STI Policy Note

www.oecd.org/sti

Smart policies for smart products

A policy maker's guide to enhancing the digital security of products

This policy brief summarises the main findings of two reports published by the OECD in 2021: "Understanding the digital security of products: An in-depth analysis" (OECD, 2021a) and "Enhancing the digital security of products: A policy discussion" (OECD, 2021b).

From "traditional" software to cloud services and Internet of Things (IoT) devices, our economies and societies are increasingly reliant upon "smart products", i.e. products that contain code and can interconnect, e.g. through the Internet. In recent years, cyber-attacks such as Mirai, WannaCry, NotPetya and SolarWinds have underlined that the exploitation of vulnerabilities in smart products can have severe economic and social consequences. Beyond financial losses and reputational damages, these attacks are also increasingly impacting users' safety and can threaten human lives.

Too often, making smart products "secure enough" is considered only as a technical issue calling for technical remedies. However, economic factors play an important role in the relative "insecurity" of smart products, and market incentives on their own are unlikely to fix digital security gaps. Complex and opaque value chains often lead to a misallocation of responsibility for digital security risk management, while information asymmetries and externalities limit stakeholders' ability to behave optimally. While code is everywhere, smart products are relatively new and do not necessarily fit in the legal categories of the 20th century. The application of liability laws, certification, insurance and guarantees to smart products is challenging, and will likely require a review of existing legal frameworks to adapt them to the dynamics of the digital economy.

The quick read

Policy makers have a key role to play to realign market incentives towards an optimal level of digital security for smart products. Increasing transparency and information sharing, promoting co-operation (including at the international level), and ensuring the duty of care of supply-side actors (e.g. through the principles of security-by-design, security-by-default and responsible end-of-life) are important avenues for policy action. Many policy tools can be leveraged to achieve these objectives, from public procurement, certification and multi-stakeholder partnerships, to labels and *ex ante* legal requirements. This policy brief and the two associated reports (OECD, 2021a; 2021b) explore these various tools extensively, analyse their benefits and limits, and provide key insights regarding their implementation across OECD countries.

In this regard, international co-operation stands out as a key success factor. Policy makers should learn from other countries' successes and challenges, and leverage policies that have already proved successful elsewhere. Some cutting-edge policies developed nationally have formed the basis of emerging international norms. For example, a code of practice developed by the government in the United Kingdom paved the way for the European Telecommunications Standards Institute (ETSI)'s technical specification for consumer IoT security. International co-operation is also instrumental to enabling interoperability between national approaches, avoiding norm proliferation and limiting inconsistencies across jurisdictions, which could significantly inhibit the development of the digital economy.

Code is everywhere

Governments, businesses and consumers today are increasingly dependent upon smart products: a category that includes "pure" software, "traditional" information technology products such as laptops and smartphones, and products associated with emerging technologies, such as Internet of Things (IoT) devices. 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 owned at least one connected device in 2019.

The COVID-19 crisis has accelerated the digital transformation, highlighting our increasing reliance on such products. As governments across OECD countries imposed lockdown measures to contain the pandemic early last year, the workforce in many sectors massively shifted to teleworking, in some cases 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.

It is difficult to measure the **global cost of digital security attacks** that leverage vulnerabilities in smart products. Many attacks remain undetected, and many organisations choose to protect their brand reputation and do not disclose that their assets have been compromised. In addition, digital security attacks resulting in personal data breaches and intellectual property theft affect non-financial assets, which makes their cost difficult to quantify. However, common estimates of global costs range from USD 100 billion to USD 6 trillion annually, and suggest that the amount is rising every year.

Code is vulnerable

Because all smart products contain code, they are all, to some extent, vulnerable. In fact, code almost always contains vulnerabilities that 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 it is likely that 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 United Kingdom's National Health Service (NHS). These attacks showed that the successful exploitation of a vulnerability in a single product can paralyse global firms and lead to billions of US dollars in damages.

Why are smart products vulnerable?

In this context, several questions are most pertinent. Why are smart products so vulnerable? Is it only a matter of technical standards and architectures, or are there economic factors at play as well? What are the responsibilities of governments, supply-side actors and end-users? What are the key dynamics and challenges, and are they similar across different markets?

