide array of hybrid products such as Internet of Things devices (e.g. connected cars, cameras, etc.).

Any digital component may entail digital security risk for the products they are part of. The Spectre and Meltdown vulnerabilities mentioned above affected all products equipped with the vulnerable microprocessors, including most smartphones and computers. In software products, vulnerabilities may arise in specific modules or libraries that are used across a variety of products.

For instance, in 2014, the Heartbleed vulnerability was discovered in Open SSL (Secure Sockets Layer), an open-source cryptography library used to implement the TLS (Transport Layer Security) protocol in web servers and applications. The vulnerability allowed theft of the servers' private keys and users' session cookies and passwords. Open SSL is widely used across the Internet: at the time of disclosure, about 17% (around half a million) (Netcraft News, 2014[24]) of the Internet's web servers using SSL certificates were considered vulnerable. In June 2020, digital security researchers discovered the "Ripple20" vulnerabilities (Cimpanu, 2020[25]), which are part of a small software library designed in the 1990s. While relatively unknown to the public, this library has been widely used and integrated into industrial and consumer IoT products in recent years. As a consequence, hundreds of millions of products are likely to contain the Ripple20 vulnerabilities. However, it is particularly difficult for supply-side actors and users to be aware of these vulnerabilities because of the complex and often opaque code supply chain of IoT products.

The distinction between products and components varies across markets: from a consumer's perspective, a microprocessor is a component of a smartphone, but from a chip manufacturer's perspective, a microprocessor is a product. This is often referred to as "product interdependency" (ISO, 2014[26]): many products are complex systems that include other products in some way. Products can use code from other products, software libraries, or other types of interfaces. Different products that support the same network protocol or file format may be affected by a vulnerability in the protocol or format. These interdependencies are important as products that use or interact with a vulnerable product may also be vulnerable.

Along with components and products, another important concept is the product's ecosystem. Although digital security professionals used to refer to information systems, the term "ecosystem" (The Internet Society, 2017[27]) is more and more used to describe the dynamics of products on the Internet, similar to that of living beings, as opposed to mechanical or static systems. Digital ecosystems usually rely on a central platform, which enables various products and communities (developers, users, tech companies) to interact.

The level of digital security of a product cannot be fully assessed if the product is analysed in isolation: a weakness in the wider ecosystem can threaten the integrity, availability or confidentiality of the data processed by the product. IoT digital security frameworks typically encompass all layers of the ecosystem, including the device, applications, network, data, etc.

The assessment of a product's level of digital security should therefore be multi-layered, and take into account a micro-dimension relative to the product's components (including various technical layers), and a macro-dimension relative to the product's ecosystem. This can be done through analysing the roles and responsibilities of actors involved in the product's supply-chain and ecosystem.

Finally, it is important to consider the context in which a product is used. In fact, the context can heavily influence a product's risk assessment (usually building on the probability and impact of possible digital security incidents), and consequently, the digital security measures that are put in place to protect the product. For instance, products that have been designed for consumers, such as routers or security cameras, can also be used in industrial settings, which would raise the impact of a potential digital security incident. For product manufacturers and designers, defining expected use-cases during the design & development phase of their products is therefore an important aspect of enhancing the digital security of their products (NIST, 2020[28]).

Therefore, the risk assessment of a product cannot be done only in an abstract way, but should always take into account the context of use, and rely on use case scenarios, including threat assessment and modelling. This is important when stakeholders attempt to define categories of “higher risk” products: while these categories would typically include connected cars or industrial IoT, this exercise should also look at other products for which the context of use could heavily impact the overall risk assessment.

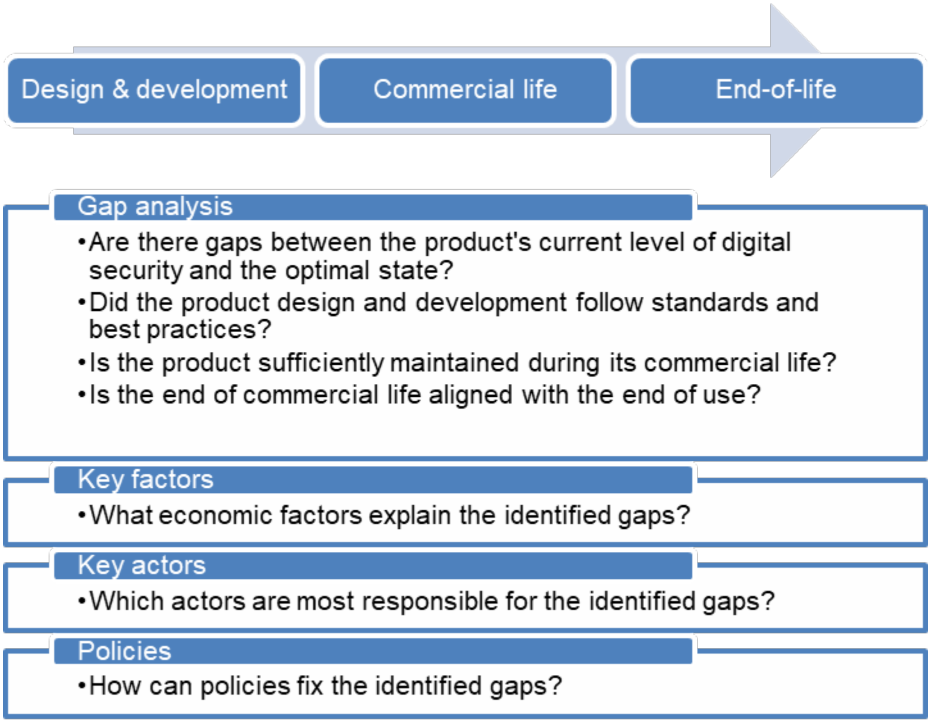
3 Analytical framework

This report relies on an analytical framework (Figure 3.1) to analyse specific categories of products through case studies. The analysis focuses on gaps, i.e. the space between the present state and the optimal state. Three approaches are used to identify and assess those gaps:

- The product's lifecycle: gaps may arise during design & development, during the commercial life or at the product's EOL;
- Roles and responsibilities of actors: gaps may arise because of specific actors that are part of the product's value chain, including components' suppliers, products' designers and manufacturers, service providers, vendors and end-users;
- Market dynamics: economic and organisational factors may explain the emergence of those gaps, including both supply-side and demand-side.

Finally, the framework explores policy options to address the identified gaps.

Figure 3.1. Analytical framework



Gap analysis

- Are there gaps between the product's current level of digital security and the optimal state?
- Did the product design and development follow standards and best practices?
- Is the product sufficiently maintained during its commercial life?
- Is the end of commercial life aligned with the end of use?

Key factors

- What economic factors explain the identified gaps?

Key actors

- Which actors are most responsible for the identified gaps?

Policies

- How can policies fix the identified gaps?

Source: OECD.

As mentioned in section 1.1, the scope of this report is limited to economic and social prosperity. Therefore, some other important aspects are not directly included in this framework. They include law enforcement, intelligence and national security activities, for which governments may decide to find, stockpile and, in certain cases, insert vulnerabilities in products, without disclosing them to the vendor or the wider public.

In addition, the development of State-sponsored attacks has contributed to increase digital security risk overall in recent years, as some governments have decided to dedicate significant resources to "offensive operations". The potentially ambiguous role of governments is further discussed in section 3.2.4.

The following sections present the three approaches used in the analytical framework.

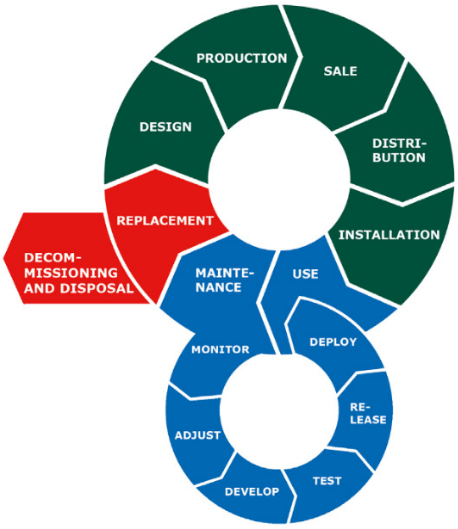
3.1. The lifecycle approach

The lifecycle approach focuses on the effect of time on the level of products' digital security. Recent policy research on the digital security of products has been focusing on the product's lifecycle, recognising that different digital security gaps may arise at different stages of the lifecycle. For instance, NIST has recently published "NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers", whose approach is structured around the activities that have a "pre-market" and "post-market" impact (2020[28]).

A product's lifecycle can be broken down into three stages: design & development, commercial life (including introduction on the market, growth and maturity) and EOL (Figure 3.2). However, these stages are not always clear-cut but often intertwined: for instance, the design and development of smart products, and software in particular, are usually iterative and may evolve after a first version of the product has already been released, requiring users to update their products to access the latest improvements and capabilities. Similarly, when products reach their EOL, additional support may be available for a fee and for a limited period.

Products may be poorly secured when first released, e.g. if the development process did not follow industry best practices, the software may contain many vulnerabilities. In the software industry, where time-to-market is important, the "build first, patch later" approach is common. Alternatively, the level of digital security of a product may be considered sufficient at the beginning of its commercial life, but decrease over time if software developers do not manage effectively the vulnerabilities found in their products, or if other actors do not deploy security updates. Eventually, products tend to become less secure over time as their vendors stop providing security updates, considering that these products have reached EOL.

Figure 3.2. Example of a product lifecycle



Note: Three major stages can be distinguished: design & development (green), commercial life (blue) and EOL (red).
Source: (Dutch Government, 2018[8]).

3.1.1. Design & Development

A significant portion of a product's level of digital security is determined before it is released on the market and purchased.

Weaknesses in code are inherent in the development of software. According to estimates, there are between 20 and 100 weaknesses every 2 000 lines of code (Dean, 2018[14]). To put things in perspective, an average iPhone application has around 50 000 lines of code, while Android has around 12 million and Windows 10 counts more than 50 million (The Economist, 2017[28]). However, as discussed in Section 2.2, not all weaknesses are vulnerabilities, and not all vulnerabilities are critical.

In addition, in many organisations, the teams in charge of developing code and / or products work in silos and do not communicate effectively with those in charge of digital security. Digital security is often not considered as a business priority, especially in SMEs or less digitally mature companies (OECD, 2019[1]). As many products are developed without security in mind, their code, and more broadly their overall architecture, tend to contain many vulnerabilities (Schneier, 2018[6]).

However, the number of vulnerabilities in code can be reduced to one flaw every 2 000 lines if appropriate methodologies are followed (Dean, 2018[14]). The concept of security-by-design intends to address these gaps and to integrate security requirements and principles early on and at every stage of development, as opposed to adjusting or adding security features afterwards at the end of a product's development. Security-by-design methodologies are usually available as industry standards or guidelines[16] and help mitigating "inherent" flaws in code (for a more detailed analysis, see policy discussion report (OECD, 2021[2])). An emerging good practice is also to bridge the gap between the development teams and the digital security teams, through "Development Security Operations", or "DevSecOps" methodologies. These practices rely on very short code development lifecycles where automated security testing and reviews are an inherent part of the product development.

Recent policy research also underlined the importance of developing use-cases early on in the product design process. For instance, NIST recommends IoT manufacturers to undertake the following activities in the "pre-market" phase: identifying expected customers and users, and defining expected use-cases; researching customer digital security needs and goals; determining how to address customer needs and goals; and planning for adequate support of customers' needs and goals (NIST, 2020[28]). The development of use-cases enables supply-side actors to assess and manage digital security risk more accurately. While this practice is more and more common in digitally mature companies, it is much less developed elsewhere, e.g. "traditional" manufacturers (e.g. for home appliances) entering the IoT market.

In an optimal digital security situation, the product's design and development would follow industry standards and best practices for security-by-design. Supply-side actors would balance accurately digital security with other factors, and be incentivised to favour a "secure to market" approach rather than a "first to market" approach (Cyberspace Solarium Commission, 2020[29]).

3.1.2. Commercial life

Managing vulnerabilities during a product's commercial life is as important as investing in the development process to make the product more secure by design. While optimising the level of digital security of a product before its release on the market is important, it is no panacea either: products cannot be secured "once and for all". The digital security of products is an on-going process of adapting to and mitigating risks rather than a static or binary state. Importantly, managing digital security risk in products is an iterative process, which often requires learning from user experience and from failure.

A first gap that may emerge during the commercial life of a product is a misconfiguration that may lead to digital security incidents, e.g. open ports that allow unauthorised parties to access data. The issue of misconfigurations illustrates the complex relations between stakeholders across the value chain, as the right balance between user's autonomy and manufacturer's control is sometimes difficult to achieve. One could argue that misconfigurations arise primarily from a lack of user awareness and education. On the other hand, producers can also be considered responsible if their products are not "secured by default" and rely too much on users and "opt in" mechanisms to enhance the digital security of the product.

Another important gap during a product's commercial life is the management of newly discovered vulnerabilities. It is very likely that any piece of code contains vulnerabilities that are unknown today, i.e. "latent" vulnerabilities (Schneier, 2018[30]). Vulnerabilities can be present but unnoticed for years or decades: some were discovered in Microsoft's Windows XP more than ten years after its release, and years after the end of its commercial life.

Vulnerabilities that have been discovered by some actor (e.g. a security researcher or a malicious actor) but are unknown to, and thus unaddressed by, the party that can mitigate them (the "code owners", see section 3.2 and (FTC, 2018[12])), are referred to as "zero-day" vulnerabilities.[17] They cease to be "zero-day" vulnerabilities once mitigation measures (e.g. a fix or a patch) are available. However, the majority of attacks exploit known vulnerabilities rather than zero-day vulnerabilities (Panetta, 2017[31]), as illustrated by security incidents such as WannaCry, NotPetya or Equifax (Goodin, 2017[32]).

To address newly discovered vulnerabilities, supply-side actors and other code owners need to provide ongoing support for their products, usually through "security updates", "patches" or other mitigations (e.g. instructions to reconfigure the product).

The challenges related to the discovery of vulnerabilities by third-parties (e.g. security researchers), and the policy challenges associated with the disclosure of vulnerabilities, are explored in a separate work stream[18].

Malicious actors are constantly evolving and adapting to security measures, e.g. through designing new techniques and exploits. They look for all possible means of exploiting vulnerabilities. For example, update mechanisms can be compromised to insert malware through supply-chain or man-in-the-middle attacks (Luettmann and Bender, 2007[33]), if proper controls (e.g., input validation, encrypted communications, authentication requirements) are not in place. In 2017, malicious actors used the update mechanism of the accounting software MeDoc, used by the majority of Ukrainian companies, as a threat vector (Greenberg, 2017[34]). The update spread the virus NotPetya, which exploited vulnerabilities in unpatched Microsoft products.

In an optimal digital security situation, products would be "secured by default", limiting as much as possible the possibility of misconfiguration. Products would also have a secured update mechanism, and security updates would be made available and deployed across the value chain in a timely manner.

3.1.3. End-of-life (EOL)

Supply-side actors usually provide security updates only for a period, corresponding to the envisioned product's lifecycle, and often until the release of a new major version of their product. When used by producers, the term "End-of-life" (EOL) actually refers to the end of commercial support, including security updates. In some cases, additional support may be available for a fee, at the customer's request, and only for a period. In many cases, the EOL may not be aligned to the end of use, as products continue to be used even though commercial support has ended.

The EOL gap is the gap between the EOL, decided by the producer, and the end of use, decided by the end-user. If products remain in use after the end of their commercial life, they are likely to become less secure over time as supply-side actors cease providing security updates while malicious actors continue to find and exploit new vulnerabilities. Furthermore, the longer patches and information about a vulnerability is publicly available, the more likely malicious actors will be able to develop and deploy exploits (the "exploit maturity" will likely increase).

In an optimal digital security situation, the end of the commercial life of a product would be aligned with its end of use.

3.1.4. What would be an optimal situation for all stages of the product lifecycle?

In an optimal situation:

- The design & development of products would follow established security-by-design guidelines and standards;
- Products would be secured by default and supported throughout their commercial life. Security updates or other fixes would be provided and deployed in a timely and effective manner;
- The EOL of products would be aligned with the end-of-use.

3.2. Roles and responsibilities of actors

The inaugural event of the OECD Global Forum on Digital Security for Prosperity focused on clarifying the roles and responsibilities of actors for digital security (OECD, 2019[1]). All actors that are part of the value chain have a responsibility in managing the digital security risk of a product. This responsibility varies according to each actor's role, ability to act and to the context (OECD, 2015[17]). The following sections explore the challenges associated with smart products' value chain, and discusses new approaches that can be used to identify relevant actors for the digital security of products.

3.2.1. The supply-side: from vendors to code owners

Supply chain is different from value chain

This report uses the concept of value chain to identify actors that have a direct role in developing a product, from designing or manufacturing components (suppliers) to delivering the product to the end-user (distribution) and offering additional services during the commercial life of a product (customer service, maintenance). The concept of value chain is similar to the concept of supply chain, even though their perspectives are different: the value chain analysis focuses on the added value each step brings for the customer, while the supply chain focuses on the logistics of the production and distribution process.

In the field of digital security, supply chain is often associated with issues related to national security (e.g. State interference), which are beyond the scope of this report.[19] The concept of value chain has therefore been preferred in order to avoid confusion, in line with recent research on digital security at the international level (PI4.0 & RRI, 2020[35]).

The role of value chains in digital security gaps

In recent years, the impact of smart products' value chains on digital security gaps has become a focus of attention for policy makers. In fact, digital security gaps may result from, or be reinforced by, challenges that are associated with smart products' value chains, which are often complex and opaque. In addition, it's increasingly difficult to allocate responsibility across the value chain and to apply liability laws to smart products.

Smart products' value chains are often complex

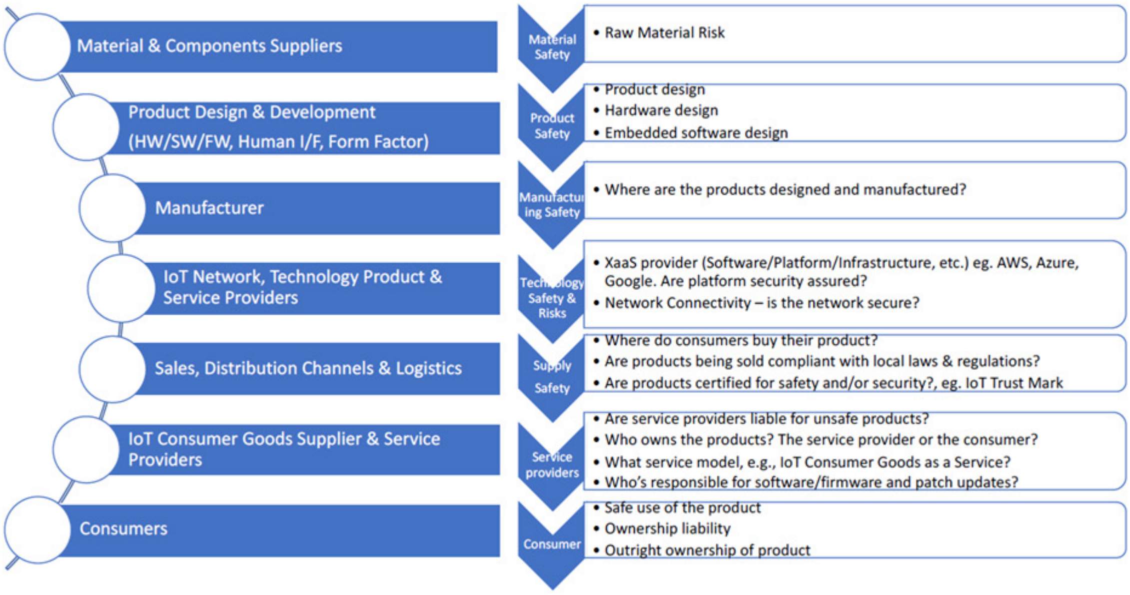
Simply put, a typical value chain can be broken down into at least three steps: production, distribution, and use. For products that contain code, however, the value chain is usually more complex and involves more steps such as design, development, supply, manufacturing, distribution, maintenance and other associated services (e.g. access to internet, application…). Different actors usually manage these steps, and many steps separate the top (or upstream) of the value chain, and the end-user at the bottom (or downstream). For software, even the design phase might involve multiple actors and levels of supply, as software is rarely designed from scratch but involves using existing and often off the shelf components, modules or libraries.

In this report, the term “supply-side actors” is used to encompass all organisations and individuals involved in the product’s value chain. The role of end-users, or the demand-side, is examined in section 3.2.2. The following definitions are key to understand the complexity of the value chain:

- Supply-side actors: all organisations involved in the production and distribution of a product, e.g. manufacturers, service providers and vendors.
    - Suppliers: organisations that supply components to the product’s designer or manufacturer.
    - Product makers or producers: these terms encompass both designers and manufacturers.
        - Manufacturers: organisations responsible for the production of tangible products (e.g. hardware).
        - Designers: organisations responsible for the development of intangible products (e.g. software).
    - Service providers: organisations responsible for the delivery of services.
    - Vendors: customer-facing organisations responsible for the sale of the product.

