OECD Policy Framework on Digital Security

CYBERSECURITY FOR PROSPERITY

OECD

Please cite this publication as:

OECD (2022), *OECD Policy Framework on Digital Security*, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en

Note to Delegations:

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

DSTI/CDEP/SDE(2021)12/FINAL

Corrigendum:

An early version of this document from December 2022 was revised:

Page 3: one paragraph was added at the end of the Foreword
Page 6-7: references to OECD Recommendations were updated
Page 20: endnote 12 was deleted and the reference to the report on *Assessing National Digital Strategies and their Governance* was updated
Page 31: reference to the *Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities* was updated

Foreword

The OECD has been at the forefront of international efforts in guiding policy makers in the area of digital security since 1990 and has become the primary international standard setter in this area. OECD Recommendations on digital security support stakeholders in developing digital security public policies for economic and social prosperity, in line with the OECD's mandate to help governments develop "better policies for better lives".

The OECD Policy Framework on Digital Security helps policy makers understand the economic and social dimension of cybersecurity, raises their awareness about the OECD approach to digital security policy, and encourages them to make use of OECD digital security Recommendations to develop better policies. The Framework provides a helpful narrative based upon OECD digital security Recommendations and identifies linkages with other policy areas addressed through existing OECD standards and tools.

The Framework also solicits interested partner economies to join the international dialogue taking place at the OECD on digital security and to align their policies with the OECD Recommendations in this area. All OECD Recommendations covered by this Framework have been developed through a multi-stakeholder process, with the active participation of the business, civil society, and technical communities. Therefore, the Framework also serves as a tool to facilitate multi-stakeholder dialogue at the domestic and international levels.

The Framework was drafted by Laurent Bernat, with input from Ghislain de Salins, and under the supervision of Audrey Plonk, Head of the Head of the OECD Digital Economy Policy Division Division. It benefited from input and feedback from delegates of the Working Party on Security in the Digital Economy and Committee on Digital Economy Policy.

Table of contents

FIGURES

BOXES

Introduction

The accelerating digital transformation of our economies and societies brings remarkable benefits to businesses, public sector organisations and individuals, from enhanced competitiveness and improved well-being, to increased resilience during major catastrophes such as the global COVID-19 pandemic. However, this transformation has been increasing our digital dependency as well as the scope, scale and overarching complexity of organisations' information systems, networks, data assets and data flows. Organisations have not always sufficiently assessed the digital security risk incurred by this evolution, nor taken proportionate security measures to manage it. Individuals are confused by complex cybersecurity technical jargon, settings and procedures such as updates, authentication processes, etc. Products and services are not sufficiently secure and expose users to security risks without giving them appropriate information and means to mitigate them. Criminal and state-sponsored threat actors are taking advantage of this situation, scaling up their nefarious actions for financial, political, and geopolitical gains, amongst others. Recent research suggests that the global cost of cyberattacks ranges from USD 100 billion to USD 6 trillion annually and that the amount is rising every year (OECD, 2021[1]). While individuals fall victim of identity theft schemes, cyberfraud, and personal data breaches, businesses face cyberattacks that harm their assets, reputation and competitiveness, and can even result in disruption of global supply chains, as demonstrated by the 2017 Wannacry and NotPetya attacks.

In this context, the economic and social dimension of cybersecurity is becoming a public policy priority as governments realise that market forces alone are insufficient to incentivise businesses, public sector organisations and individuals to better manage digital security risk, according to their role. For example, economic factors such as externalities, information asymmetries, and misaligned incentives often prevent software developers to develop "secure-by-design" products and organisations to step up their digital security risk management and more systematically address vulnerabilities (OECD, 2021[2]; OECD, 2021[1]).

The OECD is an international organisation where policy makers share experience and good practices, and establish a fruitful dialogue with the business, technical and civil society communities. It also develops widely recognised in-depth policy analyses and standards that are evidence-based, balanced and neutral. The OECD has been at the forefront of international efforts to guide policy makers in the area of digital security since 1990, long before the Internet became mainstream. With the adoption over time of a set of digital security policy Recommendations[1], the OECD has become the primary international standard setter in this area. Based on in-depth analysis, these Recommendations reflect the good practice on how to develop digital security public policies for economic and social prosperity, in line with the OECD's mandate to help governments develop "better policies for better lives".

Further introduced below, these digital security Recommendations are international legal instruments adopted by consensus by the OECD Council, the Organisation's overarching decision-making body. They are open to adherence by partner economies. While they are not legally binding, OECD Recommendations represent a political commitment to the principles they contain, as well as an expectation that Adherents will do their best to implement them.

Digital security Recommendations aim to guide policy makers to develop digital security strategies and policies that foster trust and resilience, and support digital transformation, competitiveness and growth, while protecting critical activities, human rights and fundamental values.

By the end of 2022, this set of OECD digital security Recommendations will include seven Recommendations developed and updated over time since 1992. These Recommendations are likely to continue to evolve. More may also be developed in the future to cover additional aspects of digital security policy making.

High-level public policy makers and non-governmental stakeholders are too often unaware of these OECD digital security Recommendations, and therefore many are missing the opportunity to benefit from the guidance they contain. Digital security, namely *the economic and social policy dimension of cybersecurity*, is a relatively recent policy area, often overshadowed by national and international security ("cyberdefense", "cyberwarfare", "cyberespionage"), technical ("information security"), as well as criminal law enforcement ("cybercrime") dimensions of this issue (cf. 1.1. What is digital security?). Furthermore, the growing number of OECD legal instruments in this area can also increase the difficulty to grasp the overarching OECD digital security approach.

The OECD Policy Framework on Digital Security ("Framework") has been prepared by the OECD Secretariat to provide a coherent narrative based upon OECD digital security Recommendations and identifies linkages with other policy areas addressed through existing OECD standards and tools.

This Framework aims to help policy makers understand the economic and social dimension of cybersecurity, raise their awareness about the OECD approach to digital security policy, and encourage them to make use of OECD digital security Recommendations to develop better policies. It also aims to encourage interested partner economies to join the international dialogue taking place at the OECD in this area and align their policies with these Recommendations. All the OECD Recommendations covered by the Framework have been developed through a multi-stakeholder process, with the active participation of the business, civil society, and technical communities. Therefore, the Framework is also a tool to facilitate multi-stakeholder dialogue at the domestic and international levels.

As a communication tool targeted at policy makers, the Framework does not intend to provide a detailed and exhaustive description of each OECD digital security Recommendation. It rather selects a few key aspects of each Recommendation and presents them in a manner that is easily accessible for non-experts. It is also different from technical digital security standards, such as those developed by the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), European Telecommunications Standards Institute (ETSI) and other international standards development organisations, as well as from domestic or regional technical risk management frameworks such as the United States National Institute of Standards and Technologies (NIST) Cybersecurity Framework (NIST, 2018[3]). Nevertheless, OECD digital security Recommendations introduced in this Framework are meant to be consistent with and informed by these technical standards, thereby bridging the technical and policy levels. The difference in audiences and purposes may explain in part why the Framework's terminology may not always be aligned with technical standards, which sometimes also are not always consistent among themselves.

Content of the Framework

The Framework introduces the OECD Recommendations on:

- Digital Security Risk Management ("Digital Security Recommendation") (OECD, 2022[4]);
- National Digital Security Strategies ("Strategies Recommendation") (OECD, 2022[5]);
- Digital Security of Critical Activities ("Critical Activities Recommendation") (OECD, 2019[6]);
- Digital Security of Products and Services ("Products and Services Recommendation") (OECD, 2022[7]);