To answer these questions, the OECD developed **an analytical framework based on smart products' lifecycle and value chain** (OECD, 2021a). This framework aims to identify gaps in the management of digital security risk in smart products, as well as the factors and actors responsible for these gaps. It finds that different digital security gaps may arise at different stages of the product's lifecycle:

- If the development process did not follow industry best practices for "security-by-design", smart products may contain many vulnerabilities. As time-to-market is key for many supply-side actors, the "build first, patch later" approach is common.
- Alternatively, a product's level of digital security may be considered sufficient at the beginning of its commercial life, but decrease over time if newly discovered vulnerabilities are not effectively addressed, e.g. through the timely development and deployment of security updates. If the product lacks an update mechanism, or if supply-side actors do not manage vulnerabilities effectively, e.g. through vulnerability disclosure policies and automatic security updates, gaps are likely to arise.
- Smart products tend to become less secure over time as their vendors stop providing security updates, based on the rationale that these products have reached their end-of-life (EOL). As highlighted by the WannaCry digital security attack, many products continue to be used after their EOL. Such gaps between the EOL and the end-of-

use (EOU) show how economic factors, and not only technical ones, contribute to a suboptimal digital security level in many smart products.

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. The vendors of these final products may not always be best placed to provide updates, if they are not responsible for the vulnerable layer of code. The OECD report therefore proposes to use the concept of "code owners" rather than vendors to facilitate the identification of responsible parties, and to bring more clarity to the allocation of responsibility (2021a).

The WannaCry ransomware (2017)

The WannaCry malware, which appeared in May 2017, 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 versions of Windows that were commercially supported at that time; this included Windows Vista and 7, but not, for instance, Windows XP and Server 2003, which had reached their EOL. Yet the latter versions were still widely used by less digitally mature organisations, such as small- and medium-sized enterprises (SMEs) and institutions in the healthcare sector. On 13 May, one day after the attack began, Microsoft released an emergency security update for the Windows versions it no longer supported.

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 NHS in the United Kingdom. These 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.

The virus seriously impaired the functioning of hospitals, plants and production lines. Estimates of total damages from the attack range from several hundred million to several billion euros. These damages arose, in part, from the inability of organisations to function properly for weeks, the costs of cleaning up, upgrading or replacing compromised information systems, and harm to brand reputations. In 2018, semi-conductor manufacturer TSMC had to shut down its production line for several days due to a virus that was similar to WannaCry.

Some of the organisations that fell victim to WannaCry could be considered "mainstream users", 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). Other victims, however, included global organisations that were leaders in their sectors (e.g. transport or automotive). This 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 SMEs, consumers and other mainstream users.

Source: OECD (2021a), "Understanding the digital security of products: An in-depth analysis", https://doi.org/10.1787/abea0b69-en.

Digital security gaps are often caused by economic factors

To understand why code is vulnerable, **the OECD's in-depth analysis report examines** three case studies: i) smartphones and desktop computers; ii) consumer IoT; and iii) cloud services (OECD, 2021a).

These case studies show that technical measures such as multi-factor authentication (MFA) or automatic security updates are key to enhancing 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 alone are usually not sufficient to drive optimal behaviours**.

Significant information asymmetries often prevent end-users – and particularly mainstream users such as SMEs and consumers – from making 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, as customers were often unable to compare such tools on the basis of digital security risk.

In addition, **negative 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 effect on the digital security of products.

More broadly, **there is a misperception of digital security risk and a misalignment of market incentives**. For supply-side actors, the gap between EOL and EOU can be closed by incentivising end-users to buy new products (which may have stronger digital security features or architectures), while end-users tend to not see the benefits of spending money to buy newer products and are often unaware of the risk. With billions of IoT products reaching their EOL in the coming decade, the possibility of an "Internet of forgotten things" is a looming policy challenge.

Key insights for policy makers

Below are the main findings of the case studies (smartphones and desktop computers; consumer IoT; and cloud services):

- Consumer IoT products have significant digital security gaps at each stage of the product lifecycle.
- The three case studies show significant digital security gaps during the product's commercial life (misconfigurations or limited deployment of security updates).
- The EOL gap is highly significant for goods such as IoT products and smartphones, but less significant 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 reports also shed light on some key insights for policy makers:

- The digital security of products should be seen as a continuum, rather than as a binary concept of secure or insecure. A product may be "secure enough" for a given context of use, while its level of digital security may be suboptimal in other situations.
- Managing the digital security of products goes beyond technical aspects: many economic factors are at play, and market forces 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 with 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 (OECD, 2021c).
- There is no one-size-fits-all solution or panacea. The digital security of products is complex, spanning many sectors, markets, product categories and policy areas.