The value chain and its complexity vary with each product. For instance, the value chain of an iPhone is relatively simpler than for an Android smartphone because Apple performs the role of designer, developer, and sometimes distributor. Its products largely rely on proprietary technology, which enable the vendor to have more control over the product, for instance to issue updates. On the contrary, the value chain of an Android-based smartphone is more complex because it relies much more on open source technology and is highly distributed, with various actors adding their own layer of code (e.g. device manufacturers, network operators). Figure 3.3 provides a detailed example of a product’s value chain.

Figure 3.3. Example of the value chain for consumer IoT


Material & Components Suppliers
Product Design & Development (HW/SW/FW, Human I/F, Form Factor)
Manufacturer
IoT Network, Technology Product & Service Providers
Sales, Distribution Channels & Logistics
IoT Consumer Goods Supplier & Service Providers
Consumers
Material Safety
• Raw Material Risk
Product Safety
• Product design
• Hardware design
• Embedded software design
Manufacturing Safety
• Where are the products designed and manufactured?
Technology Safety & Risks
• XaaS provider (Software/Platform/Infrastructure, etc.) eg. AWS, Azure, Google. Are platform security assured?
• Network Connectivity – is the network secure?
Supply Safety
• Where do consumers buy their product?
• Are products being sold compliant with local laws & regulations?
• Are products certified for safety and/or security?, eg. IoT Trust Mark
Service providers
• Are service providers liable for unsafe products?
• Who owns the products? The service provider or the consumer?
• What service model, e.g., IoT Consumer Goods as a Service?
• Who’s responsible for software/firmware and patch updates?
Consumer
• Safe use of the product
• Ownership liability
• Outright ownership of product

Source: IOTAA (IoT Alliance Australia) and ACCC (Australian Competition and Consumer Commission).

A vulnerability in any code component of the product may lower the level of digital security of the product overall. The more steps separating the component responsible for the vulnerability and the product's end-user, the more difficult it will be to deploy security updates and to fix the newly discovered vulnerabilities.

Smart products' value chains are often opaque

Value chain complexity is not specific to smart products. From cars and drugs to cosmetics and food, many products are designed and processed through global and complex value chains. In these sectors, however, most OECD countries have enacted or are considering enacting legal requirements that impose the traceability of the product and of its components. In many sectors, there is also an increasing pressure from public opinion to increase transparency and traceability in order to achieve various policy goals, e.g. addressing climate change and child labour.

In many OECD countries, legal requirements also usually make producers and/or vendors liable for a defect entailing safety risks in the final product, even if the defects lie in sub-components. This incentivises supply-side actors to manage their supply chain in a more transparent and effective manner.

Such requirements do not exist for smart products. There is no obligation for vendors to provide a list of subcomponents within their products, especially for software. In addition, software licenses, end-user agreements and intellectual property protection measures usually prevent third-parties, including the customer, from testing and evaluating the product's code, as they have no access to the source code (Dean, 2018[14]). The combination of a lack of legal requirements for traceability and of a limited access to the product's code results in the opacity of the value chain for many smart products (EU Expert Group on Liability and New Technologies, 2019[36]).

Allocation of responsibility across the value chain is challenging

The more complex and opaque the value chain is, the more difficult it is to appropriately allocate responsibility in case of digital security gaps, and for actors to coordinate and mitigate risk. Complexity and opacity pave the way for moral hazard, i.e. "any situation in which one person makes the decision about how much risk to take, while someone else bears the cost if things go badly" (Krugman, 2008[37]). For smart products, the actors that make the decision about how much risk to take are often not the actors that bear the costs of the risk (consumers, or the victims of a DDoS attack). In addition, complexity and opacity make it difficult and time consuming to design, coordinate and deploy security updates, as many actors across the value chain may need to take action to implement them.

From the perspective of product liability law, 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, certain components, its operation or from the absence of appropriate warnings regarding its use. While the allocation of responsibility will depend on each specific case, the primary responsibility often lies with the producer and the vendor, as they are legally responsible for the product they circulate on the market.

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 responsibility reflecting an equally complex chain of vendors.

For smart products, the complexity and opacity of the value chain tend to reduce the effectiveness of redress mechanisms, as consumers often do not know to which actor of the value chain they should turn to in case of a digital security incident. In addition, liability laws apply only in specific cases, where the defect results in injuries or damage to property. In many cases, digital security incidents resulting from vulnerabilities in products do not lead to such consequences. The challenges associated with the applicability of liability law to smart products is further discussed in the policy discussion report (OECD, 2021[2]).

Addressing value chain digital security challenges

To address these challenges, it is key to increase trustworthiness and to incentivise co-operation across the value chain. In addition to “traditional” approaches (e.g. quality assurance), which may have limits, new initiatives are underway and seem promising (e.g. code owners, coordinators and software bill of materials).

Increasing trustworthiness through product integrity and quality assurance

Trustworthiness, i.e. the ability of suppliers to meet the expectations of a contract partner in a verifiable way, is key to facilitate co-operation 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 or conformity assessments (PI4.0 & RRI, 2020[35]).

Quality assurance is also an important tool for manufacturers to verify that actors across the value chain act responsibly. It helps to ensure the integrity of the components that producers use to manufacture a product. The quality assurance process relies on defining requirements, through contracts for instance, and on controlling that these requirements are met, for instance through conformity assessments such as product testing, audits, certifications and accreditations (see the policy discussion report (OECD, 2021[2])).

However, quality assurance is costly. In many cases, market dynamics fail to properly incentivise manufacturers to allocate enough resources to quality assurance (see section 3.3). Advanced organisations that have mature value chain risk management processes often include digital security as a component of their product integrity and quality assurance processes. Less mature organisations typically have separate quality assurance and digital security risk management programs, and are not sufficiently incentivised to develop and coordinate such programs.

The use of emerging technologies such as artificial intelligence and blockchain to increase the traceability and transparency of products and components across the value chain is promising but also comes with challenges, which could be further explored (see Annex B).

Increasing traceability through software bills of materials

In the United States, the software bill of materials (SBOM), proposed by the National Telecommunications and Information Administration (NTIA), aims to explore the feasibility of incentivising supply-side actors to be more transparent about the components used in smart products, including code components such as software libraries. The National Institute for Standards and Technologies (NIST) has also developed specific tools to enable organisations to better understand and manage digital security supply chain risks (NIST, 2020[38]). At the international level, the Charter of Trust has put forward baseline requirements that companies can refer to in order to support quality assurance. These initiatives are further discussed in the policy discussion report (OECD, 2021[2]).

Increasing co-operation across code owners

As described in the previous sections, managing the digital security of products that contain code requires co-ordination across many steps of the value chain. While vendors have a legal responsibility towards their customers, other supply-side actors often have a role to play in managing digital security risk. This section explores other concepts[20] that may prove useful to better understand the dynamics amongst the actors who manage the digital security of products.

Focusing policy attention on the vendor and the product manufacturer or designer has limits. When vulnerabilities arise at a lower level of the value chain, it is also more difficult for all actors to co-ordinate and respond effectively. For example, in recent years, vulnerabilities have been discovered in the implementation of certain Internet protocols (Heartbleed, 2014) or in microprocessors (Spectre and Meltdown, 2017). In both cases, co-ordination to handle the vulnerability and mitigate it was very challenging. In fact, the vulnerable components were widely used, and their vulnerabilities affected all the products they were part of, such as websites and smartphones. Some have argued that these vulnerabilities could be considered as a new class of "systemic" vulnerabilities, a concept further explored in the Annexes. These examples illustrate how final vendors (e.g. providers of websites and smartphones) are not always the best placed to fix component vulnerabilities.

As discussed in section 2.3.3, many products are complex systems that include other products in some way, which is often referred to as "product interdependency". As a result, ISO has developed the concept of "intermediate vendor" (ISO, 2014[26]), i.e. an organisation that gets a subsystem from a vendor and uses it to supply a system or service (or a combination of both) to a user or another intermediate vendor. For example, telecommunication providers may supply a mobile phone together with a service contract. While intermediate vendors did not manufacture the product, they often have a legal responsibility to inform their customers about vulnerabilities in their products, as the customers may need to stop using the device or some of its functionality. Intermediate vendors may also be technically capable of developing workarounds to mitigate the vulnerabilities.

A recent report from the EU Expert Group on Liability and New Technologies (2019[36]) highlighted that beyond producers, many organisations have a responsibility for managing the digital security of a given product. The report uses the term "operator", defined as the (legal) "person who is in control of the risk connected with the operation of emerging digital technologies and who benefits from their operation". The report further distinguishes between "the person primarily deciding on and benefiting from the use", or "frontend operator", and "the person continuously defining the features of the relevant technology and providing essential and ongoing back end support", or "backend operator". For the authors, operators have a duty of care regarding the products for which they have a responsibility, in particular for design, monitoring and maintenance.

However, the term of "operator" may be misleading. It could be confused with network operators, or operator of critical activities, and many organisations have some responsibility even though they do not directly "operate" the product, as shown in the case of the Heartbleed vulnerability.

Therefore, this report will rather use the concept of "code owners" which is emerging as a good practice to better manage digital security across the value chain (FTC, 2018[12]). A code owner is the individual or organisation that is best placed to fix the layer of code that is vulnerable. Importantly, the concept of "code owner" is not necessarily related to intellectual property or legal ownership. It rather refers to the responsibility of the individual or organisation for a specific layer of code. In fact, a specific actor should own the responsibility to manage the security of each layer of code in a product. The code owner can be the developer of the code, the team that developed the code, the organisation that integrated the code in their product or that is in charge of its maintenance. This concept can be used to map all actors responsible for various layers of code:

- The chip manufacturer owns the deep level code on hardware;
- The operating system designer owns the operating system code;
- An open-source organisation may own a software library;
- The application designer owns the application code, etc.

When a code owner discovers or is notified of a vulnerability, they should handle it, i.e. propose workarounds, develop a patch for the code, and convey the vulnerability and patching information to its downstream and upstream partners, for example via regular security bulletins. For a given product, all layers of code should be clearly owned by a specific organisation. Beyond code ownership, it is also important for stakeholders to be able to trust the code, for instance through developing a "chain of trust" between partners. Principles and initiatives to develop trust are further explored in the policy discussion report (OECD, 2021[2]).

Identifying code owners does not challenge the legal responsibility of the vendor and the product manufacturer. In fact, in most OECD countries, the vendor is primarily responsible for any flaw that may pose safety risks to end-users, who are usually entitled to claim compensation from the vendor. The vendor is usually the "go-to" point for consumers in case of defect. The vendor may in turn claim compensation from the manufacturer, which may in turn claim compensation from suppliers, as in fact all of them can be considered as code owners.

Digital security gaps may arise in case there is:

- A lack of clarity and transparency regarding the allocation of responsibility across code owners. For instance, a vendor may not be aware of which actors own which layer of code;
- A lack of co-operation: even if there is clarity and transparency regarding the allocation of responsibility across code owners, there may be gaps related to the organisational and technical ability to co-operate;
- A variability in ability to act: even if there is transparency and co-operation, the code owners may have different levels of resources allocated to develop and deploy patches. This may result in delays or failure to process security updates.

The key role of coordinators

To better identify and allocate digital security risk, best practices show that at least one actor should step up as a coordinator. A coordinator is an entity facilitating the identification and allocation of responsibility across actors, and mainstreaming digital security best practices across the value chain.

For instance, intermediate vendors – a concept developed by (ISO, 2018[39]) and discussed above – such as telecommunications operators can sometimes have a positive effect on the management of digital security risk across the value chain by leveraging a significant market share to positively influence actors within the value chain. For example, in 2016, when many connected products were targeted by a variant of the Mirai malware in Germany, Deutsche Telekom worked with router manufacturers to accelerate the development and deployment of workarounds and security updates, in order to limit the impact of the malware on their networks and customers.

Similarly, best practices for vulnerability disclosure and management often leverage a trusted third-party acting as a coordinator between security researchers and code owners in a coordinated vulnerability disclosure process (see the vulnerability treatment report (OECD, 2021[3])). In their intermediate positions, these actors increase the level of co-operation across the value chain and therefore enable a better allocation of responsibility. Other third-parties such as certification bodies and insurance companies are also likely to have a positive impact on improving the allocation of responsibility across the value chain and mainstreaming digital security best practices.

The organisation best placed to assume the role of coordinator will vary for each category of products, depending on stakeholders' ability to act and on the context (OECD, 2015[19]). The coordinator could be the product's vendor, an intermediate vendor, a large company that can influence the value chain through their procurement and contract policies, an insurance company, a network operator, a technical body (e.g. a CERT) or a government agency. Products with a suboptimal level of digital security often lack, within their value chain, an institutionalised coordinator. The capacity of the coordinating body to build trust with all relevant stakeholders is also key.

3.2.2. The demand-side: mainstream and advanced users

While value chain analysis usually focuses on the supply-side, it is also important to take into account the demand-side when addressing digital security risk in products. In many cases, end-users (e.g. consumers or SMEs) are not able to properly perceive and assess the level of digital security of the products they use, which leads them to make suboptimal purchasing decisions, misconfigure certain products or not implement security updates in a timely manner. In other cases, certain end-users are fully able to perceive and assess the risk, and show a preference for more autonomy and control (e.g. corporate users such as industrial firms or individuals like security researchers). In that respect, it seems important to make a distinction between at least two categories of end-users:

- "Mainstream users", including consumers and some corporate users like SMEs. They often have limited skills and knowledge about digital security, are typically less aware of the associated risk, struggle to appropriately perceive and assess them, and have limited resources to manage them.
- "Advanced users" possess higher digital security skills, are more aware of the risk and may need to have more control over the products they use. They can have more resources to manage security risk. This category of more experienced, autonomous users is broad and ranges from "geeks" and tech savvy hobbyists to users in professional environments and trained security experts. Many of these users typically value the ability to reverse engineer a product (analyse "what is in the box") and test security updates before deployment.

The main difference between "mainstream users" and "advanced users" is the level of digital maturity, which is determined by several factors such as skills and financial resources. While some organisations may have significant financial resources, they may not allocate enough of these resources to digital security, consider digital security as a strategic issue or have developed a risk-based approach to digital security. Therefore, despite significant resources, these organisations have a relatively low level of digital security maturity, closer to that of "mainstream users". This was illustrated by the WannaCry digital security attack in 2017 (see Box 4.1), which severely impacted global companies leading in their respective sectors (e.g. transport, automotive), as opposed to only SMEs or individuals.

3.2.3. Threat actors and security researchers

While the value chain approach is a good starting point, it may also be limited as some stakeholders have a key impact on the digital security of products but are not necessarily part of the supply-side or the demand-side.

- Threat actors need to be taken into account to design and implement adequate digital security measures (threat assessment and modelling is a key element of "security-by-design" best practices) ;
- Security researchers can play a key role in identifying and helping to mitigate latent vulnerabilities. In this area, there is an untapped potential resulting from the absence of vulnerability handling processes and disclosure policies in many organisations, including a lack of effective management of the relations with security researchers. Legal barriers may also prevent security researchers from contributing effectively. Good practices tend to integrate those actors into the product value chain, for example through bug bounties, hackathons or vulnerability disclosure policies. The challenges related to vulnerability disclosure are examined in the vulnerability treatment report (OECD, 2021[3]).
- In addition, other economic agents can be impacted by the digital security of products in the case of negative externalities, e.g. targets of a DDoS attack.

3.2.4. The complex role of governments

Governments are key actors in the digital security ecosystem. However, the term "government" is used in a variety of contexts, and can refer to different types of entities, from national ministries or agencies to local communities (e.g. regions and cities) and other public organisations in certain sectors such as healthcare and education (e.g. hospitals and universities). Even referring to national government only entails a certain complexity, as different types of entities may have a role in digital security policy, including agencies only responsible for protection (e.g. ANSSI in France), agencies responsible for both defense and offense (e.g. the NSA in the US) or potential victims of digital security incidents (any type of governmental organisation).

Depending on the context: national governments can have the following roles:

- Regulators: governments can develop policies to incentivise stakeholders to better address digital security gaps in products.
- Economic agents, or demand-side actors:
  - As customers of smart products, governments may be considered as "mainstream users" (e.g. public healthcare institutions) or as "advanced users" (e.g. the agency in charge of digital security).
  - As economic agents, governments may also incentivise other actors, in a market rather than policy oriented manner. In particular, governments can lead by example (e.g. by implementing digital security risk management practices) and use their purchasing power to incentivise positive behaviour through defining public procurement requirements for digital security (e.g. by requiring government contractors to meet certain standards of trust).
- Supply-side actors: governments that provide smart products (e.g. online services) may be part of the product's value chain, and could be considered as "code owners" (see section 3.2.1).
- Digital security actors: governments can be considered as security researchers (e.g. a digital security agency specialised in protection) or as threat actors (e.g. an agency specialised in offense). These roles can generate conflicts within the government. The vulnerability treatment report (OECD, 2021[3]) further discusses the issue of trust in government in relation to vulnerability treatment. Core national security issues are out of the scope of this report (see section 1.1).

3.2.5. What would be an optimal situation?

In an optimal situation, there would be transparency regarding which actor owns which layer of code. Code owners would swiftly handle the vulnerabilities they are aware of in order to provide timely and effective remedies. They would follow risk-based methodologies to prioritise the mitigation of vulnerabilities (e.g. prioritising the development of a patch for high-risk vulnerabilities). Actors within the value chain and in the wider ecosystem would effectively co-operate to deploy those remedies in a timely manner. A coordinator would be available to streamline the process.

3.3. Market dynamics

In addition to the product's lifecycle and the roles and responsibilities of actors, market dynamics need to be taken into consideration to assess potential gaps. The market dynamics responsible for potential gaps are often referred to as market failure. This section introduces the main sources of market failure, namely a lack or misalignment of incentives, information asymmetries and negative externalities (Kopp, Kaffenberger and Wilson, 2017[20]; OECD, 2019[1]).

3.3.1. Misalignment of incentives

"Security failure is caused by bad [economic] incentives at least as often as by bad [technical] design" (Anderson and Moore, 2006[40]). Incentives are defined as elements that influence the rational behaviour of economic agents towards a certain direction. Incentives are misaligned when the market favours a rational behaviour for economic agents that is detrimental to the optimal level of digital security.

In some cases, economic incentives are at least partially aligned to drive actors to reach an optimal level of digital security. In competitive markets, supply-side actors are often incentivised to innovate and deliver quality products (including regarding digital security) to satisfy customers. However, those incentives are sometimes misaligned. This report focuses on those gaps.

A first example of misaligned incentives relates to emerging and highly innovative markets. These markets are often characterised by network effects which result in a winner-take-all dynamic, where a premium is placed on moving first in a market ("first-mover advantage") in order to ensure market dominance (Dean, 2018[14]). These market dynamics incentivise product designers and manufacturers, as Facebook has described it, to "move fast and break things" (Schneier, 2018[30]), rather than to sufficiently test their products and follow security-by-design guidelines. In these markets, cost-effectiveness, time-to-market and usability are often more valued than security:

- **Cost-effectiveness**: putting in place an update mechanism and hiring a team in charge of managing it will raise the price of the product. Moreover, maintaining existing software may divert resources from the development of new products (FTC, 2018[12]).
- **Time-to-market**: going through the process of securing products by design (e.g. through penetration testing, certification, labelling…) will be costly and delay the release of the product. "Time-to-market is lengthened by software testing and the cost of software development is increased", which "may result in significantly reduced revenues over the product life cycle" (Anderson and Moore, 2006[40]).
- **Usability**: making a product more secure could make it less user-friendly, which could negatively affect the demand for that product (e.g. requiring the end-user to remember long and complex passwords). More recent approaches to digital security aim to better integrate usability and functionality considerations in the development of digital security features.

From a demand-side perspective, mainstream end-users such as consumers and SMEs are less aware of the risk, and will likely take into account price, features and usability rather than digital security when choosing a product. It is difficult for those users to assess digital security, and they very often take for granted that regulatory requirements or mandatory standards set a minimum level of digital security and apply for all products they can buy, even though it is not the case (DCMS, 2018[13]) (Consumers International, 2019[41]). From a supply-side perspective, it can also be rational for product manufacturers and designers to not invest in digital security, as this investment would raise the price of the product while its results could be difficult to communicate to their customers (DHS and DoC, 2018[42]), and could affect negatively other factors such as usability. Information asymmetries can greatly reinforce the misalignment of incentives, as discussed in the next section.

Another example of misaligned incentives relates to more mature markets. It is challenging for software designers to achieve growth once they have reached market dominance, as it implies that they have to compete with their own installed base. For instance, it could be argued that one of the main competitors for Microsoft is Microsoft, as consumers need to be incentivised to buy the new version of Windows each time a new version is released. The issue was examined by Ronald Coase (1972[43]), and is usually referred to as the "durable goods monopoly problem". Corporate strategies to overcome this challenge include the following, according to Varian and Shapiro (1999[44]):

- Accelerating the rate of innovation through R&D, adding new functionalities or increasing the capacity of new products (e.g. Moore's Law on microprocessors' performance).