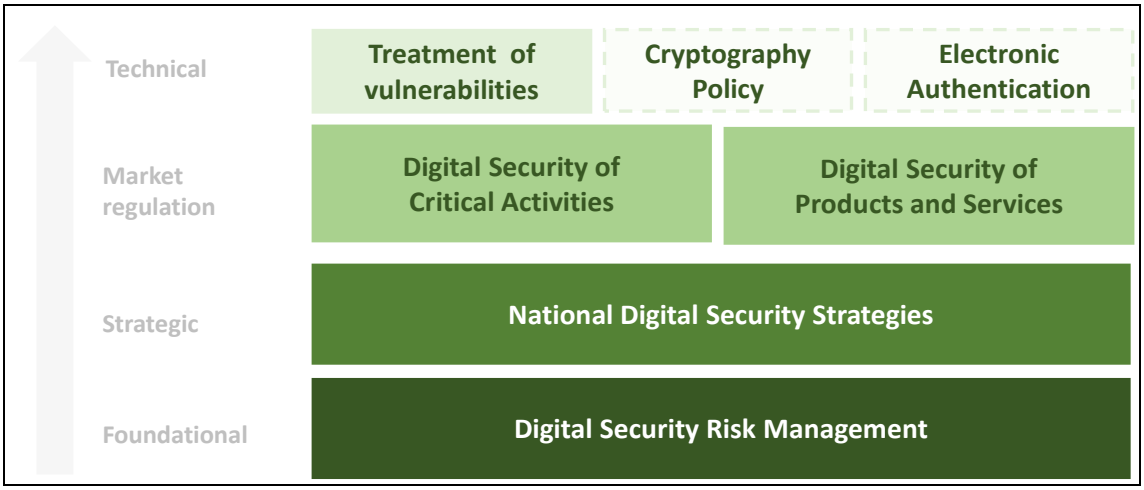
- The Treatment of Digital Security Vulnerabilities ("Vulnerabilities Recommendation") (OECD, 2022[8]);

A future version of the Framework will also cover the Recommendation on Electronic Authentication ("e-Authentication Recommendation") (OECD, 2007[9]) and Recommendation Concerning Guidelines for Cryptography Policy ("Cryptography Policy Guidelines") (OECD, 1997[10]).

The Framework aims to be used as a starting point to discover these Recommendations and facilitate their dissemination. Therefore, it is purposely short, and highlights only a fraction of the substance included in these Recommendations. Readers are encouraged to explore the Recommendations as well as related OECD analytical material.[2]

The Framework is made of building blocks focusing on specific policy issues, each addressed in one OECD Recommendation. These building blocks are organised in four layers, as illustrated in Figure 1.

Figure 1. Overview of the Framework



Note: Cryptography policy and Electronic authentication will be addressed in the next version of the Framework.
Source: OECD

- The *Foundational* layer is the basis of digital security policy making upon which all the other layers rely, namely digital security risk management. It includes the fundamental principles to bear in mind in order to approach cybersecurity from the economic and social perspective, and to establish a *culture of digital security to protect activities, people and the society without inhibiting benefits, opportunities, and human rights*. It is introduced in 1.2 below and reflects the *Digital Security Recommendation*. All the other layers of this Framework are based upon these high-level principles.
- The *Strategic* layer focuses on how policy makers should use the foundation to develop national digital security strategies that provide a clear vision to ensure that all stakeholders, from government agencies to public and private sector organisations and individuals, join forces in a coherent and consistent manner. It is introduced below in Chapter 2 and reflects the *Strategies Recommendation*. In addition to enabling a holistic and whole-of-government approach for digital security policy, national digital security strategies facilitate the creation of interfaces and synergies with other policy areas, such as digital economy policy, privacy and data protection, sectoral policies (e.g. finance, energy, education, skills) and international co-operation.

- The *Market regulation* layer addresses areas where policy intervention is needed because market forces are insufficient to create an optimal level of digital security. While many markets may require policy intervention to enhance digital security across society, so far OECD Recommendations have primarily focused on the following two areas:
  - The digital security of critical activities such as financial, health or energy services, the disruption or destruction of which would affect the functioning of the economy and society, human lives, as well as national security. The *Critical Activities Recommendation*, introduced in Chapter 3, focuses on the regulation of operators of such critical activities with a view to ensure that they align their level of digital security with the level of risk that is deemed acceptable by the society rather than by themselves only.
  - The digital security of the products that contain (computer) code and associated services (e.g. cloud) on which all stakeholders' depend to carry out their economic and social activities. OECD work showed that market forces alone are often insufficient to ensure that such products and services are sufficiently secure, and that market incentives on their own are unlikely to fix gaps in the digital security of these products and services. The *Products and Services Recommendation*, introduced below in 3.2, focuses on policies to address such market failures.
- The *Technical layer* focuses on more technical aspects that require policy guidance. It includes the need to encourage stakeholders to co-ordinate the disclosure of security vulnerabilities in products, better manage vulnerabilities in information systems, and protect vulnerability researchers. The *Vulnerabilities Recommendation*, introduced in Chapter 4, covers this area. *Cryptography policy* and *electronic authentication* will be addressed in a future version of the Framework, covering the 1997 *Cryptography Policy Guidelines* and the 2007 *E-Authentication Recommendation* (OECD, 1997[10]) (OECD, 2007[9]).

Digital security is a broad and growing policy space and the Framework only covers areas where Recommendations have been adopted by the OECD. Therefore, while it does not intend to be exhaustive, the Framework is open to extension and evolution, including as existing OECD standards may need to be reviewed in light of new developments. Furthermore, in the future, new technologies or technical challenges may require specific digital security policy guidance, adding building blocks to the top layer. Policy standards may also be needed to address challenges in specific markets (e.g. job market, sectors such as energy, health or insurance) or affecting categories of stakeholders (e.g. SMEs). The Recommendation on national digital security strategies provides a more comprehensive overview of these policy areas, many of which are not yet covered by OECD Recommendations at this stage.

There are many linkages between the various building blocks covered by the Framework, in addition to those already mentioned. For example, the digital security of products and services depends in part upon the extent to which stakeholders effectively treat digital security vulnerabilities; the protection of critical activities requires products and services to be sufficiently secure; and many technical security measures in products or critical activities rely on effective cryptography and electronic authentication. Mapping all possible linkages would extend beyond the scope of this document.

The Framework in a broader policy context

Digital security is a means to achieve economic and social objectives rather than an end it itself. Therefore it is important to design and implement digital security policies that are consistent with those developed in other related policy areas. When designed and/or implemented in isolation, digital security policies are likely to be inconsistent with other policy areas, and to be perceived as burdensome, costly, and

counterproductive. When they aim at creating synergies with other policy areas' objectives, digital security policies are likely to be more effective. The *National Strategies Recommendation* provides more details about how to develop whole-of-government digital security policies.

This section highlights the main linkages between the Framework and policy areas where the OECD has developed other Recommendations and tools. It aims to help policy makers use existing OECD standards as a compass to navigate the broader policy context for digital security policy making, while recognising that the scope of this document does not allow for mapping all the possible relationships between the Framework and every policy area. The Framework interfaces with OECD Recommendations and tools directly related to digital technologies, such as the OECD:

- **Going Digital Integrated Policy Framework** ("Going Digital Framework") (OECD, 2020[11]), which brings together the policy dimensions that are needed to make digital transformation work for growth and well-being, namely access, use, innovation, jobs, society, trust, market openness, and strategy. More specifically, digital security is a key component of the trust dimension of the Going Digital Framework, together with for example consumer and privacy protection.
- **OECD Recommendation Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines")** (OECD, 2013[12]). Digital security provides a robust foundation for the implementation of the Privacy Guidelines' Security Safeguards Principle which states that "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data". Digital security helps ensure that security measures are appropriate to and commensurate with the risk, which is an effective approach to defining "reasonable" security measures. However, digital security could undermine privacy, for example through measures if appropriate safeguards are not taken to protect personal data, such as when monitoring networks, or sharing risk-related information with third parties.[3]
- **OECD Recommendation on Consumer Protection in E-commerce** (OECD, 2016[13]), which recommends that businesses manage digital security risk and implement security measures for reducing adverse effects relating to consumer participation in e-commerce. It also includes provisions related to security measures for payment mechanisms.
- **OECD Recommendation on Broadband Connectivity** ("Broadband Recommendation") (OECD, 2021[14]), which provides a policy and regulation roadmap to unleash the full potential of connectivity for the digital transformation and to ensure equal access for all users. The Broadband Recommendation is structured around five key pillars including the need for governments to take "measures to ensure resilient, reliable, secure and high-capacity networks".
- **OECD Recommendation on Artificial intelligence** (AI) (OECD, 2019[15]), which promotes artificial intelligence that is innovative and trustworthy and that respects human rights and democratic values. Its principle on "robustness, security and safety" calls AI actors to "apply a systematic risk management approach to each phase of the AI system lifecycle on a continuous basis to address risks related to AI systems, including privacy, digital security, safety and bias".
- **OECD Recommendation on Children in the Digital Environment** (OECD, 2021[16]), which aims to help countries to find a balance between protecting children from online risks, and promoting the opportunities and benefits that the digital world provides. It sets out principles for promoting a safe and beneficial digital environment for children, recommendations on overarching policy frameworks, and highlights the importance of international co-operation.