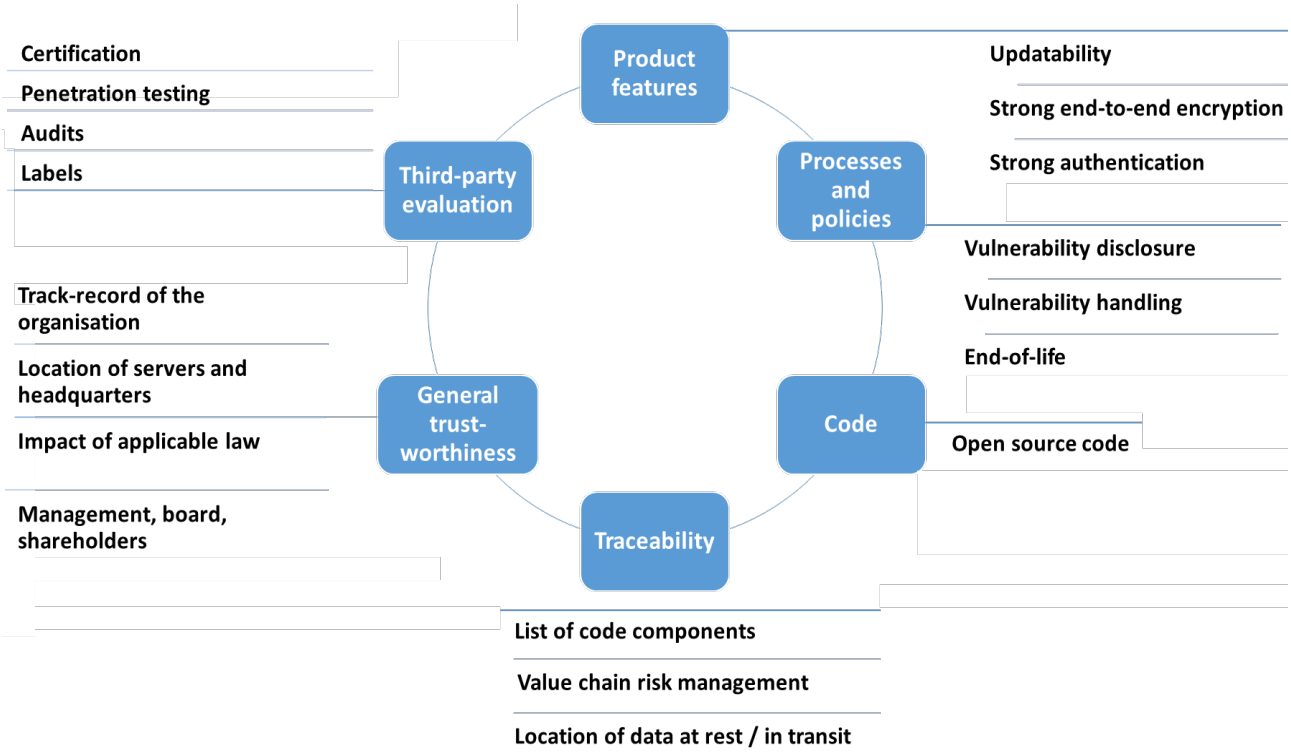
Six high-level principles to enhance the digital security of products

To address these challenges, the policy discussion report (OECD, 2021b) outlines **six high-level principles** that can guide policy makers and stakeholders in enhancing the digital security of products:

- **Increasing transparency and information sharing**, in order to address information asymmetries. Figure 1 provides an overview of six key areas where increased transparency would enable customers to make more informed, risk-based decisions. It shows that in addition to products' technical features (e.g. updatability), other areas would benefit from more transparency, including the processes and policies put in place by supply-side actors (e.g. EOL), the traceability of products' components and third-party evaluation.
- **Raising awareness and empowering stakeholders**, in particular end-users and security researchers, as they have a key role to play in managing digital security risk.

- **Ensuring responsibility and duty of care** for supply-side actors, to tackle externalities and realign market incentives. The principle of duty of care can be broken down into five sub-principles: security by design, security by default, dynamic management of digital security, digital security of the organisation and responsible EOL policies, which can address issues related to the length of support and the product's reparability.
- **Increasing co-operation** between stakeholders, government agencies and at the international level to enhance the digital security of products.
- **Promoting innovation and competition**, to unleash the positive potential of market forces.
- **Addressing digital security with proportionality, through a risk-based approach**, to account for complexity. Digital security requirements that may be necessary or effective for one market or product category may not be appropriate for another.

Figure 1. Potential areas of focus for increased product transparency and information sharing



Source: OECD (2021b), "Enhancing the digital security of products: A policy discussion", https://doi.org/10.1787/cd9f9ebc-en.