- Shifting from selling goods towards providing services based on a subscription model. Microsoft, for instance, has begun to offer Windows 10 as a service, which keeps customers on the most recent and secure version of software.
- Encouraging “planned obsolescence”, e.g. by stopping providing security updates, or updating firmware and operating systems to the point that older hardware capabilities are too low, hence diminishing performance and incentivising customers to buy new products.

The “durable goods monopoly problem” underlines misaligned incentives, as supply-side actors may be incentivised to shorten the commercial lifecycle of their products, which also affects their level of digital security, e.g. by limiting to a few years the warrantees or the delivery of security updates.

Alternatively, there are obvious incentives on the demand-side to continue using products after their EOL. For end-users, economic rationality consists in enjoying the benefits provided by the product for as long as possible. Consumers do not stop using a washing machine or a fridge after the guarantee expires: they use the product until it ceases to function, or until their needs are no longer fulfilled, for instance because new products have been released and could provide more satisfaction. Similarly, end-users keep on using their smart products after their EOL. Upgrading or acquiring new products usually incurs direct as well as indirect costs, such as interrupting production lines and managing the transition for the whole digital ecosystem.

Policy remedies exist to better align incentives, for instance through legal requirements regarding transparency or minimum security features. However, even if market incentives are aligned, the market could still fail to deliver optimal outcomes, in case economic agents misperceive risks or in the presence of information asymmetries and negative externalities.

3.3.2. Information asymmetries

Significant information asymmetries may aggravate the misaligned incentives described above. Information asymmetries refer to a market situation where one of the parties (usually the seller) has more information on the product than the other party (usually the buyer). Consequently, it is difficult for buyers to assess the quality of the products they buy, which leads to suboptimal market outcomes.

Nobel-prize winning economist George Akerlof first explored information asymmetries in his article “*The Market for Lemons*[21]*: Quality Uncertainty and the Market Mechanism"* (Akerlof, 1970[45]). For certain products, quality is difficult, if not impossible, to assess. This is particularly true of unregulated markets for products with a strong technical dimension. In his article, Akerlof takes the example of the secondary market for cars, where it is extremely difficult for prospective buyers to evaluate the quality of the product before the purchase.[22] Information asymmetries usually result in:

- Moral hazard**:** the seller of the “lemon” is aware of the low quality of the product, but does not face any consequences for it, see section 3.2.1 and (Krugman, 2008[37]).
- Adverse selection: in the end, only low-quality products are sold on the market, because sellers of higher quality (and more expensive) products cannot differentiate their products from those of their competitors.

Information asymmetries apply to many markets for products that contain code (Anderson, 2001[46]). It is difficult for consumers and businesses to assess the level of digital security of products and to properly consider it, among other factors, when making purchasing decisions (DCMS, 2018[47]). Digital security is not easily assessable, unlike usability and price (two pieces of information easily available to the prospective buyer). This can lead to adverse selection: because most users cannot distinguish more secure from less secure software, “developers are not compensated for costly efforts to strengthen their code” and are incentivised to sell products that are less secure (Anderson and Moore, 2006[40]).

During the COVID-19 pandemic, 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 some supply-side actors (Hay Newman, 2020[48]), 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 teleconferencing tool often relied on other factors than digital security, such as a functionality and usability.

One could argue that information asymmetries also exist in the other direction. For mass markets in particular, supply-side actors may lack insights regarding the context of use of their products, including the customer's risk appetite or the interactions between their products and other systems. To tackle these information asymmetries, supply-side actors need to integrate in their design processes the development of use-cases and the definition of users' digital security goals and preferences, and to exchange relevant information with their customers through well-defined communication strategies (NIST, 2020[28]).

While information asymmetries could apply to all products in theory, this greatly varies in practice. Akerlof (1970[45]) noted that remedies can correct information asymmetries, such as brand reputation, warranties and certifications (e.g., requiring a seller to provide a "road-worthy" certificate, in the case of purchasing a car).

3.3.3. Externalities

Externalities refer to the consequences of the production or consumption of a product on third-parties that were not involved in any related transaction – i.e. which are not part of the product's value chain. The archetypal example of a negative externality is the pollution of a river by a factory, which negatively affects a city downstream. If the relevant stakeholders are not incentivised to take into account – or "internalise" – those externalities (e.g. through regulatory requirements or taxes), it typically results in suboptimal market outcomes.

The case of "botnets" (i.e. networks of infected machines) is a good example of a negative externality, as the social costs of Distributed-Denial-of-Service (DDoS) attacks are not borne by the stakeholders responsible for managing the digital security of the product, which include the end-users of the compromised devices, the device manufacturers and the internet service providers. The negative externality is reinforced by the fact that the owners or end-users of a compromised device are usually unaware that their devices are used as part of a botnet. As noted by (DCMS, 2018[47]), "manufacturers are unlikely to face immediate economic costs borne by a DDoS attack conducted through their devices, and therefore do not face sufficient commercial incentive to invest in a secure by design approach".

Some consider that negative externalities also arise when complex value chains put the entity taking the risk further away from the entity bearing the risk. For instance, if a third-party software developer poorly designs the firmware of a connected device, the risk is ultimately borne by the end-user if the product is compromised. Between the end-user and the software developer, a number of intermediaries may dilute responsibility, including the product manufacturer, the brand, the retailer and other third-parties (e.g. cloud service or internet service provider). However, because all these entities have entered into a transaction at some point, it might not fit the classic definition of "externalities", but rather fall under the category of "moral hazard" and information asymmetries. Externalities are sometimes confused with moral hazard. The difference between the two lies in the fact that the stakeholders subject to moral hazard are part of the product value chain (e.g. the manufacturers and the users), while the stakeholders impacted by externalities are not part of the value chain, and therefore do not enter in a transaction with other actors of the value chain.

3.3.4. What would be an optimal situation?

In an optimal situation:

- All stakeholders would be sufficiently incentivised to provide an acceptable level of digital security;
- There would be enough transparency so that customers are able to correctly assess the level of digital security of the products they use;
- Externalities would be internalised in the product's value chain.

4 Case studies

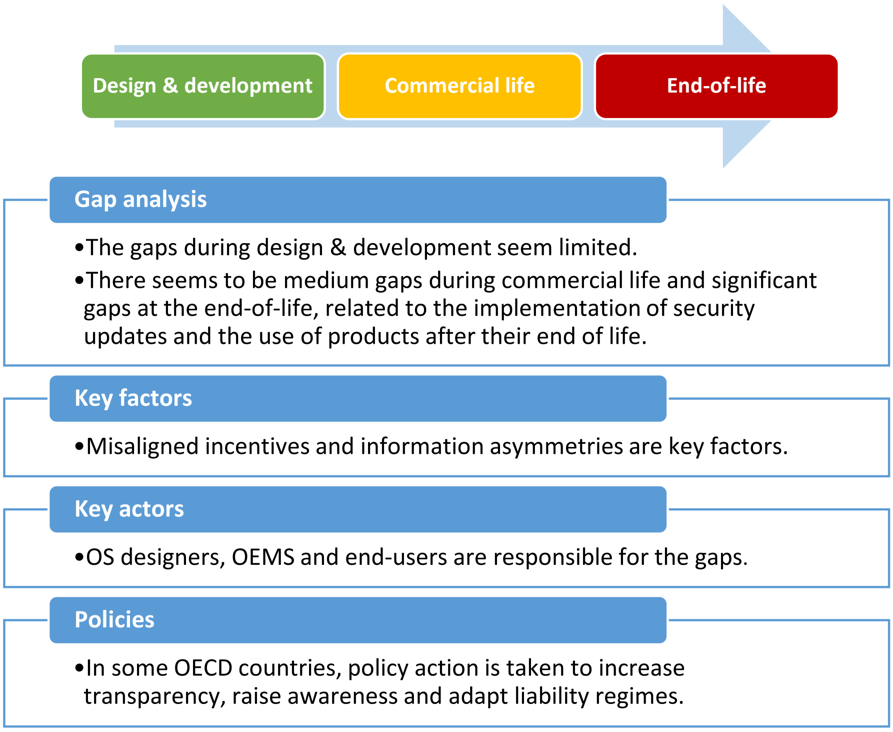
The analytical framework presented in chapter 3 has been applied to three categories of products: desktop computers and smartphones (case study 1), consumer IoT (case study 2) and cloud services (case study 3).

The following sections provide the main findings and key takeaways of these case studies. The detailed analysis of the case studies can be found in Annex A.

4.1. Case study 1: smartphones and desktop computers

The main findings of case study 1 (see Figure 4.1) are that the designers of major operating systems usually follow best practices and standards during design & development, and provide security updates throughout the commercial life of the product. However, OEMs and end-users[23] tend to not cascade and implement security updates in a timely manner during the product's commercial life. There is also a significant gap between the EOL as envisioned by the producer and the effective end of use. These gaps can be explained, *inter alia*, by misaligned incentives, a misperception of risk, externalities and information asymmetries. Policy action to enhance the digital security of smartphones and desktop computers could therefore prioritise incentivising stakeholders to deploy security updates in a timely manner, and to use and support products for a reasonable period.

Figure 4.1. Summary of the findings for case study 1: smartphones and desktop computers



Gap analysis

- The gaps during design & development seem limited.
- There seems to be medium gaps during commercial life and significant gaps at the end-of-life, related to the implementation of security updates and the use of products after their end of life.

Key factors

- Misaligned incentives and information asymmetries are key factors.

Key actors

- OS designers, OEMS and end-users are responsible for the gaps.

Policies

- In some OECD countries, policy action is taken to increase transparency, raise awareness and adapt liability regimes.

Note: at each stage of the lifecycle, the colour reflects the breadth of the gaps. Green = limited gaps, orange = medium gaps, red = significant gaps.
Source: OECD.

Box 4.1 provides insights from a recent digital security incident that affected desktop computers' operating systems.

Box 4.1. The WannaCry ransomware (2017)

Description

The WannaCry malware appeared in May 2017 and targeted computers running on Microsoft Windows operating systems. It drew on EternalBlue and DoublePulsar, two exploits presumably developed by the United States' National Security Agency (NSA) and leaked by the hacker group "Shadow Brokers" in April 2017. WannaCry was a ransomware: it encrypted all data on infected computers, making them entirely unavailable until a payment in Bitcoin was made to the perpetrators.

In April 2017, more than a month before the attack began, Microsoft released a security update to patch the vulnerabilities that were later exploited by WannaCry. However, the update was only released for the versions of Windows that were still commercially supported at that time, which included Windows Vista and 7, but not, for instance, Windows XP and Server 2003, which had reached their EOL. However, the latter were still widely used by less digitally-mature organisations, such as SMEs and institutions in the healthcare sector. The day after the attack began, on 13 May, Microsoft released an emergency security update for the Windows versions it no longer supported.

Impact

In just a few days, the virus managed to infect around 200 000 computers in more than 150 countries, without any user interaction. Many organisations and businesses in OECD countries fell victim to WannaCry, including Renault, Honda, Boeing and the National Health Service (NHS) in the United Kingdom (UK). Those organisations were infected because they had not implemented the security updates provided by Microsoft, or because they used Windows versions that had reached their EOL.

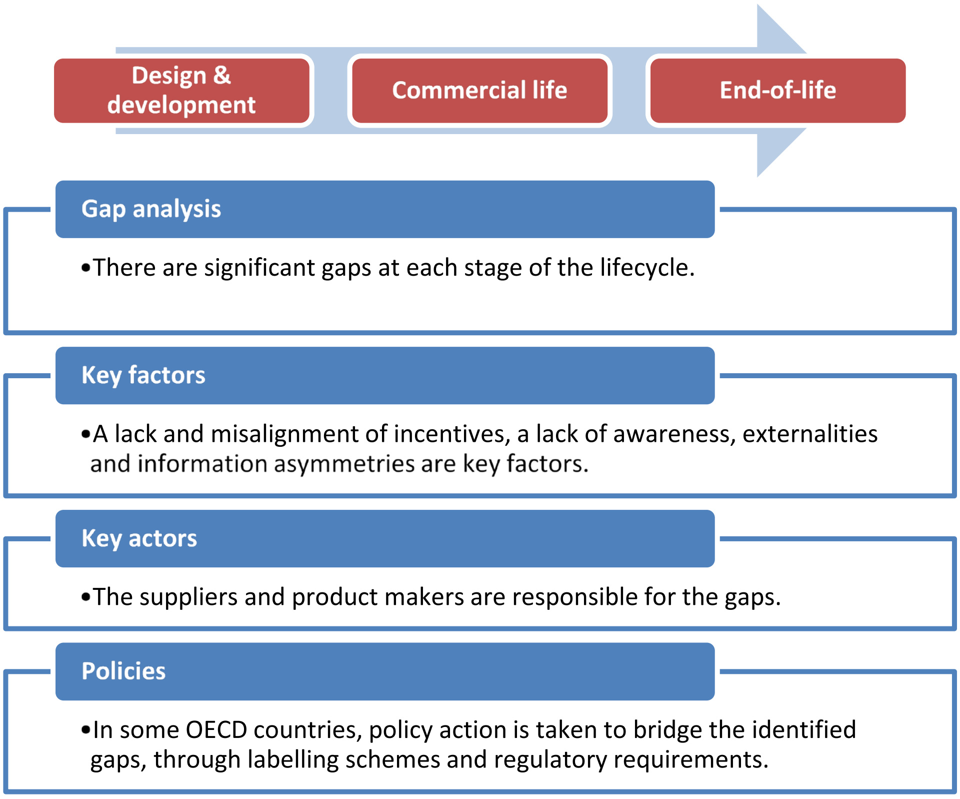
Some of the organisations that fell victim to WannaCry could be considered as "mainstream users" (see section 3.2.2), i.e. organisations that are less digitally mature, usually because of limited skills and financial resources dedicated to digital security (e.g. in the healthcare sector). However, other victims included global organisations that were leaders in their sectors (e.g. transport or automotive). It demonstrates that the dynamic management of digital security risk, including patch management and treatment of the EOL gap, is a key issue that affects stakeholders beyond those that would usually be considered as "mainstream users" (e.g. SMEs and consumers) .

The virus seriously impaired the functioning of hospitals, plants and production lines. According to estimates, total damages range between hundreds of millions to several billions EUR (Berr, 2017[49]) (e.g. inability for the organisation to properly function for weeks, costs of cleaning up, upgrading or replacing compromised information systems, brand reputation, etc.). In 2018, semi-conductor manufacturer TSMC had to shut down its production line for days due to a virus similar to WannaCry.

4.2. Case study 2: consumer IoT products

The main findings of case study 2 (see Figure 4.2) are that there are significant gaps regarding the digital security of consumer IoT products at every stage of their lifecycle. In many cases, IoT products lack basic security features such as an update mechanism or strong authentication requirements, and are not secured by default, making it easy for users to misconfigure their products. In the IoT market, many supply-side actors do not have adequate resources to manage the discovery, disclosure and mitigation of newly discovered vulnerabilities. Finally, in many cases, there are no formal policies regarding IoT products' EOL, which will likely not be aligned with its end of use. Policy action to enhance the digital security of smartphones and desktop computers could therefore address each stage of the lifecycle and focus on incentivising supply-side actors to be more responsible.

Figure 4.2. Summary of the findings for case study 2: consumer IoT products



Gap analysis

- There are significant gaps at each stage of the lifecycle.

Key factors

- A lack and misalignment of incentives, a lack of awareness, externalities and information asymmetries are key factors.

Key actors

- The suppliers and product makers are responsible for the gaps.

Policies

- In some OECD countries, policy action is taken to bridge the identified gaps, through labelling schemes and regulatory requirements.

Note: at each stage of the lifecycle, the colour reflects the breadth of the gaps. Green = limited gaps, orange = medium gaps, red = significant gaps.
Source: OECD.

Because the IoT market is still emerging, and many IoT products lack basic security features, most of the policy debate regarding the digital security of IoT has focused so far on the first stage of their lifecycle (design & development), and incentivising supply-side actors to follow "security-by-design" and "security-by-default" standards and guidelines. While it is legitimate that policies address these areas in the short term, gaps are also significant during the commercial life of IoT products as well as after their EOL. The challenges identified in the first case study on smartphones and computers, such as the suboptimal deployment of security updates and the gap between the EOL and the end-of-use, are likely to affect IoT products as well.

To avoid the emergence of the "Internet of forgotten things", some authors have suggested to empower stakeholders such as the technical community to maintain connected devices after the end of their commercial life (Zittrain, 2018[50]). Non-profit "foundations could maintain the code for abandoned products", "like the way the Mozilla Foundation has transformed the 1998 Netscape browser long after its originators left the scene". However, challenges in terms of access to source code, intellectual property rights and responsibility ownership may limit the feasibility of this idea (see the policy discussion report (OECD, 2021[2])).

Box 4.2 provides insights from a recent security incident that affected consumer IoT products.

Box 4.2. The Mirai Botnet (2016)

Description

The Mirai (Japanese word for "future") malware appeared in 2016 and specifically targeted Internet of Things (IoT) devices running on Linux (a family of open-source operating systems) such as digital video recorders, security cameras, air-quality monitors, printers and home routers. The commonality of these connected devices was that they were poorly secured (Schneier, 2018[6]), using common credentials that were not changed from their factory defaults (e.g. 0000 for password). These vulnerabilities enabled the Mirai malware to easily take control of the devices, without any user interaction. Infected devices became part of a botnet (i.e. a network of robots) remotely controlled by a malicious actor, and then automatically scanned their network in search of other vulnerable machines. According to estimates (Antonakakis et al., 2017[51]) hundreds of thousands of devices were infected, peaking at 600 000 in November 2016.

The Mirai botnet was then used to perpetrate Distributed Denial-of-Service attacks (DDoS), a "classic" type of attack breaching the availability of a system (e.g. website) by flooding it with requests from a large number of IP addresses, hence preventing legitimate users to access it during a few minutes or for entire days. While DDoS attacks leveraging botnets of infected desktop computers have been used for decades, the specificity of Mirai was to infect insecure IoT devices.

Impact

In September and October 2016, the Mirai botnet targeted, among others, digital security journalist Brian Krebs and French cloud computing and web hosting company OVH, as well as Domain Names System (DNS) service provider Dyn. The latter attack led to the unavailability of the websites of Dyn's clients, which included Netflix, Spotify, Amazon and Twitter. The Mirai source code was made public in October 2016, enabling many, including unexperienced hackers, to use it. The following month, dozens of "clones" emerged, one of them disrupting more than 900 000 routers of Deutsche Telekom.

For the owners of the infected devices, the impact is low and usually unnoticeable, except for an increased bandwidth usage during the scanning and attacking phases. For the targets of the DDoS attack, there is a debate about the severity of the impact. A DDoS attack usually does not impact the integrity or confidentiality of the product and associated data. Some consider that the unavailability of a website (but not of internal information systems, which still function) for a few hours or days mostly amounts to annoyance. Consequently, they would consider that a DDoS attack would rank lower, in terms of severity, than a personal data breach for instance. Others, however, consider that a DDoS can incur significant costs, e.g. due to the damage on brand reputation and the loss of potential sales for e-commerce platforms (in the case of Dyn and its clients, estimated costs amount to more than USD 110 million). It could also be argued that in the future, massive DDoS attacks could have much more severe consequences, for instance if they result in the unavailability of a network on which autonomous vehicles rely on to function (in this case, a DDoS attack could result in car accidents and potentially casualties). In fact, the severity of a digital security attack should be assessed on a case-by-case basis, taking into account the context, and not solely on the basis of the type or category of attack.

The Mirai botnet attacks demonstrated the global nature of the risk posed by widely used products with a suboptimal level of digital security. Most of Mirai's targets were located in the United States, while most of the infected devices were located in other jurisdictions, such as Brazil, Colombia and South Korea (Antonakakis et al., 2017[51]). Many experts agree on the need for global and coordinated action to enhance the security of IoT devices to prevent their exploitation for botnet attacks (DHS and DoC, 2018[42]).