Parts of the Framework which focus on risk management are consistent with the:

- **OECD Guidelines for Multinational Enterprises** (OECD, 2011[17]) ("MNE Guidelines")[4], which reflect the expectation from governments to businesses on how to act responsibly. The MNE Guidelines are the most comprehensive international standard on responsible business conduct

(RBC). They cover all key areas of business responsibility, such as human rights, labour rights, bribery, consumer interests, science and technology, and taxation. The MNE Guidelines recommend that businesses carry out risk-based due diligence to avoid and address adverse impacts associated with their operations, their supply chains and other business relationships. The Due Diligence Guidance for Responsible Business Conduct (OECD, 2018[18])[5] provides practical support to enterprises on the implementation of the MNE Guidelines by providing plain language explanations of its due diligence recommendations and associated provision support.

- **OECD Recommendation on Principles of Corporate Governance** (OECD, 2015[19]), also known as the G20/OECD Principles of Corporate Governance, which are intended to help policymakers evaluate and improve the legal, regulatory, and institutional framework for corporate governance, with a view to support economic efficiency, sustainable growth and financial stability (OECD, 2015[20]) (cf. 1.2 below).

As digital technologies are transforming almost all sectors of the economy, digital security risk is becoming a concern for policy makers in a growing number of areas and other sectoral issues, which are not inherently related to digital technologies and not specifically addressed in OECD standards, including for example insurance or SME policy.

Lastly, OECD digital security Recommendations are part of a broader set of high-level OECD standards focusing on digital economy policy, which all re-iterate the key role of digital security to promote trust in an increasingly digital world. They include the 2016 *Declaration on the Digital Economy: Innovation, Growth and Social Prosperity* (Cancún Declaration) (OECD, 2016[21]), the 2011 *OECD Recommendation on Principles for Internet Policy Making* (OECD, 2011[22]), as well as the 2008 *OECD Declaration for the Future of the Internet Economy* (Seoul Declaration) (OECD, 2008[23]).

1. Foundational level: cybersecurity for prosperity

This Chapter introduces key concepts that define digital security from the OECD perspective and help distinguish it from related but different areas (1.1), and introduces the digital security risk management principles of the *Digital Security Recommendation* (1.2).

1.1. What is digital security?

Digital security is the set of measures taken to *manage digital security risk* for economic and social prosperity. From a public policy perspective, it may be useful to approach digital security as a specific dimension of cybersecurity, prior to defining it more precisely.

Digital security as the economic and social dimension of cybersecurity

From an international and public policy perspective, cybersecurity can be viewed as a broad and multifaceted challenge aiming at supporting:

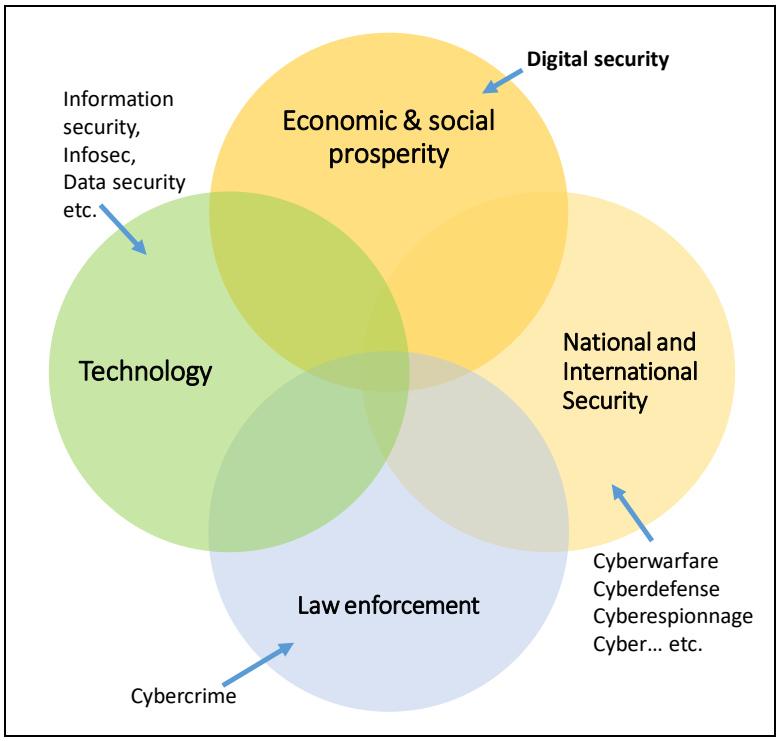
- *Technical operations*, i.e. ensuring that information systems work as expected. This is how cybersecurity started historically, namely as a technical issue for technical experts who often call it *computer security*, *information security*, *infosec, data security*, etc.
- *Prosperity*, i.e. ensuring that security serves economic and social (rather than only technical) objectives. This dimension focuses on the risk to the economic and social activities that rely on digital environment rather than on the security of the digital environment itself. The OECD calls this dimension *digital security* or *digital security risk management*.
- *Criminal law enforcement*, i.e. enforcing *cybercrime* laws to reduce threats. Cybercrime may, however, include other aspects than those introduced below, such as the exploitation of children online.
- *National and international security*, i.e. establishing confidence building and other measures to prevent and de-escalate the extension of armed conflicts in cyberspace. This dimension is often related to *cyberdefense*, *cyberwarfare*, or *cyberespionage*.

These objectives or dimensions of cybersecurity overlap to a certain extent and therefore are interrelated, as illustrated in Figure 2.

Governments have adopted various institutional frameworks to develop and implement policy issues related to each of these dimensions, leveraging different domestic agencies, with variable degrees of centralisation and co-ordination with other government bodies. At the international level, each dimension is generally addressed by different international organisations, in line with their respective mandate. For example, the OECD addresses digital security policy in line with its economic and social mandate to develop “better policies for better lives”; standards development organisations such as ISO/IEC, IETF,

ETSI, or ITU-T Study Group 17 develop technical standards; the Council of Europe, the United Nations Office of Drugs and Crime (UNODC) and Interpol (at a more operational level), focus on cybercrime; and the United Nations Group of Governmental Experts (GGE) and Open Ended Working Group (OEWG) address international security issues.

Figure 2. Digital security, the economic and social aspect of cybersecurity



Source: OECD

Digital Security Fundamentals

Digital security risk is the detrimental effect[6] that digital security *incidents* can have on economic and social activities. As all other risks, digital security risk is represented in terms of the *likelihood* and potential *impact* (i.e. severity) of incidents.[7] The definition of risk in OECD digital security Recommendations is inspired by ISO/IEC risk management and information security standards.[8] Importantly, the goal of digital security is to support prosperity. Enhancing digital security is not an end in itself.

Digital security incidents are events that disrupt the availability, integrity and/or confidentiality (*AIC triad*) of data, software, hardware and networks and, as a consequence, negatively affect the economic and social activities that rely on these assets:

- *Availability*: assets are not accessible and usable on demand by authorised users;
- *Integrity*: assets have been altered in an unauthorised manner;
- *Confidentiality*: unauthorised entities have access to the assets.

Incidents are caused by *threats* exploiting *vulnerabilities*. Threats can be intentional (i.e. attacks) or unintentional (e.g. human errors, fires, power cuts, etc.). They include malicious actors ("threat sources") willing to exploit vulnerabilities to cause harm, and the tools and techniques ("threat vectors") they use to

carry out attacks (e.g. “malware”). Malicious actors range from relatively unskilled individuals to organised criminal groups and State-sponsored actors, with considerable resources, often called Advanced Persistent Threats (APTs). State-sponsored attacks are generally pursuing geopolitical goals, and cybercriminals financial gains. Some actors also pursue ideological objectives (e.g. “hacktivists”). In many cases, it can be extremely difficult to accurately attribute attacks to specific individuals, groups or their sponsors, solely on the basis of their mode of operation or forensic evidence, in part because well-resourced threat actors can mimic other threat actors’ modes of operation. Threats exploit *vulnerabilities* in people (e.g. lack of training and awareness), processes (e.g. no backup procedures or systematic vulnerability management) and technologies (e.g. vulnerabilities in software code).