A policy toolkit: "Smart policies for smart products"

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

The dichotomy of government intervention vs. "laissez-faire" is increasingly seen as too simplistic to capture the broad spectrum of policy options available to enhance the digital security of products**.** A 2020 report by the United States' Cyberspace Solarium Commission recognised that "the status quo is not getting the job done". Policy makers can leverage many tools, from awareness-raising campaigns and multi-stakeholder partnerships, to labelling schemes and regulatory requirements. Importantly, these tools are not mutually exclusive, and there is no panacea or one-size-fits-all solution. **A strategy to enhance the digital security of products will likely require a mix of policy tools to be most effective**.

A policy toolkit outlined in the report (OECD, 2021b) aims to enable governments to foster the adoption of the high-level principles, focusing on the "how" rather than on the "what". The toolkit discusses emerging policy trends, illustrated with selected examples from OECD countries. The format of the toolkit acknowledges that each government may rely on the policy tools that are the most consistent with its country's culture, history and style of government. It discusses the following policy tools:

- **Raising awareness among mainstream users and developing digital security skills** in order to grow the expert workforce of advanced users is the starting point of public policies aimed at enhancing the digital security of products. Yet although awareness-raising campaigns are important, they alone would not be sufficient to address the economic challenges mentioned above.
- **Beyond their role as regulators, governments are also economic agents. As such, they can leverage their purchasing power and lead by example** to influence the behaviour of other stakeholders. Governments can use public procurement policies to incentivise supply-side actors to certify the digital security of smart products, and should themselves adhere to the principles they often call on others to follow – for instance, regarding the timely patching of vulnerabilities.
- **Technical standards and voluntary frameworks are paramount**. Developed by the government or the multi-stakeholder community, they provide supply-side actors with clear guidance that can be adapted to specific markets or product categories. However, in markets where externalities and information asymmetries are significant, the uptake of voluntary guidance is likely to be limited.
- **Labels** could incentivise supply-side actors to adhere to standards and frameworks, and contribute to reducing information asymmetries. As of November 2020, Finland, Germany and Japan have launched, or are considering launching, digital security labelling schemes for specific product categories such as consumer IoT or routers. However, consumer fatigue and a lack of uptake by the industry need to be considered as potential drawbacks of labelling initiatives.
- ***Ex post* mechanisms have great potential, but their effectiveness needs to be further assessed**. Although code is everywhere, smart products are relatively new and do not necessarily fit in the legal categories of the 20th century. Applying liability laws, insurance and guarantees to smart products is challenging, and will likely require a review of existing frameworks to adapt them to the dynamics and complex value chains of the digital economy.
- **Finally, there is growing interest in some OECD countries to develop more stringent regulations to enhance the digital security of products**. From technical requirements to high-level principles, such *ex ante* regulations could be very effective at realigning market incentives and ensuring the duty of care of supply-side actors. However, *ex ante* requirements carry a risk of disproportionate use, and an ill-prepared law could quickly become obsolete or unenforceable. The report (OECD, 2021b) examines the opportunities and challenges associated with *ex ante* requirements, and provides some key insights into, for instance, the need for technological neutrality, proportionality and international co-operation.

More international co-operation is key

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

In this regard**, international co-operation stands out as a key success factor**. Policy makers should **learn from other countries' successes and challenges**, and leverage policies that have already proved successful elsewhere.

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

Further reading

OECD (2021a), "Understanding the digital security of products: An in-depth analysis", *OECD Digital Economy Papers* No. 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en.

OECD (2021b), "Enhancing the digital security of products: A policy discussion", *OECD Digital Economy Papers* No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

OECD (2021c), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers* No. 307, OECD Publishing, Paris, https://doi.org/10.1787/0e2615ba-en.

OECD (2020a), "Dealing with digital security risk during the Coronavirus (COVID-19) crisis", OECD Publishing, Paris, http://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/.

OECD (2020b), "Seven lessons learned about digital security during the COVID-19 crisis", OECD Publishing, Paris, https://read.oecd-ilibrary.org/view/?ref=137_137440-yavecbtye4&title=Seven-lessons-learned-about-digital-security-during-the-COVID-19-crisis.

Website

https://oe.cd/security

Directorate for Science, Technology and Innovation Policy Note

This series of Policy Notes is designed to make available, to a wider readership, selected studies that have been prepared for use within the OECD.

Comment on this Policy Note is invited, and may be sent to OECD, 2 rue André Pascal, 75775 Paris Cedex 16, France, or by e-mail to digitalsecurity@oecd.org.

Please cite this note as:

OECD (2021), "Smart policies for smart products: A policy maker's guide to enhancing the digital security of products", *Directorate for Science, Technology and Innovation Policy Note*, OECD, Paris, www.oecd.org/digital/smart-policies-for-smart-products.pdf.