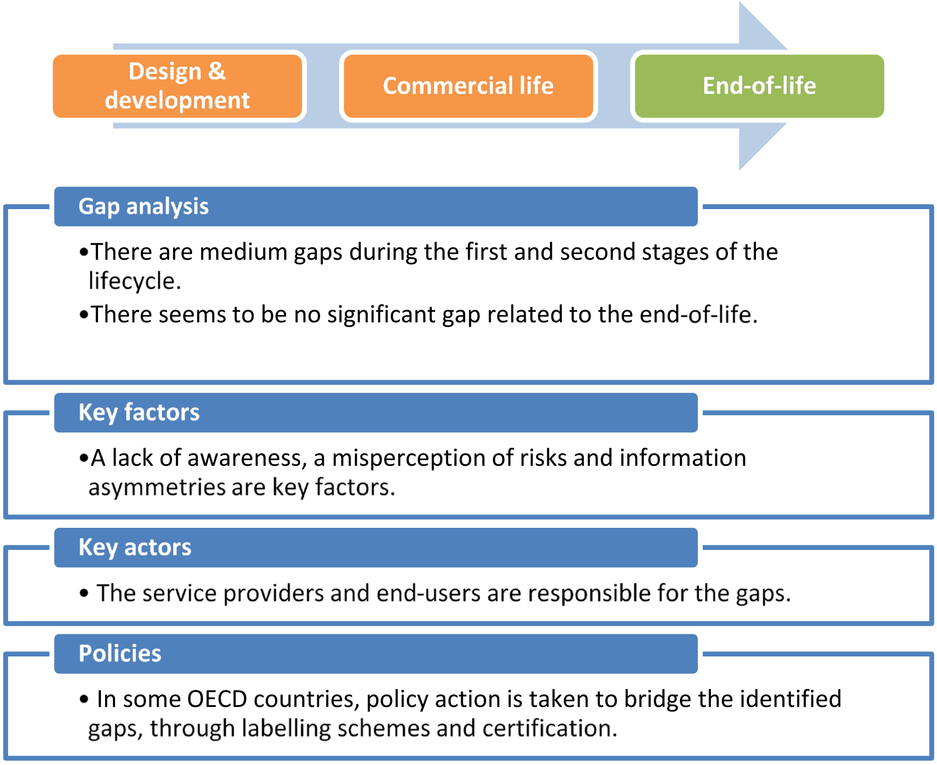
Product safety

While the Mirai malware focused on creating botnets to launch DDoS attacks leading mostly to financial and reputational damages (see Box 4.2), vulnerabilities in IoT products can also be exploited to trigger more tangible negative outcomes. One might argue that DDoS attacks on websites would rank low to medium in terms of severity, while attacks with physical consequences (e.g. making a pacemaker defective or taking control of a connected car) would rank much higher, with significant effects on consumer safety. A significant trend in IoT security is a growing concern regarding potential impacts on the integrity and availability of products and data, which can directly affect safety (Schneier, 2018[6]). Consequently, security breaches in connected devices will likely have more severe consequences in the coming years (e.g., hacked vehicles could cause a number of casualties, as opposed to a breach of personal data).

4.3. Case study 3: cloud services

The main findings of case study 3 (Figure 4.3) are that the digital security gaps for cloud services are mostly related to the architecture of cloud environments, and arise during the commercial life. They result from a lack of user awareness or education, a failure to fully implement “security-by-default” principles, a misperception of risks and a difficult attribution of responsibility across the value chain.

Figure 4.3. Summary of the findings for case study 3: cloud services



Gap analysis

- There are medium gaps during the first and second stages of the lifecycle.
- There seems to be no significant gap related to the end-of-life.

Key factors

- A lack of awareness, a misperception of risks and information asymmetries are key factors.

Key actors

- The service providers and end-users are responsible for the gaps.

Policies

- In some OECD countries, policy action is taken to bridge the identified gaps, through labelling schemes and certification.

Note: at each stage of the lifecycle, the colour reflects the breadth of the gaps. Green = limited gaps, orange = medium gaps, red = significant gaps.
Source: OECD.

To enhance the digital security of cloud services, the following opportunities could be further explored:

- Supporting the development of common standards to provide stakeholders with references, in particular to clarify the roles and responsibilities of each actor (e.g., which security controls are the responsibility of the cloud provider, and which ones are the responsibility of the user).
- Encouraging cloud providers to clarify their terms of services.
- Supporting the development of tools to reduce information asymmetries and allow for comparability of services (e.g. labels, certifications…).
- Facilitating interoperability and data portability to enable users to switch from one service to another.
- Fostering end-users’ awareness, training and education.

4.4. Takeaways from the case studies

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

Over the years, many voluntary "security-by-design" standards and guidelines have been developed, such as 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, whether by industry-led bodies and standardisation organisations (ETSI, 2020[52]), governmental agencies (DCMS, 2018[13]; NIST, 2020[28]) or civil society (e.g. Internet Society, Mozilla).[24]

However, while these tools are widely available, they are not widely used (DHS and DoC, 2018[42]). The adherence to security-by-design guidelines varies greatly 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.

Some experts consider that while it often takes time for stakeholders to adhere to standards, there is also 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. In addition, there is often a need to develop specific guidance for each vertical sector (e.g. IoT products for health, smart meters, industrial control systems…), as the digital security challenges or broader constraints may vary significantly from one sector to another.

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 case studies tends to confirm these views. In fact, significant externalities and information asymmetries, as well as a misalignment of incentives, are likely to prevent the market to "naturally" deliver optimal outcomes. The potential benefits, effectiveness and risks of policy tools to address these challenges are examined in the policy discussion report (OECD, 2021[2]).

4.4.2. 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[6]).

In theory, the ability to dynamically fix newly discovered vulnerabilities should have made smart products much more secure and safer than their analogue counterparts. Fixing defects in analogue products that have already been purchased requires physical appointments with technicians or costly and lengthy product recalls. For smart products, however, only an internet connection is needed. The scale of "repairability" also changed dramatically, as all smart products can be patched at once, while fixing analogue products would require each model to be repaired individually.

However, the reality fell short of this promise. The deployment of security updates is often suboptimal, usually because of complex value chains that require action at various steps (e.g. OEMs, network operators, users). In a recent survey of IT professionals (Tripwire, 2019[53]), 27% of the respondents declared that their organisations had been breached because of an unpatched vulnerability. While the designers of operating systems for smartphones and computers usually provide security updates in a timely manner, those are often not deployed swiftly by OEMs and end-users. Many IoT products lack an update mechanism, and for those that have one, producers often do not have teams and policies in place to manage newly discovered vulnerabilities: a 2018 study (IoT Security Foundation, 2018[54]) of 331 consumer IoT products in the UK showed that 90% of the manufacturers lack a vulnerability disclosure policy. 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[29]).

In addition, in certain cases where security updates are combined with product upgrades, the hardware components of the device may not support the update, or may lead to a degraded user experience. As a result, some users may decide to not implement the update, even though it would entail significant digital security risk. This issue can be associated with the EOL gap (see section 4.4.3).

Furthermore, patching includes inherent risks, as any update amounts to modifying the code of a product and could unintentionally or intentionally (e.g. if abused by a malicious actor) insert new vulnerabilities (ETSI, 2019[55]).

The Heartbleed vulnerability discovered in Open SSL[25] in 2014 was introduced unintentionally, through an update (IETF, 2012[56]) proposed in 2011 by a volunteer developer. While another developer reviewed the proposed update, he/she failed to notice the newly introduced vulnerability, which made around 17% of the SSL-enabled web servers in the world vulnerable to attacks upon implementation of the new version in 2012. In 2017, malicious actors used the update mechanism of the accounting software MeDoc (used by the majority of Ukrainian companies) as a threat vector (Greenberg, 2017[34]). The update spread the virus NotPetya, which exploited other vulnerabilities present in unpatched Microsoft products.

From a consumer safety perspective, this issue is often referred to as "hazardisation", which occurs when a product becomes unsafe after purchase because it has been changed. For the United States Consumer Product Safety Commission (CPSC, 2019[57]), a product "could become "hazardised" if unauthorised, or anomalous data transfer, interference or manipulation of operational code or consumer-originated data create a safety hazard where one did not exist before (e.g., a connected gas range pushes a software update that disables temperature-limiting capability)". Products that are less secure by design (e.g. weak authentication mechanisms and weak encryption for data at rest or in transit) are more prone to fall victim to such attacks.

The risks associated with implementing updates often lead end-users, in particular organisations, to not implement updates fully or in a timely manner, as they might entail unexpected bugs or crashes, which may result in financial losses if the organisation's information systems reboot randomly or cease to function for a period. These challenges are particularly significant in complex industrial systems, e.g. in aeronautics (OECD, 2019[1]).

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

Framing the issue

Products that continue to be used after their EOL tend to become less secure. In fact, security updates are no longer provided by the producer and/or other code owners. However, 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 (StatCounter Global Stats, 2020[58]), 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.

The EOL gap illustrates the misalignment of market incentives: producers' prefer to reduce their costs and incentivise end-users to buy new products, while customers prefer to continue to use a product as long as it fulfills their needs.

The EOL gap is usually wider for mainstream users, i.e. less digitally mature stakeholders such as consumers and SMEs. Importantly, mainstream users also include large corporations that may not yet address digital security through a risk-based approach, or may not invest enough resources in digital security risk management. In fact, the WannaCry digital security attack in 2017 hit many large and global corporations, which were often leaders in their market.

There is a lack of standards and clear rules across the industry regarding EOL. The EOL is sometimes specified in contracts or terms of service clauses. Some vendors such as Microsoft clearly state their products' EOL on the product's package or on their website, and the length of support typically lasts from one to five years (sometimes up to ten years with extended support, available for a fee) after the release of the product on the market. Providers of open source operating systems such as Ubuntu or Debian follow similar practices. However, in many cases, vendors do not clearly specify the length of the support period (FTC, 2018[12]), and the decision to terminate a product seems ad-hoc and arbitrary rather than based on formal and transparent policies.

From a lifecycle perspective, the digital transformation means that a community used to short lifecycles (code developers, software companies…) is colliding with a community used to long lifecycles (home appliances, industry…). The effect of that collision is that business models that worked in one community may not be adapted to the other. The resulting gaps are particularly visible in the IoT market, where many products are sold with no clear length of support or with a short period of support (1-2 years) that is not aligned with their expected length of use (Schneier, 2018[6]).

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[6]). This will result in what some have called "the Internet of forgotten things". As the number of IoT products is expected to reach 20 billion worldwide in 2020, and as their expected length of use will likely exceed the length of support, the EOL gap for IoT products is likely to become a key policy issue in the coming years.

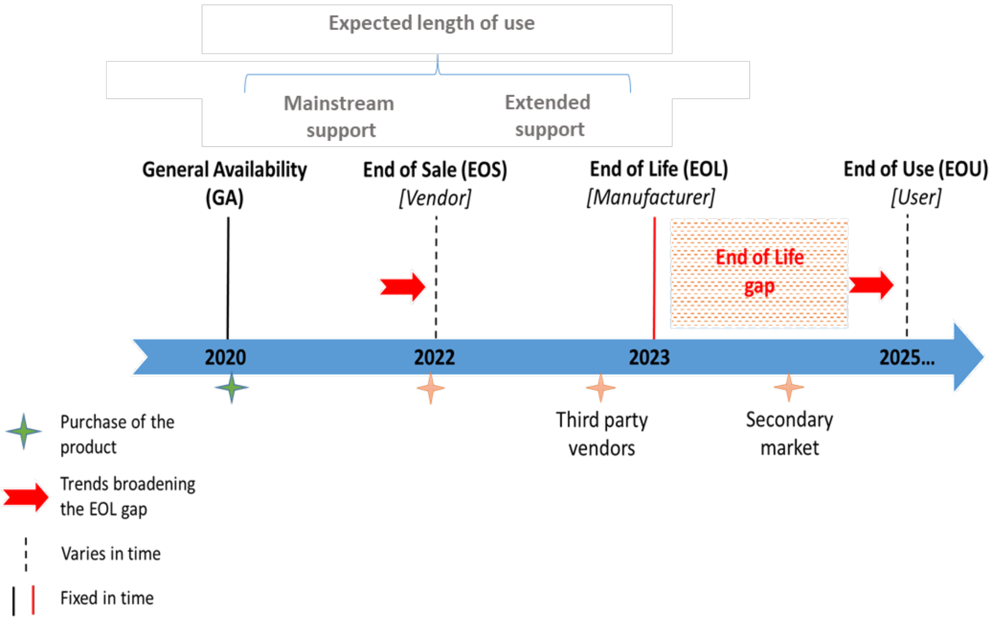
To tackle the EOL issue, the following concepts are important:

- The market release, or general availability (GA), is the date when products are made available for purchase (or use, for free products) by customers.
- The End-of-Sale (EOS) is determined by vendors when they consider that the product should no longer be available for purchase (or use, for free products). The EOS may vary according to each vendor. While there is usually a period between the EOS and the EOL, there is often no industry standards or legal requirements regarding the length of this period.
- The purchase through official vendors could happen anytime between GA and EOS. It could also happen after EOS, and even after EOL, through third-party vendors and on the secondary market.
- The EOL is determined by the manufacturer when it considers that the product has reached the end of its "useful lifespan". The main assumption of manufacturers is that their products will be used for a limited period (the length of use), the length of which differs for each product (e.g. 2 years for a smartphone, 5 years for a fridge, 10 years for a car…). The EOL of older products often matches the release of new products by the manufacturer. In fact, there is a clear economic interest for manufacturers to stop supporting older products, in order to incentivise customers to buy newly released ones. The EOL may also be triggered if the manufacturer goes bankrupt and is forced to close its business.

- The EOL is sometimes broken down into the end of mainstream support and the end of extended support. A manufacturer may decide to continue to provide support for a fee (extended support), at the request of the customer, even though mainstream support has already ended.
- The End-of-Use (EOU) is determined by users when they stop using the product.

These concepts are represented in Figure 4.4.

Figure 4.4. The EOL gap



Note: Variables will depend on each product. The green star represents an optimal date of purchase while the orange stars represent dates of purchase that could lead to a gap between the EOL and the EOU.
Source: OECD.

Two key trends (the red arrows in Figure 4.4) are likely to broaden the EOL gap:

- The closer the EOS and the purchase are to the EOL, the more likely the product will continue to be used after the EOL. In fact, the effective length of use depends on the date of purchase, not on the date of GA. It is common that intermediate vendors (see section 3.2) sell products until the EOL, or even continue to sell products that have reached their EOL (in particular on secondary markets).
- The EOL gap is the gap between the EOL and the EOU. The further away the EOU is from the EOL, the more likely latent vulnerabilities may be discovered and exploited, as security updates are no longer provided. For end-users, there are obvious incentives to continue using a product for as long as possible, as their economic rationality consists in enjoying the benefits provided by the product for as long as possible, until the product ceases to function or new products are available and could better fulfil their needs.

Policy discussion

There are mainly two ways to address the EOL gap:

- Accelerate the EOU, by:
  - Increasing users' awareness about the risks associated with the EOL gap.

  - Incentivising supply-side actors to shift from selling goods to providing services. For instance, Microsoft's modern lifecycle policy (Microsoft, 2016[59]) provides software as a service, with continuous support attached to the license agreement. However, this solution could lead to significant costs for users with little negotiating powers (e.g. consumers or SMEs), compared to the costs associated with products previously sold as goods.
  - Incentivising end-users to stop using the product. For instance, producers could provide free or discounted upgrades, or disconnect / make their products unusable after the EOL.
  - Encouraging the use of ex post mechanisms such as insurance and guarantees, which could in turn incentivise users to not use EOL products.
- Postpone the EOL, by:
  - Increasing supply-side actors' responsibility, for instance through legal requirements imposing minimum support periods after the purchase of the product (as opposed to after General Availability or GA).
  - Increasing the product's "reparability", for instance through incentivising the manufacturer to enable third-parties (e.g. the open-source / user community) to maintain the product after EOL through source code escrow.

To address the EOL gap, policy makers should also take the following aspects into account:

- *Balancing the interests of various stakeholders.* While it may be rational for end-users to continue using their products, it is also rational for producers to limit their support to the expected length of use of a product. Consumer associations and the technical community usually consider that producers should be required to support – or enable others to support – their products for a longer period. In particular, mainstream users (e.g. SMEs or organisations in the healthcare sector) are often resources-constraint, and cannot afford to buy new products or change their entire information systems every two or three years. For other experts, there is a clear security argument in favour of upgrading to more recent products, which often benefit from newer and stronger security features and architectures. For those experts, end-users should be made more aware of the risks of using unsupported products, and incentivised to upgrade.
- *There is no one-size-fits all approach.* The lifecycle and its associated EOL vary with each product category: it can be relatively short (e.g. software) or relatively long (e.g. car). Therefore, any general regulation on EOL needs to focus on the concept of reasonableness: producers should adapt their EOL policies to what is reasonable for each product. For instance, the reasonable length of use will be different for a smartphone, a home appliance or a connected car.
- *The length of support should be determined by the date of purchase of the product, or the date of end-of-sale (EOS)*. Currently, the EOL date is determined by the date of general availability of the product, which means that products that are purchased near the EOS and EOL dates will not benefit from a length of support corresponding to the expected length of use of the product. For instance, some cases of smartphones being sold a few months prior to their EOL date have been reported in the United States (FTC, 2018[12]). In such cases, smart products are often discounted and enable customers to purchase a good or service they would not be able to afford otherwise. However, it seems that customers are often unaware of the digital security impact of purchasing EOL products, and that there is a lack of transparency from supply-side actors regarding the length of security support.

Intellectual property protection often plays a key role in the EOL gap. In many cases, technical measures to protect intellectual property for proprietary software (closed source) prevent other stakeholders from taking responsibility after the EOL and provide security updates. This situation could be considered as a "tragedy of the anticommons", where an extensive application of property rights allows certain owners to prevent others from using a resource, or in this case, maintaining it (Heller, 1998[60]). For producers, such protection is justified because the source code of the EOL product is often very similar to the source code of the newer products. In this case, however, the costs of maintaining the EOL product should be acceptable for producers, as their source code is similar to the newer products that benefit from security support. For some experts, intellectual property protection measures should not be used after a product's EOL, and producers should enable third-parties (e.g. advanced users and the open-source community) to maintain the product. This can be done through transferring proprietary design information and rights to an escrow, or directly to other stakeholders so that they can maintain the product (Zittrain, 2018[50]; NIST, 2016[61]). In addition, the lack of interoperability and competition may generate lock-in effects, which may further limit the ability of stakeholders to manage digital security risk optimally.

If manufacturers go bankrupt, intellectual property rights could be transferred to third-parties (e.g. potential buyers, users or the open-source community) in order to enable them to maintain the products. There may be a need for legal requirements to guarantee that in case of bankruptcy, the responsibility and ability to maintain smart products through security updates is transferred to the actor that is best placed to do so. Mandatory source-code escrow to trusted partners (e.g. private organisations or government agencies) could be a valuable tool to facilitate continuous digital security support in case of bankruptcy.

However, the transfer of responsibility is not a panacea to resolve the EOL gap. First, it should not diminish the duty of care of producers, who have a responsibility to maintain the products they put on the market for a reasonable period. Secondly, transferring the responsibility of maintenance to a community may dilute the "responsibility" principle, as there may be no clear allocation of responsibility in case new vulnerabilities are discovered.[26] To address the issue of maintaining support for open-source products (which is an area for future research, see Annexes), some important multi-stakeholder initiatives are underway and described in the policy discussion report (OECD, 2021[2]).

The EOL gap is wider for sectors and actors with constrained resources (e.g. health, education, SMEs) as well as for low income countries.

Finally, the EOL gap also raises environmental challenges, as it contributes to significantly increase e-waste. Each year, approximately 50 million tons of electronic and electrical waste (e-waste) are produced (WEF, 2019[62]), and the amount is growing along with the digital transformation. Sustainable Development Goal (SDG) 12 on Responsible Production and Consumption intends to reduce the impact of e-waste. In particular, target 12.5 aims to substantially reduce waste generation through repair, recycling, and reuse.

4.4.4. Conclusion

The analysis of the three case studies shows that digital security gaps may vary significantly across product categories:

- IoT products have the most significant digital security gaps, at each stage of the product lifecycle.
- The gaps that emerge during the product's commercial life (misconfiguration or limited deployment of security updates) are the most significant across all case studies.
- The EOL gap is very significant for goods such as IoT products and smartphones, and less so for services such as cloud offers.
- Gaps during design and development are particularly significant in emerging and fragmented markets such as the IoT, and less so for more mature and more concentrated markets such as smartphones and desktop computers.

For policy makers, the following takeaways are important:

- To address the gaps that emerge during design and development, supply-side actors need to be better incentivised to implement standards and guidelines, e.g. through regulatory requirements, certification, conformity assessments and labels.
- All stakeholders need to be better incentivised to manage the product's digital security risks throughout their commercial life, e.g. to timely deploy security updates and avoid misconfigurations

of products. A priority could be to promote “security-by-default”, and in particular automatic updates.

- The EOL gap needs to be addressed through effective policy tools.
- The IoT market should be addressed in priority, keeping in mind that all stages of the product’s lifecycle need to be taken into account: enhancing “security-by-design” is a good first step but will not be enough.

High-level principles to address these challenges are further discussed in the policy discussion report (OECD, 2021[2]), as well as the effectiveness of various policy tools.