For the OECD, digital security risk is the *economic and social* rather than *technical* risk resulting from incidents. They are related but not the same. The economic and social risk results from the technical risk. The technical risk is limited to possible breaches of the AIC triad and ICT-related aspects, such as system failures, downtime, unauthorised access, loss of digital assets, etc. In contrast, the economic and social consequences of such breaches may include financial losses, loss of opportunity, reputational damages, intellectual property theft, privacy and human safety damages. For example, when a ransomware hits a hospital and spreads across the network, some infected information systems may become unavailable and others have to be shut down to mitigate the incident (technical risk). As a result, patients being operated during the incident may be in danger because medical equipment may be disabled, scheduled surgeries may have to be postponed (economic and social risk), and personal data may be breached. According to a 2021 survey by the research firm Ponemon, 22% of IT and IT security professionals in healthcare delivery organisations agreed that a ransomware attack increases mortality rate.[9]

Digital security risk management is what people and organisations do to address digital security risk while maximising economic and social opportunities. Risk management is the assessment of the risk, followed by its treatment, i.e. a decision on what to do with the risk: reduce, avoid, transfer or take it (further introduced below in 1.2). We manage risk all the time, we just don’t realise it. For example, if we want to cross a street, we watch for cars or bicycles to *assess* the risk before deciding what to do. If it is a highway, we don’t cross it to *avoid* the risk which his too high. To *reduce* risk we use pedestrian crossings, and we have an insurance policy to *transfer* the risk, “just in case”. If we simply cross the street without assessing the risk, for example while walking and multi-tasking on a smartphone, we simply *accept* the risk, and will have to face the consequences. *Risk assessment is absolutely central for security*, including digital security. While accepting the risk after a careful and systematic risk assessment is perfectly fine, blindly accepting it without a risk assessment is not responsible.

Digital security risk management roots security decisions in the economic and social reality of the activity at stake. It drives the selection of security measures which are appropriate to, and commensurate with, the risk and activity at stake. In so doing, *it ensures that the security measures will support the economic and social activities at stake, and will not undermine them*, for example, by inappropriately closing the environment or reducing functionality in a manner that would limit the possibility of taking advantage of ICTs to innovate and increase productivity. Digital security risk management prevents decisions from being made in isolation, from a separate technical or sole security point of view (security as an end in itself).

Digital security risk is a sub-category of digital risk, which itself is one among many other risks that a person or organisation may face when using digital technologies. All risks are interrelated and therefore risk management should not be approached in silo. Other digital risks include anything else that can go wrong in the digital environment, from mis- and disinformation, to fraud (e.g. business email compromise), to the exploitation of children online, etc. While there may be intersections between digital security risk and other digital risks, it is important to avoid confusion and not conflate these distinct categories, in particular when addressing digital security risk at the international level.

1.2. Digital security risk management principles

This section introduces the nine interrelated high-level principles that form the basis of an effective economic and social approach to cybersecurity and are included in the OECD *Digital Security Recommendation*. All other OECD digital security Recommendations are based upon them.

These principles are at the core of a *culture of digital security* for public policy makers as well as leaders and decision makers in public and private organisations, who pursue the same goals: protecting activities that rely on the digital environment from cyber threats *i)* without inhibiting these activities, hindering innovation, impeding digital transformation, and undermining human rights; and *ii)* while taking into account the dynamic nature of technologies, economic activities that rely on them, as well as the threat landscape. The principles may also be useful for individuals, although they usually have a limited ability to act.

The general principles briefly introduced below address all stakeholders, the operational principles address leaders and decision makers in organisations. The italic text in the boxes is a short extract from the *Digital Security Recommendation*, which contains more details.[10]

General principles

1. Digital Security Culture: Awareness, skills and empowerment	*All stakeholders should create a culture of digital security based on the understanding of digital security risk and how to manage it.*
2. Responsibility and liability	*All stakeholders should take responsibility for the management of digital security risk based on their roles, the context and their ability to act.*
3. Human rights and fundamental values	*All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.*
4. Co-operation	*All stakeholders should co-operate, including across borders.*

A culture of digital security is essential to manage digital security risk (Principe 1). It is the mind-set with which stakeholders should approach digital security, whether to develop and implement public policy, or protect their organisation (business, government agency, NGO), personal assets, and safety without inhibiting benefits, opportunities, and human rights.

First, **it is essential to understand that such risk exists, and to acquire appropriate skills** – through education, training, experience or practice – to make responsible decisions (empowerment). While the possible consequences of a car crash are intuitive, the complexity of the digital environment blurs the link between an incident and its consequences. For example, many people are aware that a virus may infect their equipment, but do not understand the potential consequences such as identity theft, financial fraud or theft of trade secret. Consequences to others are even less visible, such as when an infected machine becomes part of a botnet used to launch denial of service attacks to third parties. Thus digital security awareness raising should focus on the possible economic and social consequences (i.e. risk) of incidents, rather than only on risk factors such as threats and vulnerabilities.

It is a fundamental principle of our social life that one should face the consequences of their actions, including on others. Therefore, **we all share responsibility for our digital security decisions**, or the lack thereof (Principle 2). However the nature and levels of responsibility vary according to stakeholders' *role.* For example, the responsibility of the user of a digital device is different from the responsibility of that device's vendor, manufacturer, third-party developers of software components embedded in the device, cloud providers hosting data processed by the device, etc. The *context* is also important. For example, the

responsibility of designers, vendors or users of software or devices is different if the product is used in an entertainment (e.g. gaming), medical (e.g. to check insulin levels) or other critical contexts (e.g. connected valve on a pipeline). Lastly, stakeholders' *ability to act* needs to be taken into account. For example, average consumers cannot use products responsibly if these products do not embed basic user-friendly security features (e.g. multi-factor authentication) and security configuration settings (e.g. automatic updates). Users have no ability to address vulnerabilities affecting a product during its design phase. The ability to act of specific groups such as vulnerable consumers (e.g. children, elders, disabled, disadvantaged persons) or organisations with limited resources (e.g. small and medium-size enterprises, local governments, NGOs, hospitals, etc.) needs to be taken into account when considering responsibility and liability. Responsibility with respect to others is at the core of the OECD risk-based due diligence recommendations contained in the OECD MNE Guidelines[11] (OECD, 2011[24]) and OECD Due Diligence Guidance for Responsible Business Conduct (OECD, 2018[18]). Although it does not address digital security specifically, the latter can be used as a helpful resource for high-level best practice on how stakeholders can conduct risk-based due diligence, including specific guidance on stakeholder engagement and reporting on their risk assessment and risk mitigation efforts.

The rights that apply "off-line" should also apply online. Therefore, **human rights and fundamental values need to be protected in the digital environment** (Principle 3). Depending on how they are used, security measures can *support or undermine* human rights and fundamental values. For example, some security measures can enhance privacy protection, provide anonymity to whistle-blowers and protect human rights activists from authoritarian surveillance. They can also enable the illegitimate surveillance of citizens or employees, or prevent access to activists' content. A responsible digital security approach requires that decisions to manage digital security risk be made in light of their consequences on these rights and values.

While the global interconnectedness of the digital environment enables considerable economic and social benefits, it also increases complexity, facilitates propagation of threats and vulnerabilities, and increases collective risk. **Co-operation is essential at the domestic and cross-border levels** to address these drawbacks (Principle 4). Isolated stakeholders cannot successfully address digital security. For example, organisations' leaders and decision makers need to cooperate with technical experts to assess digital security risk, and technical experts need to co-operate with leaders to ensure that technical security measures do not undermine their organisation's objectives and activities. Co-operation is also needed within and across organisations, for example to share information about the spread of threats and vulnerabilities both within an organisation and among its partners, along supply chains, or within the government, between organisations in the same economic sector, including competitors (e.g. through Information Sharing and Analysis Centres – ISACs), between the public and private sectors, organisations and their consumers, users and, more generally, the civil society. Similarly, public policy making and implementation are more effective when informed by business, technical and civil society experts.

Operational principles

Operational principles focus on the implementation of digital security risk management in organisations. They are based on the digital security fundamentals introduced in 1.1.

5. Strategy and governance	*Leaders and decision makers should ensure that digital security risk is integrated in their overall risk management strategy, and managed as a strategic risk requiring operational measures.*
6. Risk assessment and treatment	*Leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment.*
7. Security measures	*Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.*

8. Innovation	*Leaders and decision makers should ensure that innovation is considered.*
9. Resilience, preparedness & continuity	*Leaders and decision makers should ensure that a preparedness and continuity plan based on digital security risk assessment is adopted, implemented and tested, to ensure resilience.*

The first step to manage digital security risk in organisations is the adoption of a **strategic approach and the establishment of appropriate governance** (Principle 5). Integrating digital security risk management in the organisation's overall risk management framework (often called "enterprise risk management") is essential to ensure that digital security decisions are driven by business objectives rather than only technical considerations, and follow established risk management good practice (e.g. systematic approach, continuous improvement cycle, etc). The corporate board of directors has a clear role in the management of digital security risk, in line with the *G20/OECD Principles for Corporate Governance* chapter on boards which underlines that a key function of the board is to set risk management policies and to ensure "the integrity of the corporation's accounting and financial reporting systems, including […] that appropriate systems of control are in place, in particular, systems for risk management […]" (Principle VI.D.7) (OECD, 2015[20]).

Digital security governance should set clear roles, responsibilities and processes, and ensure that appropriate resources and competences are available. *Leaders and decision makers responsible for achieving economic and social objectives should be responsible for digital security risk to these activities* ("risk ownership"). Risks and benefits are inherently related, because by definition risks affect benefits of an activity. As managing risk is a means to increase an activity's likelihood of success, those individuals in an organisation who are responsible for an activity's benefits should also be responsible for addressing the digital security risk to that activity. They should work in co-operation with security experts who own the technical security risk and help understand how it can affect the economic risk, and how both risks may be reduced through technical measures, among others. In large organisations, security experts may be organised under a technical committee, which may also include other experts (e.g. legal, communication, etc.). However, leaders and decision makers should not simply delegate to technical experts the responsibility to manage digital security risk. Management of digital security risk and related decision making require a holistic view of the activity being carried out and the consequences it may have on stakeholders at large. While effective and regular communication between the leadership (e.g. CEO and board in the private sector) and the technical IT security experts is key, risk management should be a business (as opposed to only technical) decision making process because:

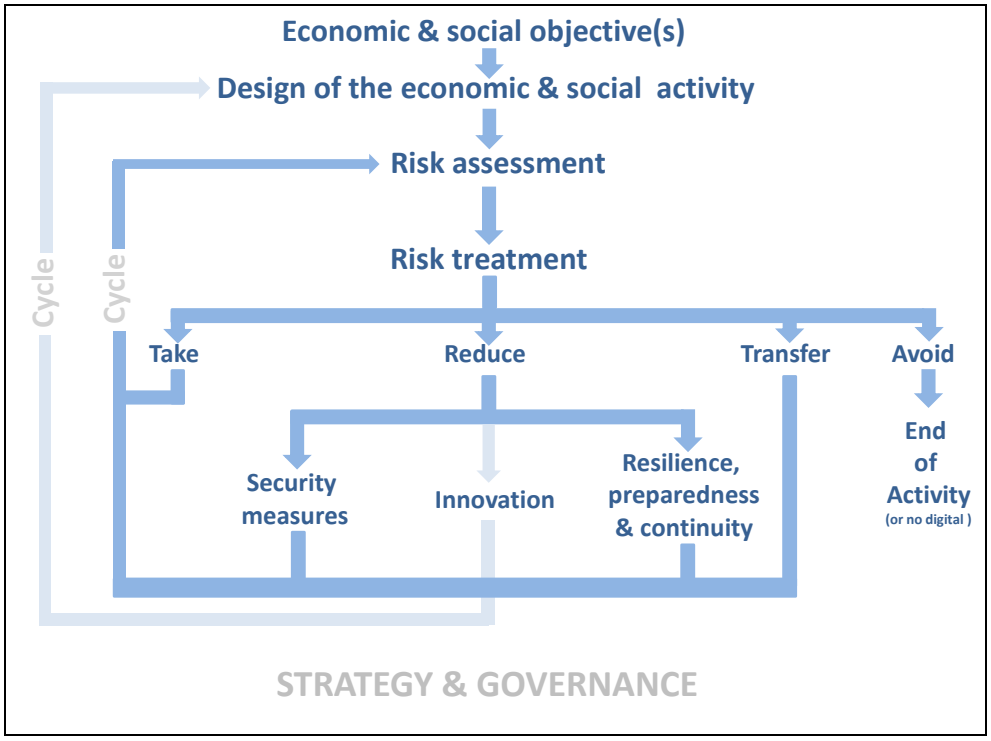
- *The economic and social consequences of incidents can be much more severe than their technical (i.e. ICT) impact* for the organisation, its partners and third parties. For a hospital, patients can die because of ransomware-encrypted hard drives. For a company, multi-year R&D investments can be lost if a competitor successfully accesses intellectual property prior to patents being registered. The technical cost is generally far below these investments and lost opportunities.
- *Security measures can undermine the activity they aim to protect*. They can create barriers and constraints for this activity, such as increased financial cost, system complexity and time to market, reduced performance, usability, capacity to evolve, innovation, and user convenience. They can also generate privacy threats and other adverse social consequences. These constraints and adverse effects can often be addressed and mitigated, but at a cost.

Every activity is exposed to uncertainties that can reduce its chances of success. To increase the likelihood of success, a **risk assessment and treatment cycle** (Principle 6) addresses such uncertainties. As shown in Figure 3, it starts with the definition of the objectives and design of the activities that rely on the digital environment. The risk is then assessed to evaluate the probability and possible effects of uncertainties on

the objectives of the activity. On the basis of this assessment process, a decision is made on what to do with the risk (risk *treatment*), i.e. whether and how the risk should be modified to increase the likelihood of the success of the activities to support and preserve the objectives. The risk treatment process determines which part of the risk should be:

- **Taken** (i.e. accepted), because the risk is below the level that is deemed acceptable by the entity carrying out the activity, also known as its "risk appetite" or "risk tolerance". Taking the risk means accepting the potential detrimental economic and social consequences of incidents.
- **Avoided**, knowing that it is not possible to eliminate the digital security risk entirely without at the same time giving up the benefits of using ICTs. In other words, the best way to avoid digital security risk is to not use digital technologies.
- **Reduced** to the acceptable level according to the entity's risk appetite, by establishing security measures that prevent the occurrence of incidents. However, some detrimental events can always happen, despite all the security measures in place. It is impossible to create a fully safe and secure digital environment. There will always be some "residual risk" that cannot be eliminated and must be accepted. Therefore, it is essential to create resilience and ensure business continuity, to always be prepared for incidents and ready to reduce their consequences.
- **Transferred** to a third-party, for example through insurance, if there is an insurance market.

Figure 3. Overview of the digital security risk management cycle



Source: OECD

Continuous, systematic and cyclical risk assessment is essential for leaders and decision makers to make informed risk treatment decisions that are tailored to the constantly changing risk, as threats, vulnerabilities, incidents, technologies, their uses, and their benefits – to name a few variables in the risk equation of an activity – are extremely dynamic. The risk assessment needs to take into account risk

related to suppliers, and partners with whom the organisation is digitally connected. The possible risk treatment decisions (take, reduce, transfer, avoid) require that leaders and decision makers set their organisation's digital security level of risk appetite (or tolerance) for each activity that relies on the digital environment.

To reduce the risk, **security measures** can then be selected and operated (Principle 7). Security measures, also called "mechanisms", "controls", or "safeguards", can be of different natures: digital (e.g. security software), physical (e.g. locks, cameras, fences) or mixed (e.g. smart card); related to people (e.g. training), processes (e.g. organisational rule or practice) or technologies (e.g. cryptography), legal (e.g. contract), procedural (e.g. standards), managerial, etc. Security measures may also address vulnerabilities, as addressed in the *Vulnerabilities Recommendation* (cf. Chapter 4).

In addition to adopting security measures, stakeholders can reduce their exposure to digital security risk by **innovating** with respect to the activity as well as the security measures (Principle 8). Innovation to reduce digital security risk can take many forms, which may or may not be related to digital aspects. For example, innovation may relate to the organisation's economic or business model, to processes such as payment methods, or even to redesigning physical, legal or other non-digital components of a product. As introducing innovation itself can create uncertainties in an activity, it should trigger a reassessment and treatment cycle, as shown in Figure 3. Thus *digital security can add value to an organisation, product or service, and become a driver for innovation, a stimulus for competitive advantage,* provided that it is approached as an integral part of the economic and social decision making processes related to an activity rather than as an isolated and only technical issue.