References

(n.a.) (2017), *Why everything is hackable - Computer security is broken from top to bottom*, The Economist, https://www.economist.com/science-and-technology/2017/04/08/computer-security-is-broken-from-top-to-bottom (accessed on 1 February 2021). [130]

Akerlof (1970), *The Market for “Lemons”: Quality Uncertainty and the Market Mechanism*, The Quarterly Journal of Economics, http://www.jstor.org/stable/1879431. [45]

Anderson (2001), *Why Information Security is Hard - An Economic Perspective*, https://www.acsac.org/2001/papers/110.pdf. [46]

Anderson and Moore (2006), “Information Security Economics – and Beyond”, https://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf. [40]

Andreessen (2011), *Why software is eating the world*, https://a16z.com/2011/08/20/why-software-is-eating-the-world/. [9]

Anise, O. (2016), *Thirty Percent of Android Devices Susceptible to 24 Critical Vulnerabilities*, Decipher, https://duo.com/decipher/thirty-percent-of-android-devices-susceptible-to-24-critical-vulnerabilities (accessed on 1 February 2021). [71]

Antonakakis et al. (2017), *Understanding the Mirai Botnet*, Usenix, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. [51]

BBC (2018), *Samsung won’t be forced to update old phones*, BBC News, https://www.bbc.com/news/technology-44316364 (accessed on 1 February 2021). [76]

BBC (2017), *German parents told to destroy Cayla dolls over hacking fears*, BBC News, https://www.bbc.com/news/world-europe-39002142 (accessed on 1 February 2021). [77]

Berr, J. (2017), *“WannaCry” ransomware attack losses could reach $4 billion*, CBS News, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ (accessed on 1 February 2021). [49]

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. [121]

Brown, W., V. Anderson and Q. Tan (2012), *Multitenancy - Security risks and countermeasures*, http://dx.doi.org/10.1109/NBiS.2012.142. [87]

Cable, P. (2018), *Access Management Lessons From Timehop’s Cloud Security Breach*, Threat Stack, https://www.threatstack.com/blog/access-management-lessons-from-timehops-cloud- [89]

security-breach (accessed on 1 February 2021).

Church, P. and C. Potratz Metcalf (2019), *U.S. CLOUD Act and GDPR – Is the cloud still safe?*, Linklaters, https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe (accessed on 1 February 2021). [88]

Cimpanu, C. (2020), *Ripple20 vulnerabilities will haunt the IoT landscape for years to come*, ZDNet, https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come/ (accessed on 1 February 2021). [25]

Cloud security alliance (2017), *Security Guidance*, https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf. [92]

Coase (1972), *Durability and Monopoly*, Journal of Law and Economics, http://www.econ.boun.edu.tr/yilmaz/EC301%20-%20Reading1%20-%20Coase%20-%20Durability%20Monopoly.pdf. [43]

Consumers International (2019), *Consumers and the Internet of Things*, https://www.consumersinternational.org/media/261950/thetrustopportunity-jointresearch.pdf. [41]

Counterpoint (2019), *Software and Security Updates- The Missing Link for Smartphones*, https://www.counterpointresearch.com/nokia-leads-global-rankings-updating-smartphone-software-security/. [73]

CPSC (2019), *Report on IoT and consumer safety*, https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf?6sv9HwTXKHrkdmAyAkQ0_TsKCkpl1lR2. [57]

CWE (2019), *CWE-352: Cross-Site Request Forgery (CSRF) (4.3)*, CWE, https://cwe.mitre.org/data/definitions/352.html (accessed on 2 February 2021). [81]

Cyberspace Solarium Commission (2020), *Cyberspace Solarium Commission Report*, https://www.solarium.gov/. [29]

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. [13]

DCMS (2018), *Mapping of IoT Security Recommendations*, https://aioti.eu/wp-content/uploads/2019/06/DCMS_Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf. [102]

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. [47]

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. [115]

Deahl, D. (2018), *Apple and Samsung fined in Italy for slowing down their phones*, The Verge, https://www.theverge.com/2018/10/24/18018322/apple-samsung-italy-phone-slowdown-fine-antitrust (accessed on 1 February 2021). [74]

Dean, B. (2018), *Strict Products Liability and the Internet of Things*, Center for Democracy and [1

Technology. [14]

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. [42]

Drahos, P. (2017), *Regulatory Theory: Foundations and applications*, http://dx.doi.org/10.22459/RT.02.2017. [113]

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. [8]

ENISA (2019), *IoT Security Standards Gap Analysis*, https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis. [117]

ENISA (2018), *Threat landscape*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018. [86]

ENISA (2017), *Baseline Security Recommendations for IoT*, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. [101]

ENISA (2015), *Cloud Security Guide for SMEs*, https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes. [85]

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. [52]

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. [55]

EU (2019), *The EU Cybersecurity Act*, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act. [114]

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. [36]

FIRST (2020), *Common Vulnerability Scoring System*, https://www.first.org/cvss/v3.0/specification-document. [22]

Forrest, C. (2017), *98% of WannaCry victims were running Windows 7, not XP*, TechRepublic, https://www.techrepublic.com/article/98-of-wannacry-victims-were-running-windows-7-not-xp/ (accessed on 1 February 2021). [68]

Frei, S. (2020), *ETH Zurich / ICT Swirzerland*, https://techzoom.net/. [120]

Frison-Roche (2019), *Rapport sur "l'apport du droit de la compliance à la gouvernance d'internet"*, https://www.economie.gouv.fr/files/files/2019/Rapport_MAFR_Compliance_et_Gouvernance_du_numerique_juin_2019.pdf. [66]

FTC (2018), *Mobile Security Updates: Understanding the Issues*, https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf. [12]

Furman (2019), *Report "unlocking digital competition"*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf. [65]

Gartner (2019), *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020*, Gartner, https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020 (accessed on 1 February 2021). [84]

Gartner (2019), *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018*, Gartner, https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018 (accessed on 1 February 2021). [83]

GCSC (2018), *Norms package*, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf. [97]

GDPR (2018), *GDPR*. [116]

Goodin, D. (2017), *Failure to patch two-month-old bug led to massive Equifax breach*, Ars Technica. [32]

Google (2020), *Google Terms of Service – Privacy & Terms*, Google, https://policies.google.com/terms?hl=en-US (accessed on 2 February 2021). [23]

Google (2019), *Android Security and Privacy year in review 2018*, https://www.blog.google/products/android-enterprise/look-back-2018-android-security-privacy-year-review/. [75]

Google (2017), *ANDROID SECURITY 2016 YEAR IN REVIEW*, https://source.android.com/security/reports/Google_Android_Security_2016_Report_Final.pdf. [72]

Greenberg, A. (2017), *The Petya Plague Exposes the Threat of Evil Software Updates*, WIRED, https://www.wired.com/story/petya-plague-automatic-software-updates/ (accessed on 1 February 2021). [34]

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). [48]

Heller (1998), *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, Harvard Law Review, https://ssrn.com/abstract=57627. [60]

IEEE (2017), *Internet of Things (IoT) Security Best Practices*, https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf. [104]

IETF (2012), *RFC 6520 - Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension*, https://tools.ietf.org/html/rfc6520 (accessed on 1 February 2021). [56]

IoT Security Foundation (2018), *Crazy! Less than 10% of consumer IoT companies follow Vulnerability Disclosure guidelines*, IoT Security Foundation, [54] https://www.iotsecurityfoundation.org/less-than-10-of-consumer-iot-companies-follow-vulnerability-disclosure-guidelines/ (accessed on 1 February 2021).

ISO (2018), , https://www.iso.org/fr/standard/44651.html. [39]

ISO (2018), *27000*, https://www.iso.org/fr/standard/73906.html. [100]

ISO (2018), *31000*, https://www.iso.org/iso-31000-risk-management.html. [18]

ISO (2014), *ISO/IEC 29147*. [15]

ISO (2014), *ISO/IEC 29147*, https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip. [26]

Kaspersky (2020), *What is a Data Breach & How to Prevent One*, Kaspersky, https://www.kaspersky.com/resource-center/definitions/data-breach (accessed on 1 February 2021). [90]

Kopp, Kaffenberger and Wilson (2017), *Cyber Risk, Market Failures, and Financial Stability*, IMF Working Paper, https://www.cybersecitalia.it/wp-content/uploads/2017/10/wp17185.pdf. [20]

Krugman (2008), *The Return of Depression Economics and the Crisis of 2008*. [37]

Levite and Hoffman (2017), *Private sector cyber defense : can active measures help stabilize cyberspace?*, Carnergie Endowement for International Peace, https://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236. [127]

Levite, A. (2019), *ICT Supply Chain Integrity*, Carnegie Endowment for International Peace. [128]

Leyden, J. (2017), *Half-baked security: Hackers can hijack your smart Aga oven 'with a text message'*, The Register, https://www.theregister.com/2017/04/13/aga_oven_iot_insecurity/ (accessed on 1 February 2021). [78]

Luettmann, B. and A. Bender (2007), “Man-in-the-middle attacks on auto-updating software”, *Bell Labs Technical Journal*, Vol. 12/3, pp. 131-138, http://dx.doi.org/10.1002/bltj.20255. [33]

Maynard (2017), *Counting the cost of cyber exposure*, https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost. [98]

McAfee (2017), *Mobile threat report*, https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2017.pdf. [7]

McLean, R. (2019), *A hacker gained access to 100 million credit card applications and accounts*, CNN, https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html (accessed on 1 February 2021). [94]

Mell, P. and T. Grance (2011), *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*, http://dx.doi.org/10.6028/NIST.SP.800-145. [82]

Microsoft (2016), *Modern Lifecycle Policy*, https://docs.microsoft.com/en-us/lifecycle/policies/modern (accessed on 1 February 2021). [59]

MITRE (2017), *Terminology*, https://cve.mitre.org/about/terminology.html. [126]

Munro, K. (2018), *What will happen when the IoT reaches its end of life?*, Electronic Specifier, https://www.electronicspecifier.com/products/iot/what-will-happen-when-the-iot-reaches-its-end-of-life (accessed on 1 February 2021). [80]

NCSC (2020), *Glossary*, https://www.ncsc.gov.uk/information/ncsc-glossary. [11]

Netcraft News (2014), *Half a million widely trusted websites vulnerable to Heartbleed bug*, Netcraft News, https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html (accessed on 1 February 2021). [24]

NIST (2020), *Glossary*, https://csrc.nist.gov/glossary/. [21]

NIST (2020), *NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers*, https://doi.org/10.6028/NIST.IR.8259. [28]

NIST (2020), *NISTIR 8272 - Impact Analysis Tool for Interdependent Cyber Supply Chain Risks*, https://doi.org/10.6028/NIST.IR.8272. [38]

NIST (2018), *Cybersecurity Framework*, https://www.nist.gov/cyberframework. [111]

NIST (2016), *Intel Corporation Supply Chain Risk Management*, https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Intel-Case-Study.pdf. [61]

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. [4]

OECD (2021), "Encouraging vulnerability treatment: overview for policy makers", *OECD Digital Economy Papers*, OECD Publishing, Paris, https://doi.org/10.1787/20716826. [3]

OECD (2021), "Enhancing the digital security of products: a policy discussion", *OECD Digital Economy Papers*, OECD Publishing, Paris, https://doi.org/10.1787/20716826. [2]

OECD (2021), "Understanding the digital security of products: an in-depth analysis", *OECD Digital Economy Papers*, OECD Publishing, Paris, https://doi.org/10.1787/20716826. [129]

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. [124]

OECD (2020), *Encouraging Digital Security Innovation*. [109]

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. [123]

OECD (2020), *Recommendation on Consumer Product Safety*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0459. [107]

OECD (2020), *The role of sandboxes in promoting flexibility and innovation*, [110 https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf.]

OECD (2019), *Principles on artificial intelligence*, https://www.oecd.org/going-digital/ai/principles/. [106]

OECD (2019), *Recommendation on the Digital Security of Critical Activities*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. [95]

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

OECD (2019), “Vectors of digital transformation”*, OECD Digital Economy Papers*, No. 273, OECD Publishing, Paris, https://dx.doi.org/10.1787/5ade2bba-en. [10]

OECD (2018), *Guidance for responsible business conduct*, http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf. [105]

OECD (2018), *IoT measurement and applications*, https://doi.org/10.1787/20716826. [16]

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. [5]

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. [19]

OECD (2015), *Recommendation on Digital Security Risk Management*, https://oe.cd/dsrm. [17]

OECD-APEC (2005), *Integrated checklist on regulatory reform*, https://www.oecd.org/regreform/34989455.pdf. [112]

Open source initiative (2020), *Open source initiative*, https://opensource.org/. [99]

Panetta, K. (2017), *7 Top Security Predictions for 2017*, Gartner, https://www.gartner.com/smarterwithgartner/7-top-security-predictions-for-2017/ (accessed on 1 February 2021). [31]

Paris call (2018), *Paris call for trust and security in cyberspace*, https://pariscall.international/en/call. [96]

Pen Test Partners (2017), *IoT Aga. Cast iron Security Flaw*, Pen Test Partners, https://www.pentestpartners.com/security-blog/iot-Aga-cast-iron-security-flaw/ (accessed on 1 February 2021). [79]

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. [103]

PI4.0 & RRI (2020), *IIoT Value Chain Security – The Role of Trustworthiness*, https://www.plattform- [35]

i40.de/PI40/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.html.

Protalkinski, E. (2017), *Google finally updates Android distribution dashboard, Pie passes 10%*, VentureBeat, https://venturebeat.com/2019/05/07/google-finally-updates-android-distribution-dashboard-pie-passes-10/ (accessed on 1 February 2021). [69]

Ralph Nader (1965), *Unsafe at any speed*. [125]

Rundle, J. (2019), *Human Error Often the Culprit in Cloud Data Breaches*, WSJ, https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203 (accessed on 1 February 2021). [93]

Rushe, D. (2014), *Apple blames 'very targeted attack' for hack of nude celebrity photos*, The Guardian, https://www.theguardian.com/technology/2014/sep/02/apple-denies-hacker-celebrities-naked-photos-icloud (accessed on 1 February 2021). [91]

Schneier, B. (2018), *Click here to kill everybody*, Norton. [6]

Schneier, B. (2018), *Patching Is Failing as a Security Strategy*, VICE, https://www.vice.com/en_us/article/439wbw/patching-is-failing-as-a-security-paradigm (accessed on 31 March 2020). [30]

StatCounter Global Stats (2021), *Desktop Operating System Market Share Worldwide Dec 2019 - Jan 2021*, StatCounter Global Stats, https://gs.statcounter.com/os-market-share/desktop/worldwide (accessed on 2 February 2021). [64]

StatCounter Global Stats (2021), *Mobile Operating System Market Share Worldwide Dec 2019 - Jan 2021*, StatCounter Global Stats, https://gs.statcounter.com/os-market-share/mobile/worldwide (accessed on 2 February 2021). [63]

StatCounter Global Stats (2020), *Desktop Windows Version Market Share Worldwide Jan 2019 - Jan 2020*, StatCounter Global Stats, https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/#monthly-201901-202001 (accessed on 2 February 2021). [58]

Symantec (2018), *Internet Security Threat Report 2017*. [67]

The Internet Society (2017), *The Internet Ecosystem*, The Internet Society, https://www.internetsociety.org/wp-content/uploads/2017/09/factsheet_ecosystem.pdf (accessed on 1 February 2021). [27]

Thomas, Beresford and Rice (2015), *Security Metrics for the Android Ecosystem*, https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf. [70]

Traficom (2019), *IoT Information Security Label Concept introduction*. [122]

Tripwire (2019), *Tripwire 2019 Vulnerability Management Survey*, https://www.tripwire.com/state-of-security/wp-content/uploads/sites/3/Tripwire-Dimensional-Research-VM-Survey.pdf (accessed on 1 February 2021). [53]

UN (2016), *United Nations Guidelines for Consumer Protection*, https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf. [118]

Varian and Shapiro (1999), *Information rules*. [44]

Verizon (2019), *Data breach investigation report*, https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/. [108]

WEF (2020), *Global Risk Report*, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. [119]

WEF (2019), *A New Circular Vision for Electronics*, http://www3.weforum.org/docs/WEF_A_New_Circular_Vision_for_Electronics.pdf. [62]

Zittrain (2018), *From West World to Best World*, https://www.nytimes.com/2018/06/03/opinion/westworld-internet-of-things.html. [50]

Annex A. Detailed case studies

Case study 1: desktop computers and smartphones.

Introduction

Desktop computers and smartphones are widely used products part of the “traditional Internet” (OECD, 2018[16]). This case study focuses in particular on the operating systems of desktop computers and smartphones, i.e. the core software that manages a product’s hardware and software resources and provides common services for computer programs. The market for desktop and mobile operating systems (OS) is concentrated. According to estimates (StatCounter Global Stats, 2021[63]) (StatCounter Global Stats, 2021[64]), desktop computers primarily run Microsoft Windows (78%) and Apple OS X (17%) while smartphones primarily run Google Android (75%) and Apple iOS (25%). For both desktop and mobile operating systems, the market structure is largely a global duopoly (Furman, 2019[65]). However, this case study does not take into account other types of devices (e.g. servers or industrial computers), which may run on other operating systems (in particular, Linux).

From a digital security perspective, the operating systems of smartphones and desktop computers are important because of their central role in the product’s architecture. A breach of their integrity or availability would likely seriously impair the ability of their users[27] to use their smartphones or desktop computers, on which their economic and social activities are increasingly dependent. Box 4.1 provides insights from such a security incident, which affected desktop computers’ operating systems.

Key actors

From a digital security perspective, the relevant actors in the ecosystems of smartphones and desktop computers are the following:

- Suppliers of hardware and software components (e.g. chips, module libraries…);
- Operating systems (OS) designers;
- Original Equipment Manufacturers (OEMs);
- Network operators;
- Third-party applications developers;
- End-users.

Design & development

Are there any gaps during the design and development of the product?

It seems that the design and development of operating systems generally follow industry standards and best practices. This does not mean that no gaps exist at this stage of the lifecycle, but rather that the existing gaps are less pressing and severe compared to gaps identified at other stages of the lifecycle.

Key factors

From an economic theory perspective, this situation can be explained, inter alia, by aligned incentives and a strong influence of brand reputation on those concentrated markets. As noted above, brand reputation was identified by Akerlof (1970[45]) as a significant remedy to information asymmetries, as established brands rely on a guarantee of quality to retain consumers. Established operating systems designers are digitally mature companies, leading innovators, and invest significant resources in digital security. Because of their central (or "bottleneck") position on the value chain, they also tend to mainstream security requirements (e.g. through licensing agreements and certifications for Android). This led some to consider those platforms as "second level regulators" (Frison-Roche, 2019[66]).

In fact, Google, Apple and Microsoft have shown strong adherence to industry best practices and standards, e.g. through Microsoft's SDL (Security Development Lifecycle). For desktop computers, corporate clients' demand for security has driven OS designers to review the architecture of their products and develop security-by-design approaches (OECD, 2019[1]). However, this is a relatively new phenomenon, and such adherence was not widespread some decades ago in the desktop market (OECD, 2019[1]). In the mobile market, application stores are tightly linked to their respective operating systems, and impose certain security requirements on application developers. Sandboxing also enables limited access for new applications. According to Symantec (2018[67]), the majority of detected harmful applications result from so-called third-party application stores, i.e. unofficial application stores not supervised by the operating system's designer that usually require less security checks. However, more data are needed to evaluate the efficiency of application stores in increasing the level of digital security of smartphones. Mobile security is a relatively new topic for researchers, and recent data show that the number of attacks targeting mobile devices has increased sharply in the past few years (FTC, 2018[12]).

Key actors

OS designers are the most responsible for this situation, as well as end-users' demand for security.

Commercial life

Are there any gaps during the product's commercial life?

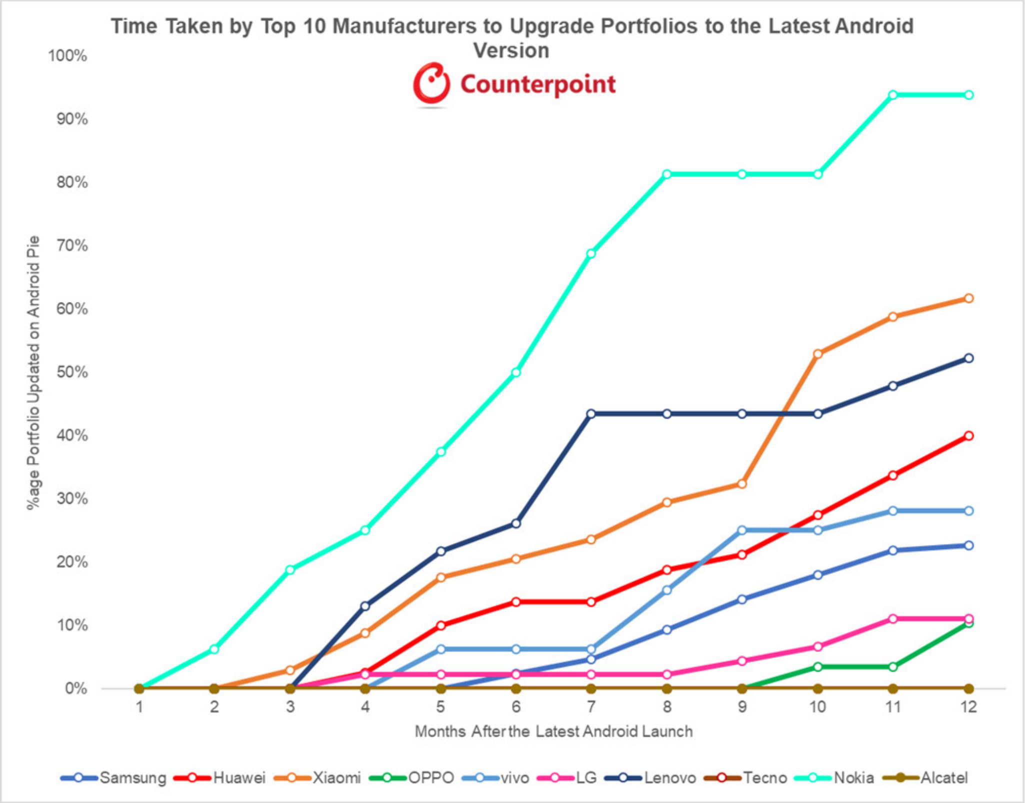
There are significant gaps in the maintenance of operating systems during the commercial life of desktop computers and smartphones. Even though significant resources are often deployed by operating systems' vendors to maintain security (e.g. through security research, processing vulnerability reports from other organisations, developing and testing patches, providing fixes, etc.), the implementation or deployment of updates by device manufacturers, network operators or users is often insufficient. The WannaCry ransomware showed that despite the availability of security updates, these were not systematically cascaded across the value chain and implemented in a timely manner. Some studies (Forrest, 2017[68]) reported that the majority of the machines infected by WannaCry were running Windows 7, for which a security patch was made available weeks before the attack.