To further reduce risk, **resilience, preparedness and continuity measures** can be defined in order to be applied when an incident happens (Principle 9). In addition to security measures and innovation, which aim to prevent the occurrence of harmful incidents, resilience, preparedness and continuity measures aim to *mitigate economic and social consequences when incidents do occur*. Preparedness and continuity plans are essential to define in advance how to protect, detect, respond, and recover from incidents. Such plans should take into account the extremely rapid pace with which incidents can propagate and escalate in the digital environment.

2. Strategic level: creating a culture of digital security

Digital security policy making is a multifaceted area, which requires a strategic approach based on a clear vision to ensure that all stakeholders, from government agencies to public and private sector organisations and individuals, join forces in a coherent and consistent manner. The *National Strategies Recommendation* provides high-level guidance to achieve this goal and create a culture of digital security throughout the economy and society.

2.1. Objectives and institutional framework

National digital security strategies ("national strategies") should articulate a clear vision of the country's objectives with respect to digital security. They should aim to create a culture of digital security and protect individuals as well as public and private organisations from digital security threats while taking into account the need to safeguard national and international security and to preserve human rights and fundamental values. National strategies should create the conditions for all stakeholders to manage digital security risk, foster trust and confidence in the digital environment, strengthen security and resilience, and facilitate digital transformation. They should also aim to strengthen the digital security of critical activities, an area addressed in Chapter 3.

In addition to digital security, a national strategy may address several other dimensions of cybersecurity, which are beyond the mandate of the OECD (cf. 1.1 and Figure 2 above). Governments may refer to "cybersecurity" instead of "digital security", often because of these additional areas, or because the term cybersecurity has gained a high visibility in the general public, or because the country has a more (or less) specific definition of cybersecurity, different from that of the OECD. In fact, there is no consistency across countries on how to use this term, in particular at the international level. Nevertheless, regardless of their title, these national strategies should ensure consistency and complementarity between all the dimensions of cybersecurity.

The effectiveness of the institutional framework is essential for developing, implementing and reviewing the national strategy. It should consist of a mix of intra-governmental co-ordination and multi-stakeholder processes. Because the strategy needs to build upon a whole-of-government approach, it needs to be supported at the highest level (e.g. President, Prime Minister), to mitigate challenges arising from competing objectives and diverging priorities in different parts of the government.

Engaging with the business, technical, and civil society communities in the development and implementation of the strategy is particularly important and should not be viewed as a mere formality. On the contrary, it is a powerful tool to align the strategy and implementation policies with the economic, technical and social reality of the country, and to inform stakeholders of aspects of digital security challenges they may not be aware of. Furthermore, multi-stakeholder engagement can lay the foundations for trust-based partnerships (e.g. for information sharing), which are a key element of a national strategy.

The national strategy needs to assign clear responsibilities to one or more existing or new government bodies for the development and implementation of digital security policies called for by the strategy. Such body(ies) with core digital security responsibility should nevertheless co-ordinate with other agencies in areas such as criminal law enforcement, sectoral regulation, privacy and data protection, consumer protection, innovation, digital government, education, and foreign affairs.

In addition, the national strategy itself should be consistent and inform other national strategic efforts, such as skills, education, innovation, and industrial strategies. As noted above, depending on a country's size and style of government, collaboration with public bodies in charge of these other strategies may be a challenging task, as there may be institutional or cultural obstacles (OECD, 2018[25]). For instance, national security-focused bodies may not be used to transparently collaborate with ministries in charge with economic and social issues and with non-governmental stakeholders.

Recently, many countries have developed national *digital* strategies, i.e. comprehensive strategies that exclusively or primarily address digital policy issues across policy areas affected by or affecting digital transformation. These strategies often include digital security (Gierten and Lesher, 2022[26]) and their development provides an opportunity to identify potential synergies across the government and increase the whole-of-government dimension of digital security policy approaches. Challenges related to co-ordination among sectoral regulators are particularly acute with respect to digital security of critical activities, as explained in Chapter 3.

2.2. Content of the Strategy

The *National Strategies Recommendation* maps nine areas where national strategies should provide for policy measures, although additional areas may also be covered. The Recommendation does not recommend an order of priority among these areas. However, many governments have historically started with the first three: awareness raising, the establishment of incident response capacity (generally through one or more Computer Security Incident Response Teams (CSIRT) or Computer Emergency Response Teams (CERT)), as well as the promotion of risk management standards. As digital security becomes more mature in a country, these areas need to be complemented with further measures. To meet the job market needs, public policies should support the development and retention of a skilled workforce, for example by addressing digital security risk management in broader skills strategies. In addition to a response capacity, the establishment of vulnerability co-ordination mechanisms is also essential to support co-ordinated vulnerability disclosure, further discussed in Chapter 4. Furthermore, governments should encourage private actors to respond to cyberattacks in a responsible manner and discourage them from counterattacking (cf. Box 1).

Other areas include the development of a cybersecurity industry, as well as initiatives to encourage research and innovation (OECD, 2020[27]), and the protection of individuals and SMEs (OECD, 2021[28]). National strategies should also anticipate the growing digital security challenges affecting different sectors such as smart transports, energy or health, where different regulators may have a role, and stakeholders may express different needs and requirements. Sectoral ministries, departments and regulators often do not have yet the critical mass of expertise to approach digital security and lack the broader global risk awareness and technical competence that is often concentrated in a specialised cybersecurity agency. Therefore, effective co-ordination mechanisms as well as multi-stakeholder collaboration are instrumental to the success of such sectoral policies.

To implement the Co-operation principle of the *Digital Security Recommendation* (cf. 1.2 above), governments should create the conditions for all stakeholders to collaborate for digital security, in particular through trusted partnerships including to share risk-related information. Information Sharing and Analysis Centres (ISACs) provide one example of such multi-stakeholder partnerships. They are sometimes

initiated by the government, operated with or without its active participation, generally organised at sectoral level (e.g. financial sector, aviation, energy, etc.), and may have a national, regional or international scope (ENISA, 2018[29]; CISA, n.d.[30]; NCSC-NL, 2018[31]). Trust for co-operation among stakeholders is a recurring theme in OECD Digital Security Recommendations. It is for example addressed in the context of critical activities (cf. Box 3) and vulnerability treatment (Cf. 4.1). Last, but not least, international co-operation should be an important component of national strategies, for sharing experience and good practices, providing and benefiting from mutual assistance, improving incident response at operational level and developing comparable risk metrics.

To implement their national digital security strategy, governments should allocate sufficient resources and engage with other stakeholders. They should lead by example, including by adopting best digital security risk management practices to protect the government's own activities. Another avenue is to use public procurement to foster digital security risk management across the economy and society.

Digital security risk is extremely dynamic, with constantly evolving threats and vulnerabilities affecting technologies, products and services used in numerous innovative ways across the economy and society. In this moving landscape, national strategies provide goals and directions that need to remain valid for a sufficiently long period of time for stakeholders to co-ordinate their actions and progress in the same direction. However, national strategies should not be set in stone. Threat actors are well-known for their agility and adaptability, and digital security is particularly sensitive to international tensions and crises, which multiply in an increasingly uncertain world. Therefore, governments should adopt a cycle of improvement by regularly assessing, reviewing and improving their strategy and implementation policies.

Box 1. Encouraging responsible response and discouraging counter-attack ("hack back")

Over the last few years, experts have noticed a rise in the underground commercialisation of counter attack services to private actors, which can be used to deter malicious actors from attacking, damage their attack infrastructure, or simply "give them a lesson".

These practices, sometimes called "hack-back", are generally offered covertly to legitimate businesses, sometimes across borders. They are counter-effective and can significantly increase the risk of collateral damage to third-parties whose equipment is being used as a proxy by attackers to hide their tracks. Furthermore, these practices may also increase the likelihood of escalation and exacerbate international tensions. In some cases, victims may think they strike back against a cybercriminal when in reality they are dealing with a state-sponsored group with political or geopolitical goals, and quasi-unlimited resources.

According to the *National Strategies Recommendation*, governments should encourage private actors to respond to cyber attacks in a responsible manner, discourage them to carry out any form of counter attack, directly or through a private third-party, and discourage the provision or procurement of counter attack services by private actors.

3. Market level: strengthening security without inhibiting prosperity

There are cases where market forces alone do not allow for some stakeholders to optimally address digital security, and where public policies are needed to encourage them to strengthen digital security. This is particularly the case for critical activities and for products that include code and related services.

When they manage digital security risk, operators of critical activities such as energy, telecom or financial services providers, may aim at reducing the risk to the level they deem acceptable *to them*, according to *their* risk tolerance. However, their acceptable level of risk may not be aligned with that of the society as a whole. As they are responsible for activities that are critical to the functioning of the entire economy and society, the residual digital security risk these operators inevitably have to take (as explained in 1.1) is partly born by all other economic and social actors. The consequences of failure, in these cases, extend far beyond these operators and can be catastrophic for all. They can cross sectoral boundaries through cascading effects (e.g. a cyberattack on the electric grid creating a blackout that affects public transports and hospitals), and jurisdictional borders if the affected economic activity is itself subject to cross-border dependencies (e.g. cyberattacks paralysing systemic banks). Market forces alone are unlikely to address this issue. It is the governments' role and responsibility to ensure, through public policy, that the interests of the broader economy and society are taken into account in the way operators manage digital security risk.

Furthermore, most economic and social actors use products that contain code and associated services (e.g. cloud storage, processing, etc.) to carry out their economic and social activities. However, how can they manage digital security risk in a responsible manner if the products and services they use are not secure enough, i.e. do not embed appropriate security features, throughout their lifecycle, such as security updates? How can individuals and organisations make informed purchasing decision about products and services if the market does not provide them with enough information about their level of security? Here again, market forces do not seem to be sufficient to ensure that suppliers take responsibility according to their role (cf. Principle 2, in 1.2 above), and public policy can help improve this situation.

In these two areas, apparently very different in nature, operators of critical activities and suppliers of products and services are responsible to make risk treatment decisions that can affect others, a situation often referred to as a *moral hazard*: "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, 2009[32]). This layer of the Policy Framework covers OECD policy guidance addressing this moral hazard to enhance digital security without inhibiting prosperity, slowing down innovation and reducing the benefits from digital technologies.[12]

3.1. Digital security of critical activities

This Section provides a brief overview of the 2019 *Critical Activities Recommendation*. The Going Digital Toolkit Note on *Enhancing Digital Security of Critical Activities* provides more details and illustrations of public policies in this area (Bernat, 2021[33]).

Digital technologies have become so pervasive across value and supply chains that most economic and social activities are now digitally dependent, a dependency that the current digital transformation is increasing and accelerating. Among these activities, some are critical to the health, safety, and security of citizens; the effective functioning of essential services; or economic and social prosperity more broadly (cf. Box 2).

Box 2. What is a critical activity?

According to the OECD *Critical Activities Recommendation*, a critical activity is an economic and social activity, the interruption or disruption of which would have serious consequences on:

- The health, safety, and security of citizens (e.g. the provision of healthcare in hospitals, or emergency services); or
- The effective functioning of services essential to the economy and society (e.g. the provision of energy, financial services or transports), and of the government; or
- Economic and social prosperity more broadly.

The latter type of critical activities includes those that are essential for prosperity without being necessarily critical to the functioning of the economy and society, nor affecting the health, safety and security of citizens. For example, this would include car manufacturing or mining, in a country where such activities would represent a significant share of the GDP. Critical activities are sometimes called critical functions or essential services.

Over the last ten years, our economies and societies have become more and more digitally dependent, and critical activities have been increasingly exposed to digital security threats, which have grown in number and sophistication. This presses governments to shift gears and adopt innovative policies to strengthen the digital security of critical activities. However, strengthening digital security can introduce significant costs and other constraints on operators of critical activities. A key policy challenge is to ensure that policy measures *focus on what is critical* for the economy and society, *without imposing unneeded burdens* on the rest, and *without undermining the benefits* from digital transformation in critical sectors through constraints that would unnecessarily restrict the use and openness of digital technologies.

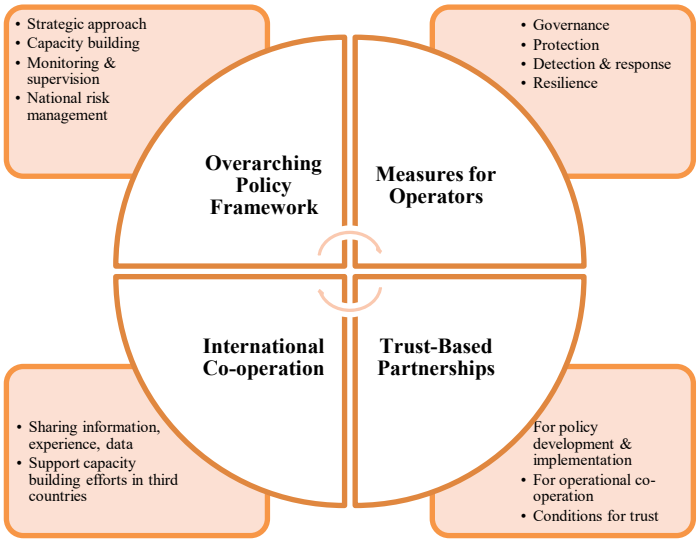
The protection of critical activities is not a new policy area. In 2008, the OECD adopted the *Recommendation on the protection of critical information infrastructure* (CIIP) (OECD, 2019[6]), which focused on public communication networks as well as information systems owned by operators of critical infrastructure such as banks and energy distributors. However, the CIIP Recommendation was replaced by the 2019 *Critical Activities Recommendation* to focus on the digital security risk to the critical economic and social services (critical activities) rather than to the information infrastructure on which the delivery of these services rely. In other words, the focus evolved from the technical to the economic and social risk, as introduced in 1.1.[13]

Policies to enhance the digital security of critical activities aim primarily at encouraging public and private operators of these activities ("operators") to better manage digital security risk. They include, for example, banks, hospitals, water and energy distributors, telecommunication network providers, airports, rail companies, etc.

Targeting too many operators that are not truly vital to the delivery of the critical activities at stake would impose unnecessary burdens on large parts of the economy. Targeting too few would not sufficiently protect the economy. To identify which operators should be in the scope of their policy, governments can build upon an existing critical infrastructure protection framework. In lack of such a framework, they need to develop a national risk assessment covering all economic and social activities, and work with relevant public and private actors, to identify critical activities and their most relevant operators on this basis.

As shown in Figure 4, the *Critical Activities Recommendation* provides guidance for policy makers on how to define what operators should do, set up the right institutional framework, establish trust-based partnership, and co-operate at international level.

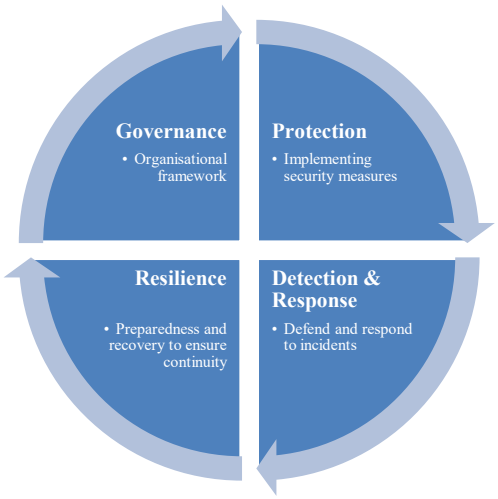
Figure 4. Content of the Critical Activities Recommendation



Source: OECD

To avoid creating unnecessary burden for operators, governments should focus their policies on the digital security of operators' critical functions, which are those processes without which operators could not effectively carry out critical activities. Governments can encourage or require that operators take governance, protection, detection and response, as well as resilience measures (cf. Figure 5). They can use many public policy tools, including promoting standards, creating legal obligations, regulating, co-regulating, encouraging self-regulation, providing assistance for crisis management and technical support, etc. The creation of trust-based partnerships, briefly introduced in Box 3, is one of the key elements of policies among those covered by the *Critical Activities Recommendation*.

Figure 5. Types of measures for operators



Source: OECD

Box 3. Promoting trust-based partnerships

The multiplicity of digital dependencies across sectors and borders and along critical activities' value chains create a shared digital security risk that no single actor can significantly reduce for all. Each actor is therefore dependent upon and responsible towards all others to manage digital security risk.

The establishment of sustainable public-public, public-private and private-private partnerships across sectors and borders, is an essential tool to ensure that the digital security of critical activities takes account of such dependencies. Such partnerships enable participants to share information, good practice and experience on risk and its management. They can also help improve public policies. However, trust among stakeholders is essential for such partnerships to emerge, in part because of the sensitivity of the information to be exchanged.