In the mobile ecosystem, the security update deployment process can be complex and time-consuming. Some studies (Protalkinski, 2017[69]) show that it usually takes 8 to 12 months for a new version of Android to reach a 10% adoption rate across Android-based devices globally, and that the majority of Android-based devices run on outdated operating systems. A study from researchers at the University of Cambridge found that nearly 88% of Android devices had at least one of 11 known critical vulnerabilities (Thomas, Beresford and Rice, 2015[70]). In 2016, a security research firm published data analysis indicating that only 17% of Android phones were operating with the latest security patch, and about a third had 24 critical vulnerabilities (Anise, 2016[71]). In its Android Security 2016 Year in Review report, Google reported that by the end of 2016, "over half of the top 50 Android devices worldwide had a recent security patch" (Google, 2017[72]).

These gaps result from the complexity of Android's value chain. An Android operating system may be customised at various levels, including by the OEM and the network operator. As a result, a single operating system update may require dozens or hundreds of customised updates, which may need to be tested at the OEM and carrier levels (FTC, 2018[12]).

According to a recent study (Counterpoint, 2019[73]), the variability of delays for deploying upgrades is high between brands but also within brands, as the upgrades policies vary for each smartphone model in the brand portfolio (Figure A A.1). High-priced and recent devices typically get upgraded first while low-end devices or devices which have been on the market for a long time tend to get upgraded much later. A device may receive security updates every month, a few times a year, once a year, or not at all. Some devices receive regular updates for three years or longer while other devices do not receive any updates after a few months (FTC, 2018[12]).

Figure A A.1. Variability in deploying upgrades across Android-based smartphones



Source: Counterpoint

Key factors

Successful and timely patching can confer reputational benefits by providing evidence to consumers of the OS designers' investment in their product (FTC, 2018[12]). This case of aligned incentives explains why OS designers usually provide security updates in a timely manner.

The identified gaps relative to inefficient deployment and adoption of security updates mostly result from information asymmetries and misaligned incentives. For OEMs, support comes with costs, and security is sometimes not a business priority, compared with developing new products.

While some actors such as Microsoft have put in place formal policies and contributed to increase transparency, there seems to be no clear rules across the industry regarding the frequency and deployment speed of security updates. For smartphones, the decision-making process of OEMs is often ad-hoc and does not follow formal policies. It seems to usually depend on the severity of the vulnerability, the number of parties involved, and their contractual relationships and norms. For instance, for a medium vulnerability, an OEM may decide to cascade the update only to high-end smartphones, while an update for a critical vulnerability may be cascaded faster and more broadly across the portfolio. There is also a lack of transparency regarding the practices of OEMs, which are often not publicly disclosed (FTC, 2018[12]).

End-users may also be reluctant to implement the updates for many reasons. Patching can impose direct time and inconvenience costs on consumers, and some patches may change device functionality (FTC, 2018[12]). Patching includes inherent risks, as it amounts to modifying the code of the operating systems. Updates of operating systems usually require the shutdown of the computers that rely on them, which could disrupt the associated economic and social activities. This disruption can be particularly cumbersome in critical sectors such as energy, health or industry (OECD, 2019[1]). As a result, some organisations prefer to test and deploy patches on specific segments before deploying to the entire organisation in order to better mitigate risks.

End-users might also use legacy equipment, the hardware of which might not fully support a new firmware, and consequently may prefer not to update their operating systems. Some OS designers do not separate security updates from general OS updates, hence imposing full updates to end-users that might prefer to only implement the security parts of the update. For instance, in October 2018, the Italian anti-trust authority (Deahl, 2018[74]) ruled that updates that were forced or “insistently pushed” by manufacturers such as Apple and Samsung, and led to a decrease in performance (e.g. a slower operating system and a lower battery performance), amounted to “forced obsolescence” and revealed a lack of transparency in their business practices. Apple and Samsung were fined respectively EUR 10 and 5 million, the authority considering that their updates “*caused serious dysfunctions and reduced performance significantly, thereby accelerating the process of replacing them*” with newer models.

Key actors

These gaps mostly result from OEMs policies and end-users behaviour.

To address those gaps, some OS designers have developed new strategies. For instance, Google has developed more stringent requirements in their agreements with OEMs, as well as voluntary programmes such as Android Enterprise Recommended, in order to make progress in releasing timely security updates (Google, 2019[75]). With Windows 10, Microsoft offers different servicing channels so that customers can implement security updates but postpone feature changes. This reinforces the hypothesis that OS designers have a positive role in streamlining behaviours and standards across the products’ value chain.

End-of-Life

Is the end of commercial life aligned with the end of use?

The end of commercial life for operating systems does not always match the end of use. The length of commercial life envisioned by the OS designers and OEMs (usually between 2 and 5 years, sometimes up to 10 with extended support) is often shorter than the length of use of the product by the end-users. There are many legacy operating systems (i.e. no longer supported by their designers) still widely in use. For example, Microsoft discontinued support for Windows XP in April 2014, thirteen years after it was first released. In 2017, however, around 10% of all desktops were still running Windows XP, as well as a number of other devices (e.g. ATMs and medical scanners). In January 2020, the following statistics (StatCounter Global Stats, 2020[58]) were available regarding desktop computers and smartphones’ operating systems still used after their EOL, worldwide:

- 30% of desktop computers running Windows used a version that reached EOL (25% on Windows 7 and 5% on Windows 8.1);

- 17% of desktop computers running Mac OS used a version that reached EOL;
- 30 % of iPhones used an iOS version that reached EOL;
- For Android, the analysis is more complex as EOL is often determined by the OEM, rather than by the OS designer. In January 2020, 57% of Android smartphones worldwide were running on an outdated version of Android.

For Windows, the length of the support period is transparent, and EOL dates are officially disclosed on the vendor's website. Often, Microsoft also provides customers with incentives to upgrade to newer products. However, as shown in Table A A.1, it was possible in 2016 to buy from intermediate vendors PCs running on Windows 7, even though the mainstream support for this operating system had already ended (only an extended support was available for a fee). Similarly, a consumer or an SME could buy in October 2016 PCs running on Windows 8.1, even though the mainstream support for this product would end a year later, in January 2018. Too often, the period between the end of sale and the EOL does not correspond to a reasonable period of use from the end-user's perspective, in particular for mainstream users.

Table A A.1. Product lifecycle for selected Windows operating systems

This table is based on Microsoft's Fixed Lifecycle Policy. Other products such as Windows 10 rely on Microsoft's Modern Lifecycle Policy.

	Market release / Date of general availability	Retail software end of sales	End of sales for PCs with Windows preinstalled	End of mainstream support	End of extended support
Windows 7	October 2009	October 2013	October 2016	January 2015	January 2020
Windows 8.1	October 2013	September 2015	October 2016	January 2018	January 2023

Note: when the retail software product reaches its end-of-sales date, it can still be purchased through an OEM until it reaches the end-of-sales date for PCs with Windows preinstalled.
Source: Microsoft.

In the smartphone market, support periods are highly variable and not always transparent. Smartphones manufacturers that develop and control their own operating systems tend to commit in advance to longer support periods (usually for several years) for devices. While the EOL is sometimes specified in contracts or terms of service clauses, in many cases, vendors and other code owners do not clearly specify the length of the support period (FTC, 2018[12]). For Android, the provision of upgrades and security updates vary greatly between OEMs. Low-end smartphones tend to have shorter lifecycle, with some models reaching their EOL a few months after their purchase (FTC, 2018[12]). The decision-making process regarding the EOL varies not only between brands, but also within portfolios. In many cases, this process seems to lack any formal policies as it rather relies on an informal assessment leading to ad-hoc decisions (FTC, 2018[12]). This assessment usually focuses on the device's date of release (which often does not match the date of purchase, as purchases can take place anytime between the date of release and the end of sale), price and popularity, as well as on the cost of support.

Key factors

Misaligned incentives, a lack of awareness and information asymmetries across the value chain may explain this gap. For OS designers and OEMs, maintaining existing software incurs significant costs and may divert resources from the development of valuable new products.

For end-users, there are obvious incentives to continue using an operating system for as long as possible. Their economic rationality consists in enjoying the benefits provided by the product for as long as possible. Consumers do not stop using a washing-machine or a fridge after the guarantee expires: they use the product until it ceases to function, or until their needs are no longer fulfilled (for instance because new products have been released and could provide more satisfaction). Similarly, end-users keep on using their smart products after their EOL. Changing operating systems (through upgrading or acquiring new products) usually incurs direct costs as well as indirect costs. For corporate customers, these indirect costs include interrupting production lines, managing the transition for the whole digital ecosystem relying on the operating system and training employees to use the new operating system. Alternatively, the benefits of upgrading to newer operating systems, such as access to more effective security features, are not always fully perceived by end-users. There is often a gap between the end-users' needs, which are likely to stay the same for years, and the product's lifecycle as determined by the smartphone or computer manufacturer and the operating systems designers. For SMEs using computers for office productivity, for instance, it may be rational to continue using the same product for years or even decades, as there is no need for more functionalities.

Because the market for operating systems is relatively concentrated and mature, there are also strong incentives for OS designers and OEMs to shorten the commercial life of their products, which are often referred to as part of the "durable goods monopoly problem" (see section 3.3).

One could also argue that it would be unreasonable to require OS designers to maintain their products indefinitely for free, and that a balance needs to be found between the end-users' willingness to continue to use their products and what would be viable from a supply-side perspective.

For instance, in June 2018, a Dutch court (BBC, 2018[76]) ruled that manufacturer Samsung, which guaranteed two years of security updates for its smartphones, could not be obliged to provide patches for a longer period. The Dutch consumer rights group that sued Samsung, *Consumentenbond*, considered that security updates should be provided for at least 4 years after the smartphone was first released on the market, and that Samsung had an obligation to fully and timely pass on the security updates provided by Android's designer, Google.

In addition, it can be argued that the design and architecture of newer operating systems would include stronger security features, and would be more adapted to the evolving threat landscape. Hardware requirements for operating systems also tend to increase when new versions are released, some of which may not be compatible with older devices whose capabilities do not match minimum requirements.

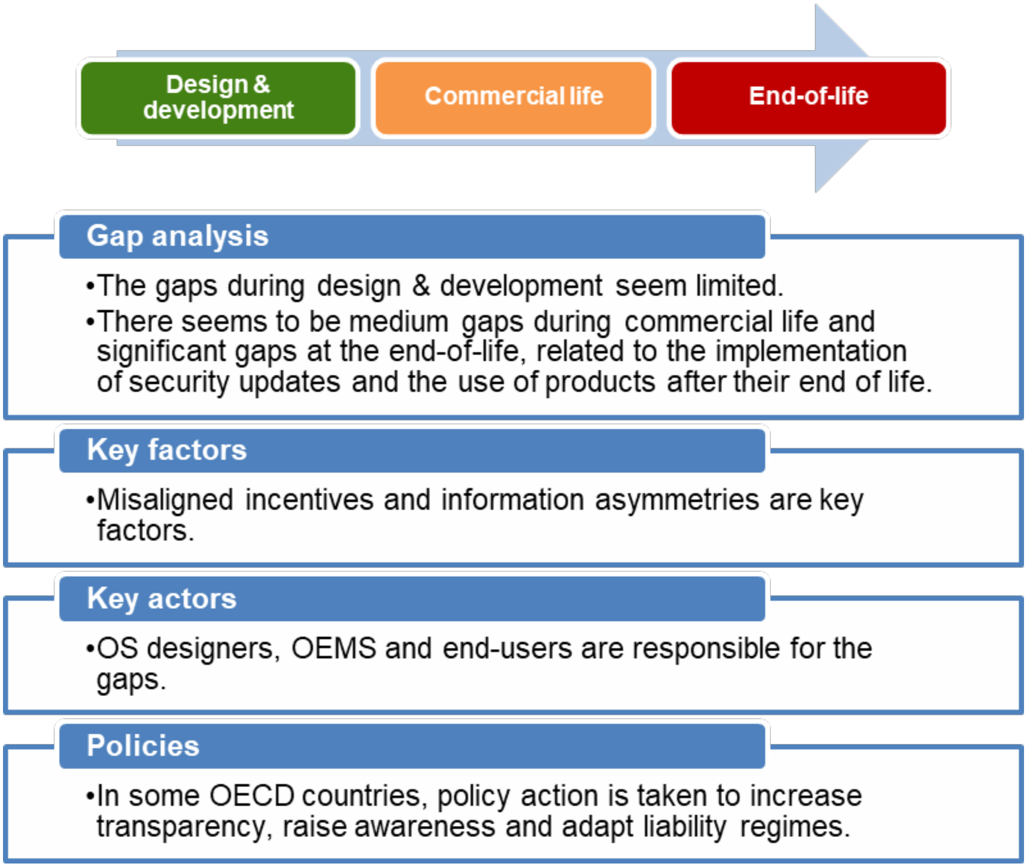
Key actors

These gaps mostly result from the policies of OS designers and OEMs, and from the behaviour of end-users.

Main findings and policy implications

The main findings of this case study are that the designers of major operating systems usually follow best practices and standards during design & development, and provide security updates throughout the commercial life of the product. Windows patches are available directly from Microsoft regardless of the hardware OEM. However, for smartphones, OEMs and end-users[28] tend to not cascade and implement security updates in a timely manner during the commercial life. There is also a significant gap between the EOL as envisioned by the product designer and the effective end of use. These gaps can be explained, *inter alia*, by misaligned incentives, a misperception of risk and information asymmetries. For policy makers, it means that policy action to enhance the security of smartphones and desktop computers could prioritise tools to incentivise stakeholders to deploy security updates in a timely manner, and to use and support products for a reasonable period.

Desktop computers and smartphones



Gap analysis

- The gaps during design & development seem limited.
- There seems to be medium gaps during commercial life and significant gaps at the end-of-life, related to the implementation of security updates and the use of products after their end of life.

Key factors

- Misaligned incentives and information asymmetries are key factors.

Key actors

- OS designers, OEMS and end-users are responsible for the gaps.

Policies

- In some OECD countries, policy action is taken to increase transparency, raise awareness and adapt liability regimes.

Case study 2: consumer IoT products

Introduction

Connected devices, usually referred to as the Internet of Things (IoT), are becoming widespread: their number could reach 20 billion worldwide in 2020 (Schneier, 2018[6]). They include a wide spectrum of products, ranging from smart home appliances (e.g. ovens, thermostats, locks) to toys, security cameras, medical devices (e.g. pacemakers) or connected vehicles. Their common trait is that they challenge the digital / physical dichotomy, as they enable and/or rely on interactions between the physical and digital environment. While there is no internationally agreed definition of the IoT, it can be described as encompassing "all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals" (OECD, 2018[16]). It can also be argued that "while connected objects may require the involvement of devices considered part of the "traditional Internet", this definition excludes laptops, tablets and smartphones already accounted for in current OECD broadband metrics" (OECD, 2018[16]).

From a digital security perspective, IoT devices raise new challenges. First, their sheer number could lead to a new level of risk, e.g. massive-scale DDoS attacks in case even a fraction of IoT devices are enrolled into a botnet. Second, IoT devices enable new physical-digital interactions, which induce a potential impact on consumer safety, i.e. physical damages and possibly life-threatening situations (e.g. connected cars). Third, the market of connected devices is emerging and fragmented, including new actors that may not be digitally mature nor security conscious. As a result, IoT products often lack secure defaults, update mechanisms or vulnerability disclosure policies, enabling the spread of basic vulnerabilities (see Box 4.1). Fourth, connected devices often stand in a grey zone when it comes to applicable regulation. While many connected devices are subject to sectoral regulations (e.g. connected pacemakers or bulbs), these regulations do not necessarily address the challenges of digital security, or are themselves challenged by digital features (e.g. how to certify a product that constantly evolves through updates?).

IoT devices are clearly an area of interest for policy makers, however they do not form a homogenous group. The safety risk they pose may be very different and range from high (e.g. a fault in the automated braking system of an autonomous vehicle) to medium or low. Importantly, the level of risk will depend on the context of use. For instance, IoT products designed for consumers may be used in an industrial context, which would significantly increase the potential impact of a digital security incident.

Box 4.1 provides insights from a recent security incident that affected connected devices.

Key actors

From a digital security perspective, the relevant actors in the ecosystems of connected devices – consumer IoT are the following:

- Suppliers of hardware and software components (e.g. chips, module libraries, operating systems, third-party application developers …);
- Manufacturers / product makers;
- Network operators;
- End-users.

Design & development

Are there any gaps during the design and development of the product?

The Mirai botnet attacks showed that the design & development of many IoT devices is suboptimal. Industry standards and best practices are often not followed (Schneier, 2018[6]) and many connected devices are commercialised even though they lack basic security features such as strong and user-defined passwords. IoT products often lack digital security capabilities that customers would expect their computers and smartphones to have. Consequently, many IoT products are not adequately secured in face of evolving threats (NIST, 2020[28]).

Product safety

In 2017, researchers found a vulnerability in “My friend Cayla”, a connected doll (BBC, 2017[77]) for children. A lack of authentication requirements in the product’s design allowed any Bluetooth-enabled device within range to connect with the doll (send and receive data to / from the product). The industry best practice is usually to require the owner of such a device to activate a “pairing” mechanism to authorise another device to connect through Bluetooth. This vulnerability led consumer associations to file complaints and regulators to start investigations in various OECD countries, including Norway, the United States, the Netherlands and France.

Shortly after the vulnerability became public, the German Federal Network Agency (*Bundesnetzagentur* or BNetzA) decided to ban the product in Germany. However, in the absence of specific regulations that could be relevant for this case, the German regulator had to resort to an older set of laws that prohibited “illegal espionage” through radio-equipment. For some consumer advocates, this case revealed a legal gap, which called for a new set of regulations for smart products, and IoT in particular, in order to put more responsibility on producers and vendors.

If exploited, the vulnerability could lead to indirect but serious consequences for the safety of the children playing with the toy (e.g. a criminal could communicate with the child through the toy and give them instructions).

Key factors

These gaps result from misaligned incentives, a lack of awareness, externalities, a misperception of risks and information asymmetries.

From a supply-side perspective, the IoT market is still emerging and a significant proportion of IoT manufacturers neglect security when designing products (Antonakakis et al., 2017[51]) as they are much more incentivised to value speed (go-to-market strategies), usability or cost-effectiveness (DHS and DoC, 2018[42]). IoT supply-side actors may also lack awareness or resources to provide adequate levels of security for their devices. In many cases, the value chain of IoT products is complex and opaque: as companies from “traditional” sectors (e.g. home appliances) lack the technical skills to develop software, they often rely on third-parties to provide code and integrate it with the product. This results in a misallocation of responsibility across the product value chain.

From a demand-side perspective, consumers tend to believe that regulatory requirements or mandatory standards set a minimum level of digital security and apply for all the IoT products they can buy (Consumers International, 2019[41]), even though it is often not the case. In addition, significant information asymmetries prevent end-users from being able to properly assess the level of security of connected devices: “Consumers are struggling to distinguish between good and bad security in devices primarily due to a lack of information about built-in device security. This further limits the incentives for supply-side actors to develop products with sufficient security built-in from the start” (DCMS, 2018[47]).

Key actors

Software and hardware suppliers and device manufacturers are mostly responsible for these gaps.

Commercial life

Are there any gaps during the product's commercial life?

The maintenance of connected devices during their commercial life seems to be suboptimal. Many connected devices lack a patching mechanism (Schneier, 2018[6]). Even if some IoT products have an update mechanism, the product's manufacturer often does not have a vulnerability management policy in place. A 2018 study (IoT Security Foundation, 2018[54]) of 331 consumer IoT products in the UK showed that 90% of the manufacturers lack a vulnerability disclosure policy.

Product safety

In 2017, security researchers (Leyden, 2017[78]) discovered vulnerabilities in Aga connected ovens. The vulnerability enabled anyone to turn the oven on or off with a text-message. The only information needed was the phone number associated with the oven. On Aga's "register my cooker" webpage, a vulnerability allowed malicious actors or researchers to access the phone numbers associated with the ovens.

The security researchers attempted to contact (Pen Test Partners, 2017[79]) the manufacturer to disclose the vulnerability. However, the company had no vulnerability disclosure policy, and no security team in charge of managing vulnerabilities. No security update or other form of fix (e.g., disabling the remote control function) was provided.

If exploited, the vulnerability could lead to serious consequences for the safety of product's owner, such as fire hazard.

Key factors

These gaps result from externalities, a lack of awareness, a misperception of risks, misaligned incentives and information asymmetries.

The case of Mirai, and botnets in general, exemplifies the prevalence of negative externalities in many products containing code. Only the victims of DDoS attacks were impacted by the botnet, while other stakeholders involved in the value chain, including suppliers, manufacturers, Internet service providers (ISPs) and end-users, were most of the time unaware that the devices were infected and had no incentives to take action.

In the IoT market, the code owners do not implement best practices for the management of newly discovered vulnerabilities (e.g. vulnerability disclosure policies, regular and timely security updates or fixes…) often because of a lack of resources, awareness and incentives. The implementation of these best practices requires digital maturity and awareness, and come with significant costs, which may be at odds with other business priorities (cost effectiveness, etc.).

From a demand-side perspective, the absence of clear information about the producer's policies makes it also difficult for consumers to compare products and make security-conscious purchase decisions.

The challenges related to updating hardware or developing ongoing security functionality in low cost devices are also key elements.

Key actors

Software and hardware suppliers (e.g. application developers) as well as device manufacturers are mostly responsible for these gaps.

End-of-Life

Is the end of commercial life aligned with the end of use?

The end of commercial life for connected devices often seems to not correspond to the end of use. Experts consider that the EOL rate (i.e. the percentage of products that are no longer supported but still in use) for IoT products is likely to be as significant, and probably higher, than for desktop computers and smartphones. In fact, from a lifecycle perspective, the digital transformation means that a community used to short lifecycles (code developers, software companies…) is colliding with a community used to long lifecycles (home appliances, industry…). The effect of that collision is that business models that worked in one community may not be adapted to the other. The resulting gaps are particularly visible in the IoT market, where many products are sold with a limited support period (2-3 years) while their expected length of use could be much longer (Schneier, 2018[6]). As the number of IoT products is expected to reach 20 billion worldwide in 2020, and as their expected length of use will likely exceed the length of support, the EOL gap for IoT products is likely to become a key policy issue in the coming years.

Product safety

In 2018, security researchers (Munro, 2018[80]) discovered vulnerabilities in TP-Link security cameras that allowed malicious actors, through Cross Site Request Forgery (CSRF) (CWE, 2019[81]) techniques, to remotely compromise the cameras' video streams. Even though the product was still widely in use, the product manufacturer considered that it had reached its EOL and therefore decided to not issue any security updates.

If exploited, the vulnerability could lead to indirect but serious consequences for the safety of the product owners: if the camera was protecting a house, criminals could disable it and enter the premises without being detected.

Key factors

These gaps result from externalities, a lack of awareness, a misperception of risks, misaligned incentives and information asymmetries.

In most OECD countries, there are no legal requirements for IoT producers to provide security updates for their products, and no specifications of minimum support periods. The only legal obligation would derive from product safety and liability legislations, whose application to IoT products is very limited (see (EU Expert Group on Liability and New Technologies, 2019[36])). Many IoT producers do not have formal and transparent policies to decide for a product's EOL. In addition, as the IoT market is fragmented and still emerging, many product manufacturers may decide to stop providing commercial support or go bankrupt (Zittrain, 2018[50]), thus leaving a number of IoT devices without security support.

It is also likely that the growing gap between vendors' envisioned EOL and end-users actual use generates tensions in terms of security, especially for smart products that might replace traditional products that had a longer life expectancy (e.g. an oven or a car).

Key actors

Software and hardware suppliers as well as device manufacturers are mostly responsible for these gaps.

Main findings and policy implications

There are significant gaps regarding the digital security of consumer IoT products at every stage of their lifecycle. In many cases, IoT products lack basic security features such as an update mechanism or strong authentication requirements, and are not secured by default, making it easy for users to misconfigure their products. Many IoT manufacturers do not have adequate resources to manage the discovery, disclosure and mitigation of newly discovered vulnerabilities. Finally, in many cases, there are no formal policies regarding the IoT product's EOL, which will likely not be aligned with its end of use.

For policy makers, it means that policy action to enhance the digital security of consumer IoT products should prioritise, in the short term, tools to incentivise product manufacturers to follow security-by-design and security-by-default standards and guidelines. The effectiveness, benefits, risks and limits of various policy tools to achieve this goal (e.g. labels, voluntary frameworks, *ex ante* requirements and *ex post* mechanisms) are further discussed in the policy discussion report (OECD, 2021[2]).

Because the IoT market is still emerging, and many IoT products lack basic security features, most of the policy debate regarding the digital security of IoT has focused so far on the first stage of their lifecycle (design & development). However, gaps are likely to emerge during the commercial life of IoT products as well as after their EOL. The challenges identified in the first case study on smartphones and computers, such as the suboptimal deployment of security updates and the gap between the EOL and the end-of-use, are likely to affect IoT products as well.

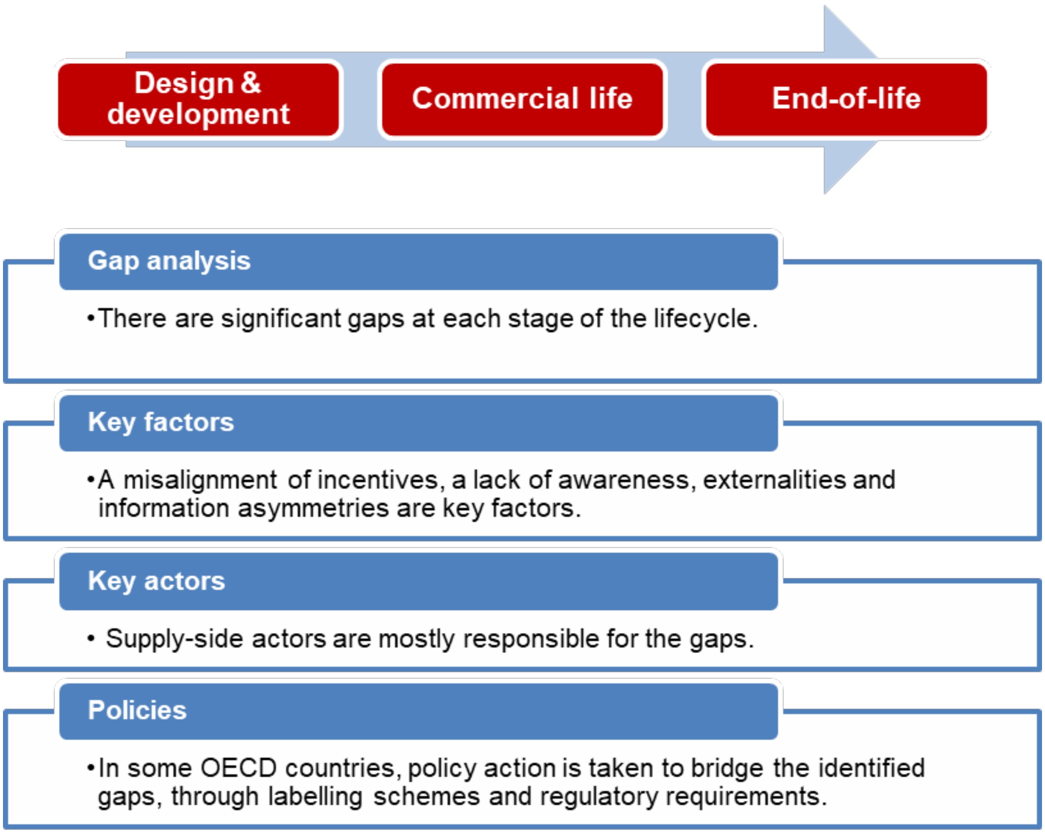
Some authors (Zittrain, 2018[50]) have suggested empowering stakeholders such as the technical community to maintain connected devices after the end of their commercial life, e.g. non-profit "foundations could maintain the code for abandoned products", "like the way the Mozilla Foundation has transformed the 1998 Netscape browser long after its originators left the scene". However, this could create challenges in terms of access to source code and intellectual property rights.

The Mirai botnet attacks demonstrated the global nature of the risk posed by widely used products with a suboptimal level of digital security. Most of Mirai's targets were located in the United States, while most of the infected devices were located in other jurisdictions, such as Brazil, Colombia and South Korea (Antonakakis et al., 2017[51]). Many experts agree on the need for global and coordinated action to enhance the security of IoT devices to prevent their exploitation for botnet attacks (DHS and DoC, 2018[42]).

Product safety

While the Mirai malware that spread in 2016 focused on creating botnets and launching DDoS attacks leading mostly to financial and reputational damages (see Box 4.2), vulnerabilities in IoT products can also be exploited to trigger more tangible negative outcomes. One might argue that DDoS attacks on websites would rank low to medium in terms of severity, while attacks with physical consequences (e.g. making a pacemaker defective or taking control of a connected car) would rank much higher, with significant effects on consumer safety. A significant trend in IoT security is a growing concern regarding potential impacts on the integrity and availability of products and data, which can directly affect safety (Schneier, 2018[6]). Consequently, security breaches in connected devices will likely have more severe consequences in the coming years (e.g., hacked vehicles could cause a number of casualties, as opposed to a breach of personal data).

Consumer IoT products



Design & development

Commercial life

End-of-life

Gap analysis

- There are significant gaps at each stage of the lifecycle.

Key factors

- A misalignment of incentives, a lack of awareness, externalities and information asymmetries are key factors.

Key actors

- Supply-side actors are mostly responsible for the gaps.

Policies

- In some OECD countries, policy action is taken to bridge the identified gaps, through labelling schemes and regulatory requirements.

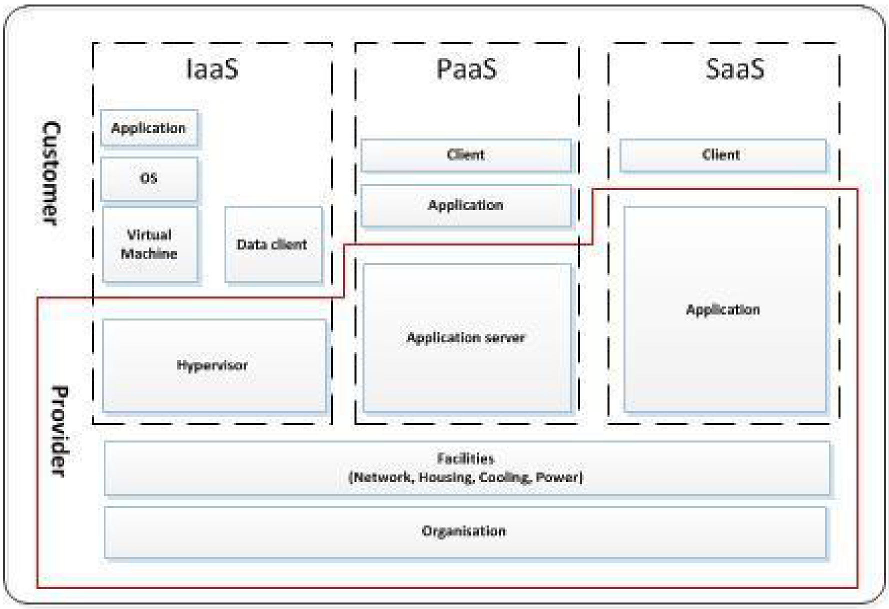
Case study 3: cloud computing services

Introduction

Cloud services can be defined as centrally-hosted and "shared computing and storage resources, accessed as a service, instead of hosted locally" (NCSC, 2020[11]). By subscribing to a cloud service, customers no longer need to acquire and maintain these resources, as they can instead access them on-demand over the Internet, e.g. via a web browser or through APIs.

These resources (Figure A A.2) can include infrastructures (Infrastructure-as-a-service, or IaaS), platforms (Platform-as-a-service, or PaaS) and software (Software-as-a-service, or SaaS). The IaaS model provides processing, storage, networks and other fundamental computing resources only (Mell and Grance, 2011[82]), and allows for complete user control on the OS and other applications, while the PaaS model provides for hardware and middleware resources (e.g. OS). The SaaS model provides even more resources, including applications running on the cloud provider's infrastructure and managed by the cloud provider, such as Customer Relationship Management (CRM) tools. A software available on-demand over the internet, and enabling a user to access data not stored on-premises or on-device, would usually be considered as a cloud service (e.g. most emails service such as Gmail).

Figure A A.2. IaaS, PaaS and SaaS



Source: ENISA, Cloud Security Guide for SMEs, 2015;

In 2018, the IaaS market represented 32 billion USD of revenues globally (Gartner, 2019[83]). This market is relatively concentrated and led by Amazon Web Services (AWS) with a 48% market share, Microsoft Azure (16%), Alibaba (8%), Google (4%) and IBM (2%). The SaaS market represented 84 billion of revenues globally in 2018 (Gartner, 2019[84]), led by Microsoft, Salesforce, SAP, Oracle and Adobe.

Cloud services are usually categorised as either public (the services are provisioned for open use by the general public, and the resources are shared across all clients), private (the resources are provisioned on or off premises for exclusive use by a single organisation), community (the resources are provisioned for exclusive use by a specific community of consumers or organisations that share similar security concerns), or hybrid (a combination of two or more distinct cloud models). More recently, new cloud architectures have emerged to satisfy the end-users' needs: federated cloud and multi-clouds. This case study focuses on public cloud services.

Key actors

From a digital security perspective, the relevant actors for cloud services are the following:

- Cloud service providers;
- Third-party applications providers;
- Users / customers.

Design & development

Are there any gaps in the product's design and development?

The architecture of cloud services presents specific opportunities and challenges in terms of digital security. Some experts consider that shifting from a traditional IT environment to a cloud-based environment usually provides a higher level of digital security (ENISA, 2015[85]), as leading cloud services usually implement state-of-the-art security measures, which tend to be scalable and cost-effective. However, there are also some specific challenges related to the architecture of cloud services:

- **Centralisation**: with cloud services, the user's data is centrally stored. The service provider's data centers are therefore high-value targets for malicious actors (ENISA, 2018[86]), as a data breach may leak a vast amount of information (including personal, financial, etc.). Similarly, a breach in the availability of the service, through a DDoS attack for instance, may impair the functioning of thousands of companies. A security failure at the infrastructure level will also likely compromise the security of all customers.
- **Multitenancy**: in public clouds, many organisations share and store their data in the same infrastructure. An attack leveraging vulnerabilities that allow for a change of scopecould therefore compromise other tenants' data. This is often referred to as "isolation failure" (Brown, Anderson and Tan, 2012[87]) through side-channel attacks. However, such attacks seem to have rarely succeeded so far, as leading cloud services providers have developed strong security measures against them.
- **Conflicts of jurisdiction**: an emerging risk regarding the architecture of cloud services relates to potential conflicts of jurisdiction, in case the service provider, the customer and / or the data center are subject to conflicting legal obligations regarding the confidentiality of data (Church and Potratz Metcalf, 2019[88]), e.g. in balancing personal data protection and law enforcement access to data.
- **Access points**: by definition, cloud services can be accessed from anywhere and from any device, especially if certain security measures such as MFA are not put in place. In addition, if users' credentials are re-used across multiple cloud services, one stolen credential can lead to data breaches across multiple cloud services.

In many cases, digital security incidents related to cloud services (e.g. multiple access points) result from the use of stolen access credentials (Cable, 2018[89]) (Kaspersky, 2020[90]) rather than code vulnerabilities. In 2014, malicious actors managed to access and leak personal data of dozens of celebrities stored in Apple's iCloud service. The sheer number of victims first led experts to suspect the exploitation of a code vulnerability. However, it was later discovered that the attack vector was in fact social engineering (Rushe, 2014[91]). The malicious actors obtained credentials (usernames and passwords) through spear-phishing. This reveals a lack of security in managing access control and monitoring telemetry and logins.

Key factors

There are many incentives for cloud service providers to deploy strong security measures. A major security failure would likely seriously undermine the trust that a public cloud provider needs in order to maintain relationships with its customer base. Cloud providers are also usually subject to a wide range of security requirements in order to meet regulatory and industry compliance frameworks (Cloud security alliance, 2017[92]).

The gaps related to unauthorised access through stolen credentials can be described as resulting from a lack of awareness or poor digital security hygiene on the user side, or as a failure of "security-by-default" measures on the cloud service provider side. Security measures can be used to prevent such unauthorised access, for instance through MFA. Since the 2014 iCloud leakage, such measures (e.g. additional authentication measures when the account is accessed through a new device) have been put in place "by default" on iCloud services.

Key actors

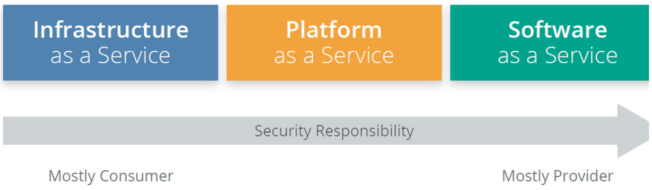
These gaps result from the cloud services providers' policies and from user behaviour.

Commercial life

Are there any gaps during the product's commercial life?

Between IaaS, PaaS and SaaS, the roles and responsibilities of the user and of the cloud service provider vary significantly (Figure A A.3). The responsibility tends to be higher for the service provider in SaaS environments (where they control the infrastructure and the software) but lower in IaaS environments (where they only control the infrastructure).

Figure A A.3. Security responsibility varies across cloud models



Source: Cloud Security Alliance, Security Guidance.

In all cases, the use of cloud services usually entails a shift in responsibility from the client to the service provider, even though the intensity of this shift varies between IaaS, PaaS and SaaS. This shift in responsibility leads to some specific challenges:

- **Loss of governance and visibility** for the user (e.g. monitoring and telemetry).
- **Complex allocation of responsibility**: cloud customers are often unaware of the responsibilities assigned to them within the terms of service, which are often complex and lack clarity (Rundle, 2019[93]). There is often some confusion regarding the attribution of responsibility for activities such as archive encryption or software update.
- **Risk transfer through liability limitations**: typical terms of contract service level agreements (SLAs) significantly limit the liability of the service provider in case of a digital security incident.

These challenges often pave the way for security incidents, such as server misconfigurations, which are one of the most common causes of data breaches in a cloud environment. In 2019, for instance, a flawed firewall implementation in a server managed by the bank Capital One, and hosted by Amazon, allowed the attacker to gain access to more than 100 million Capital One customers' accounts and credit card applications (McLean, 2019[94]).

In SaaS, the deployment of security updates is usually better managed than in traditional IT environment: software modules can be pre-hardened and updated with the latest patches and security settings (Cloud security alliance, 2017[92]). The deployment of security updates seems therefore optimal in SaaS. However, in PaaS and IaaS environments, there is often a lack of clarity about responsibility of each actor. Many incidents in the cloud environment result from unpatched vulnerabilities on applications that are managed by the user or third-party service providers, while the users are not always aware of the responsibility allocation.

Key factors and actors

The gaps result from as a lack of awareness on the user side and / or as a failure to implement "security-by-default" principles on the service provider side. Better user education, co-operation between stakeholders and assessment of the fairness and clarity of SLAs, for instance through certification mechanisms, could help mitigate those gaps.

End-of-Life

Is the end of commercial life aligned with the end of use?

Whether they offer infrastructure, platforms or software, cloud offers are "pure" services, as opposed to IoT devices or smartphones, which are rather on the "goods" side of the "goods-services" spectrum. They are intangible,[29] and entail no ownership transfer as they rely entirely on access. As a consequence, the EOL usually matches the end of use for cloud services. In certain circumstances, however, gaps may emerge. For instance, the bankruptcy of a cloud provider may lead to a breach of integrity, confidentiality or availability of customer's data. Similarly, if there are no legal requirements for data portability and interoperability of cloud services, then it could lead to digital security incidents (e.g. inability for the client to maintain the integrity or availability of their data if they decide to change cloud service providers).

Main findings and policy implications

For cloud services, digital security gaps are mostly related to the architecture of cloud environments and arise during the commercial life. They result from a lack of user awareness or education, a failure to fully implement "security-by-default" principles, a misperception of risks and a difficult attribution of responsibility across the value chain.

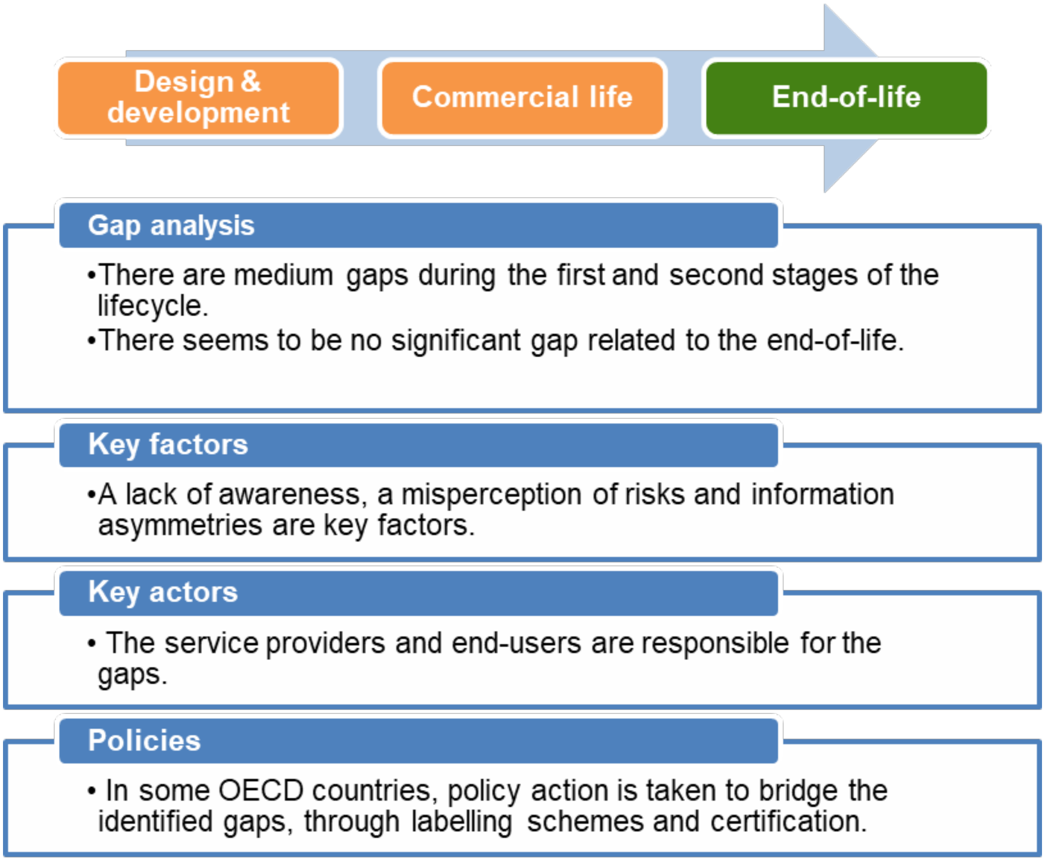
For policy makers, it means that policy action to enhance the digital security of cloud services should focus on:

- Supporting the development of common standards to provide stakeholders with references (e.g. which security controls are the responsibility of the cloud provider, and which ones are the responsibility of the user). While there is no one-size-fits-all approach for all cases, profiles or baselines could prove useful to support risk-based decisions.
- Encouraging cloud providers to clarify their terms of services, e.g. for risk allocation.
- Supporting the development of tools to reduce information asymmetries and allow for comparability of services (e.g. labels, certifications…).
- Developing policy measures to facilitate data portability to make it easy for users to switch from one service to another.
- Fostering end-users' awareness raising and education.
- Facilitating multi-stakeholder partnerships.

- Establishing a certification authority (and a registry) that would be responsible for asserting the security posture of the service providers.

The effectiveness, benefits, risks and limits of various policy tools to achieve this goal (e.g. labels, voluntary frameworks, *ex ante* requirements and *ex post* mechanisms) are further discussed the policy discussion report (OECD, 2021[2]).

Cloud services



Gap analysis

- There are medium gaps during the first and second stages of the lifecycle.
- There seems to be no significant gap related to the end-of-life.

Key factors

- A lack of awareness, a misperception of risks and information asymmetries are key factors.

Key actors

- The service providers and end-users are responsible for the gaps.

Policies

- In some OECD countries, policy action is taken to bridge the identified gaps, through labelling schemes and certification.

Annex B. Areas for future research

This Annex explores areas that have been touched upon in this report and could benefit from further analysis in the future.

Systemic aspects of digital security risk in products

In recent years, vulnerabilities have been discovered in software libraries implementing Internet protocols (Heartbleed, 2014) or microprocessors (Spectre and Meltdown, 2017). Some have argued that these vulnerabilities could be considered as a new class of "systemic" vulnerabilities: the vulnerable components were widely used, and their vulnerabilities affected all the products they were part of, such as websites and smartphones. In June 2020, digital security researchers disclosed the "Ripple20" vulnerabilities (Cimpanu, 2020[25]), which are part of a small software library designed in the 1990s. While relatively unknown to the public, this library has been widely used and integrated into industrial and consumer IoT products in recent years. Hundreds of millions of products are likely to contain the vulnerabilities. However, because the vulnerabilities originated at a lower level of the value chain, which is often opaque and complex, it has been difficult for all actors to be aware of the presence of these vulnerabilities in their products, to coordinate and to respond effectively.

The use of concepts such as "systemic risk" or "systemic products" is an emerging trend in the areas of internet governance and digital security. Whether it is attached to an entity (e.g. an institution or a product) or to the consequences of their potential failure (e.g. harm or risk), "systemic" suggests a higher level of risk, which would call for more scrutiny from policy makers. The following sections explore this notion and propose a working definition based on the measurement of the scale and scope of these products.

Conceptual approach

From a conceptual perspective, "systemic" entails an impact on the system itself (e.g. the economy or the global Internet), as opposed to only one part of the system (e.g. a single company or a single economic sector). Systemic risks result from the interlinkages and interdependencies in a system or market, where the failure of a single entity or cluster of entities can cause a cascading failure. Historically, systemic risks have been mostly associated with the financial sector. A collapse of one or several major financial institutions (often considered as "too big to fail") would likely lead to the collapse of the financial sector, which would in turn likely lead to the collapse of the whole economy, as other economic sectors depend on the financial sector to function (e.g. for liquidities, loans…).

The concept of "systemic" can also be associated with criticality (critical activities or infrastructures), which refers to certain economic and social activities, the interruption or disruption of which would have serious consequences on national security, the effective functioning of services essential to the economy and society or economic and social prosperity more broadly (OECD, 2019[95]).

Systemic products and digital security

In 2018, the Paris call for trust and security in cyberspace (Paris call, 2018[96]) condemned malicious activities, in particular "the ones threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure". Similarly, the Global Commission on the Stability of Cyberspace (GCSC, 2018[97]) introduced the concept of a "public core" of the Internet and considered that there are "products […] on which the stability of cyberspace depends" and for which developers and manufacturers should "take reasonable steps to ensure that [they] are free from significant vulnerabilities". The GCSC lists a number of products as potential candidates, such as "operating systems", "Industrial Control Systems", "routers" and "widely used end-user consumer applications". The report does not provide, however, specific criteria to define "systemic", which could virtually apply to a wide range of products.

Tentative definition

There is no internationally agreed definition of what a "systemic" product would be in the areas of internet governance and digital security. The following section aims to propose two criteria for such a definition: scale and scope.

Scale

The first criterion to define a "systemic" product could be the scale of its use, which can be measured by the number of users. Above a certain number of users (e.g. 100 M users), a product would be defined as "systemic". In addition to the absolute number of users, the relative market share of the product is important. In fact, a limited market share may enable users to easily switch to other products, while a dominant position of the product will likely increase its systemic risk. A vulnerability in a single product that is widely used would enable security incidents to scale to the point they would affect the whole system, as opposed to only a part of it. Digital security attacks exploiting vulnerabilities in widely used products could affect the product itself or other products. Two recent examples illustrate the notion of scale:

- In 2017, the WannaCry and NotPetya malwares exploited vulnerabilities present in Windows operating systems, which represent a 78% market share of operating systems for personal computers (StatCounter Global Stats, 2021[63]) (StatCounter Global Stats, 2021[64]). The ransomwares encrypted all data on the infected computers, making them unavailable for authorised users and resulting in the paralysis of global companies in many sectors (e.g. health, industry, transport).
- In 2016, the Mirai botnet exploited vulnerabilities in consumer IoT products such as security cameras and routers. While the malware did not affect the availability of these products for authorised users, it enrolled them into a botnet, which was then used to launch massive DDoS attacks. At the peak, several hundreds of thousands of IoT products were compromised.

However, using scale as the only criterion might be misleading. While some products are widely used, a breach of their availability, integrity or confidentiality would not necessarily result in systemic consequences. For instance, the Candy Crush application has more than 270 M users, but would probably not be considered "systemic", as its unavailability would be unlikely to affect the entire system (e.g. the Internet or multiple sectors of the economy).

One should also differentiate vulnerabilities from threat vectors. A widely used product can be used as a threat vector to spread a malware, while the vulnerability itself, whose exploit will cause systemic consequences, lies in another product. In 2017, malicious actors used the update mechanism of the accounting software MeDoc (used by the majority of Ukrainian companies) as a threat vector (Greenberg, 2017[34]). The update spread the virus NotPetya, described above.

Scope

In addition to scale, an important criterion to define a systemic product could be the scope. The scope can be measured by the degree of interdependency of the product, which can relate to:

- Economic and social activities: users are dependent on the product to perform certain social and economic activities. This could include communications (e.g. WhatsApp, Gmail…), office productivity (e.g. Word or Excel) or the management of industrial systems (ICS).
- Other products: certain products rely on other products (operating systems or components like microprocessors) to be able to function.

A systemic product would likely entail a change of scope, as the risk is no longer contained within one application, one company or one sector, but spreads beyond, to other products or to the economic and social activities that are enabled by the product.

From a value chain perspective, this interdependency would be referred to as a "bottleneck", constituting for their users the main point of access to other products, or the main tool to achieve certain economic and social activities. Consequently, the Candy Crush app would not be considered as "systemic" because a breach of its availability, integrity or confidentiality would not prevent users from accessing other products or achieving essential economic and social objectives. Alternatively, a critical vulnerability in WhatsApp or in microprocessors would likely have systemic consequences.

Working definition and scoring

A working definition of systemic products could therefore rely on measuring its scale and its scope. The examples below are only given for illustrative purposes.

- Scale (from 1 to 4):
  - Absolute number of users.
    - Null (<1M): 0 point.
    - Limited (1~10 M): 0.5 point
    - Medium (50~100M): 1 point
    - Significant (100~500M): 1.5 point
    - Critical (+500M): 2 points
  - Relative market share
    - Null (<5%): 0 point.
    - Limited (5~10%): 0.5 point
    - Medium (10%~30%): 1 point
    - Significant (30%~50%): 1.5 point
    - Critical (>50%): 2 points
- Scope (from 1 to 4):
  - Interdependency to perform economic and social activities
    - Null: 0 point.
    - Limited (e.g. videogames): 0.5 point
    - Medium (e.g. home appliances): 1 point
    - Significant (e.g. communications): 1.5 points
    - Critical (e.g. critical infrastructures, health, transport): 2 points
  - Interdependency to other products
    - Null: 0 point.
    - Limited: 0.5 point.

- Medium: 1 point.
- Significant: 1.5 point.
- Critical (e.g. operating systems, microprocessors): 2 points.

Considering these criteria, the following categories of products could fall under the “systemic” umbrella: cloud services and operating systems (Maynard, 2017[98]), as well as routers, microprocessors or some widely used open-source libraries.

Policy impact

From a policy perspective, products associated with systemic risks deserve particular attention. Policy makers could set higher requirements (accountability, transparency, duty of care…) on such products. The working definition of systemic products may vary from country to country dependent on the absolute number of users in relation to the amount of citizen or the relative market share of a certain industry.

Digital security and open-source products

There has been much debate about the role of open-source code for the digital security of products.

There are two main criteria to define open-source code (Open source initiative, 2020[99]):

- Free Redistribution: the open-source license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.
- Access to source code: the open-source program must include source code, and must allow distribution in source code as well as compiled form. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a translator are not allowed.

The benefits and limits of open source software with respect to digital security have been a matter of debate for many years in the digital security community. For some, the openness (or public availability) of open source code enables many advanced users to review the code, find vulnerabilities and propose fixes. However, others have argued that the possibility of review does not guarantee the effectiveness of review.

More specifically, there is an argument about the application of the responsibility principle to open-source products. Can a single individual or developer be held responsible for a digital security gap in an open-source product, or should the entire community be held responsible? How would liability regimes apply in such cases? What incentives are in place to drive stakeholders to act responsibly and take their fair share of responsibility?

Furthermore, while the use of proprietary code products may result in a tragedy of the anticommons,[30] the use open-source products may result in a tragedy of the commons. For economists, the tragedy of the commons usually refers to a situation where the absence of ownership rights for a common good (defined as non-exclusive but rival[31]) results in the overuse of the resource. Economic agents would rationally seek to gain maximum profit by using the resource, and the absence of ownership rights would not allow any limitation of the use of this resource. Typical examples include public space such as pastureland. In the context of digital security and open source, the absence of ownership rights does not lead to overuse, as software is non-rival (the consumption of one unit does not prevent others to use the resource). However, the absence of ownership rights may, in some cases, disincentivise economic agents to devote time and resources to maintain the resource, even though it is widely used.

To address this issue, common resources need to be allocated to public goods (defined as non-rival and non-exclusive, a definition that is aligned with open-source code). Several initiatives are underway to achieve this goal, such as the Core Infrastructure Initiative (see the policy discussion report (OECD, 2021[2])).

These aspects could be further explored at a later stage.

Digital security of products in low-income countries

Low-income countries face particular challenges for the digital security of products. The following issues and trends seem to indicate that stakeholders in these countries are, and will continue to be, particularly vulnerable to digital security risks associated with smart products:

- Managing digital security **throughout the commercial life**: in low-income countries, the availability and quality of service of broadband is often much lower than in high-income countries. This can significantly limit the ability of stakeholders, including network operators and end-users, to deploy security updates in a timely and effective manner.
- **EOL**: in low-income countries, many smart products, including smartphones, computers and IoT devices, are purchased on secondary markets, often after they have reached their EOL in high-income countries. This means that end-users in these markets will likely purchase products that have already reached their EOL and are no longer supported. As a result, the digital security risks related to the EOL gap may become much more significant in low-income countries in the near future.
- Access to quality control: tools that enable quality assurance and conformity assessments (e.g. certifications, labels…) are often expensive, and may be less accessible for stakeholders in low-income countries.
- Education and awareness.

New public policy governance frameworks

Code is becoming widespread in products across many sectors. This overlap raises challenges in terms of governmental responsibility and oversight. In some cases, it may call for new frameworks to clarify roles and better integrate digital security policy across ministers and institutions.

For example, in March 2019, the German Federal Ministry of the Interior introduced a draft bill for the IT Security Act 2.0 (IT-SiG 2.0). The bill would extend the competences of the Federal Ministry for Information Security (BSI) by adding new responsibilities regarding consumer protection, assessment of IT products and systems, including mobile and IoT, as well as detection and mitigation of malware and security gaps.

In France, the agency in charge of digital security (ANSSI) has developed in-house sectoral expertise, with teams dedicated to addressing the digital security challenges of specific economic sectors.

The impact of emerging technologies on the digital security of products

Emerging technologies will likely have a significant impact on the digital security of products. So far, research has focused on how such technologies can positively impact the digital security of products, e.g. how blockchain could enhance the traceability of components for smart products. However, the impact of emerging technologies is likely to be more nuanced, and could go both ways. In a world where AI-based decisions are becoming pervasive, what is the potential for malicious actors to abuse and exploit AI systems to cause harm? Can they use AI to bypass traditional digital security measures? Alternatively, can AI bring digital security to the next level, e.g. by helping us develop more secure code, detect anomalies, mitigate intrusions and reduce the overall level of digital security risk? What would be the consequences of a situation where stakeholders are forced into an AI digital security arms race against malicious actors? These questions could be further explored.

Notes

[1] To use an analogy, one could argue that to address car theft, governments can look at both policies and tools to make the car more secure, and policies and tools to better prosecute the criminals. This report focuses on enhancing the digital security of products, not on prosecuting or deterring malicious actors.

[2] In 1992, the OECD adopted guidelines for the security of information systems.

[3] To avoid confusion, the term “smart products” was preferred to “digital products” because the latter is used in other international policy contexts (e.g. trade) to designate products that are “purely” digital, without a physical component (e.g. software).

[4] Software and code are often used interchangeably.

[5] Notions such as vulnerability, exploit, and mitigation are further explained in the report on vulnerability treatment (OECD, 2021[3]).

[6] Through open or closed networks, such as the Internet and organisations’ internal networks (“intranet”), as well as through IP or other protocols such as Bluetooth.

[7] The ability of a product to connect fundamentally changes the nature of the attack vectors: vulnerabilities can be exploited remotely, through the network, as opposed to machines that can only be accessed physically.

[8] Guarantees or liability law can be considered as ways to transfer the risk to supply-side actors (see 3.2).

[9] Digital security attacks such as Stuxnet demonstrated that air-gapped networks could also be breached, e.g. through targeting the supply chain, using a compromised USB device or near-field wireless solutions. Air-gaping reduces the risk without entirely eliminating it.

[10] For more details, cf. the Companion document of the 2015 Recommendation (OECD, 2015[17])

[11] Vulnerabilities are further discussed in the report on vulnerability treatment (OECD, 2021[3]).

[12] In this context, the term “vulnerability” is much broader than “code vulnerability”, and refers to any weakness that could be exploited and impact the confidentiality, availability or integrity of data, software, hardware and networks.

[13] For instance, in France, the risk assessment method EBIOS Risk Manager uses a two-layer model for digital security risk scenarios. First, operational scenarios at the technical level, where the target is a “critical asset”, such as an information system). Secondly, strategic scenarios at the business level focus on “feared events” such as tangible consequences on “business assets” (https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/).

[14] In the automobile industry, crash tests would typically take into account environmental factors, for instance extreme weather conditions. While this could be considered as a form of threat modelling, it would usually not include intentional threats.

[15] For instance, in the European Union, Directive 85/374/EEC on liability for defective products compels producers to provide compensation for any defective product that causes physical damage to consumers or their property. The EU Commission is currently working on evaluating the impact of new technologies such as the Internet of Things on this directive and on the potential need to revise it.

[16] They include 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.

[17] Depending on the context, a "zero day" is a vulnerability for which no mitigation has yet been released or a vulnerability that is unknown to the vendor, i.e. the vendor has had zero days to develop a mitigation.

[18] Vulnerabilities are further discussed in the vulnerability treatment report (OECD, 2021[3]).

[19] These issues are examined in depth in other reports, such as (Levite, 2019[128]).

[20] For instance, Article 4 of the EU's GDPR has set up two new categories of actors: data controllers and data processors.

[21] In American slang, a "lemon" is a "bad" or low-quality car.

[22] In this example, information asymmetries lead to a situation where all used cars are sold for the same average price, no matter what their level of quality is, which is impossible to assess for the buyer before the purchase. The sellers, on the other hand, know the quality of their products. The owners of a "lemon" will therefore sell their car at the average price (which is well above the value of their car, generating a comfortable margin) while the owners of a "good" car will end up leaving the market, because the average price will be below the value of their car.

[23] While recognising that the architectures of smartphones and desktop computers are different, this case study shows that the digital security challenges for both categories of products are quite similar. A notable difference is that OEMs have a more prominent role in the market for smartphones, in particular for Android products, as they often act as a control point for the deployment of security updates and for determining the product's EOL. For desktop computers, however, the role of OEMs is much less significant.

[24] For a thorough mapping of IoT standards, see (DCMS, 2018[102]).

[25] Open SSL (Secure Sockets Layer) is an open-source cryptography library used to implement the TLS (Transport Layer Security) protocol in web servers and applications.

[26] This argument compares a situation in which a corporate actor is clearly responsible for maintaining a product to a situation in which an informal community would be responsible for maintaining the product. However, in the case of EOL products, one should rather compare a situation in which no security support is possible (as supply-side actors do not provide support and do not authorise third-parties to provide support), to a situation in which some security support is possible for the user community. As a result, it seems that the transfer of responsibility and intellectual property to the open-source / user community is likely to be more optimal than the absence of any security support.

[27] Alternatively, a security breach of a sub-component of a desktop computer or of a smartphone (e.g. an application) would likely not prevent the user from continuing to use the product.

[28] While recognising that the architectures of smartphones and desktop computers are different, this case study shows that the digital security challenges for both categories of products are quite similar. A notable difference is that OEMs have a more prominent role in the market for smartphones, in particular for Android products, as they often act as a control point for the deployment of security updates and for determining the product's EOL. For desktop computers, however, the role of OEMs is less significant.

[29] Even though cloud offers rely on the use and management of infrastructures such as a data centres by the provider, from the customer's point of view, the use of the product is entirely intangible.

[30] A situation where ownership rights that are too stringent limit the ability of stakeholders to use a resource optimally, or to maintain it in an optimal manner (Heller, 1998[60]).

[31] A good is rival when its consumption by one economic agent prevents another agent from consuming it (e.g. food) and non-exclusive when economic agents are not able to exclude others from consuming it. Alternatively, a good can be non-rival (e.g. air) or exclusive (e.g. a private club).