The *Critical Activities Recommendation* provides a list of conditions to establish trust. They include the need for clear aims, values and rules, mutual benefits over time, respect for personal data protection and other regulation protecting the confidentiality of information such as trade secrets. Furthermore, partners need to ensure that the information they exchange will only be used for defensive purposes.

3.2. Digital security of products and services

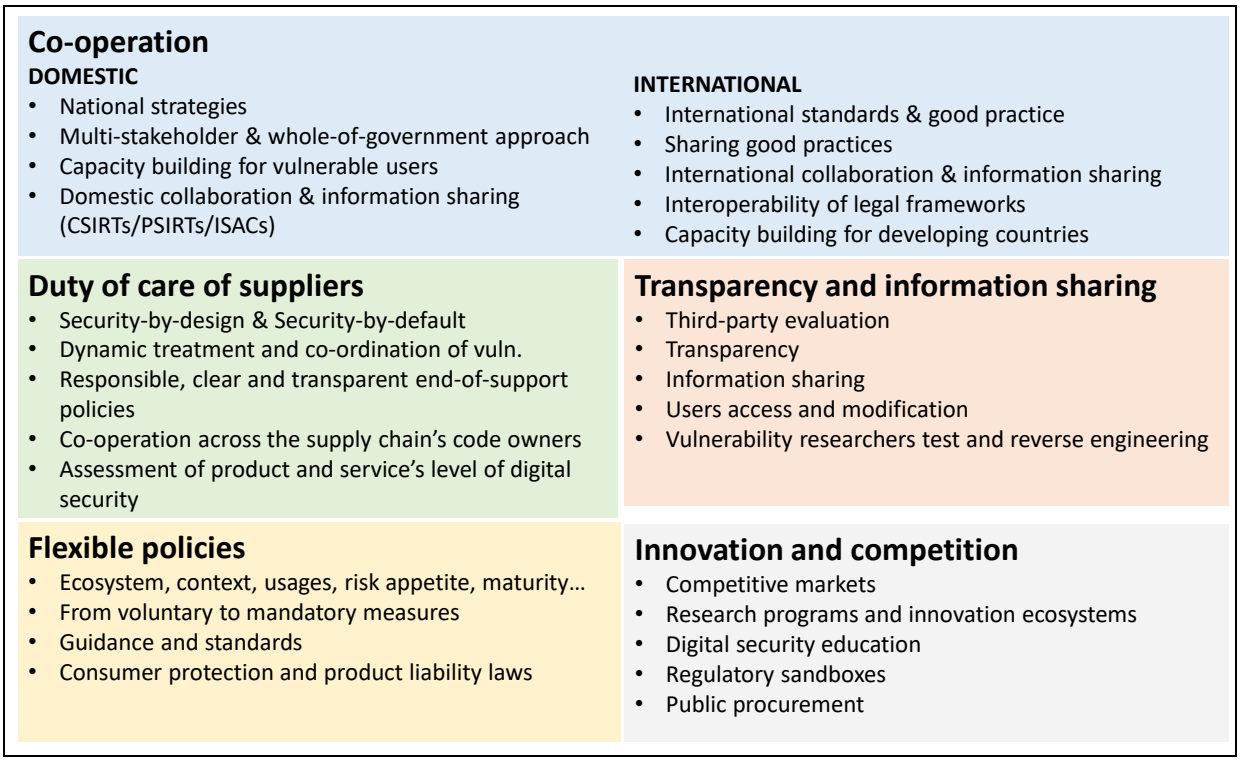
In an ideal world, market forces would ensure that products that include code (software, IoT devices, etc.) and related services are sufficiently secure, and that their security measures are proportionate to the risk faced by their users, hence increasing the marginal cost of cyberattacks for malicious actors and discouraging their efforts. However, OECD analysis shows a market failure often prevents stakeholders to optimally value the digital security of products and services, and that market incentives on their own are unlikely to fix gaps in digital security risk management (OECD, 2021[34]; OECD, 2021[35]; OECD, 2021[1]). In particular, complex and opaque supply chains often lead to a misallocation of responsibility for digital security, and significant *information asymmetries* prevent end-users – particularly SMEs and consumers –

from making informed decisions about the products and services they purchase. In addition, *negative externalities* often lead the suppliers and users of products to neglect digital security, enabling malicious actors to use these products to launch attacks, including across borders. More broadly, there is a misperception of digital security risk and a misalignment of market incentives.

The *Products and Services Recommendation* includes guidance on policies to realign market incentives and empower stakeholders to enhance the digital security of products and services. It outlines areas of action for policy makers, and provides guidance on which policy tools can be effective. It covers the five areas highlighted in Figure 6. This section introduces only a few of them.

The digital security of products and services is much more than a technical issue calling for technical remedies. It is rather a key public policy challenge calling for a whole-of-government approach. Policy makers need to take a holistic approach this issue, be proactive rather than reactive, and shape the policy environment for the digital security of products and services with foresight. In this regard, international co-operation stands out as a key success factor and 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.

Figure 6. Overview of the Products and Services Recommendation



Source: OECD

To realign market incentives, policy measures can aim to ensure that suppliers take responsibility for the digital security of their products and services throughout their products and services' lifecycle. This "*duty of care"* can be broken down into 6 action lines, whereby suppliers adopt:

- *Security by design*: suppliers integrate digital security at every stage of the product's lifecycle, taking into account digital security risk in the product's supply chain;

- *Security by default*: suppliers take responsibility for digital security rather than shifting it to users, for example by pre-configuring and activating security features by default in the product, and providing users with security updates until the product's end of support;
- Ongoing treatment and co-ordination of vulnerabilities, in line with the Vulnerabilities Recommendation (cf. 4.1);
- *Responsible end-of-support policies*: suppliers reduce the gap between the end-of-support and end-of-use, for instance to avoid the emergence of an "Internet of Forgotten Things";
- *Co-operation across the supply chain's code owners*: suppliers identify all code components and dependency relationships (bill of material), and vulnerabilities are treated across the value chain with the help of a co-ordinator;
- *Assessment of the level of digital security*: suppliers self-assess the level of digital security of their products based on international standards, and/or certify that level through third party evaluation.

In addition, to reduce information asymmetries, public policies should aim to *increase transparency and foster information sharing* about the digital security of products and services. Increased transparency and information sharing aim to raise awareness and empower users to effectively assess digital security risk related to products and services, and make informed decisions on how to use them. They can also incentivise suppliers to further value and invest in the digital security of their products and services. Policies in this area should further incentivise suppliers to provide more information regarding their products and services' technical features (e.g. updatability), the processes they put in place (e.g. end-of-support) and the traceability of components (e.g. bill of materials). Developing third-party evaluation such as audits, inspection tests and certification is also a promising avenue to increase transparency.

4. Technical level: encouraging good practice

The last layer of the Framework includes policy issues that are more technical in nature. The treatment of digital security vulnerabilities is introduced below (4.1). The OECD Cryptography Policy Guidelines and E-Authentication Recommendation [will be included in a future version (OECD, 1997[10]) (OECD, 2007[9]).

4.1. Vulnerability treatment

Vulnerabilities are weaknesses that can be exploited to damage economic and social activities. They are a major source of digital security risk. Code, the engine of digital transformation, is never perfect, and almost always has vulnerabilities: where there is code, there are vulnerabilities, and the more code there is, the more vulnerabilities there are, with variable levels of severity. Furthermore, information systems also have vulnerabilities related to how software is implemented, configured and updated.

Criminals and other ill-intentioned actors actively seek to discover such code and system vulnerabilities, and develop or use tools such as “malware” to exploit them through incidents that harm businesses, governments and individuals, threaten critical activities and undermine trust in digital transformation. Addressing these vulnerabilities before attackers take advantage of them is an effective means to reduce the probability of incidents.

Vulnerabilities are a fact of digital life, a by-product of the increasing complexity of code and systems, combined with weak digital security practices among suppliers and users. While it is not possible to completely eradicate vulnerabilities from all code and systems, improving their treatment is a major opportunity to reduce digital security risk and increase trust in the digital transformation era.

To reduce security risk, stakeholders should treat vulnerabilities, each according to their role. Developers should look and test for vulnerabilities in their code, develop mitigations to fix them (e.g. “patches”, “security updates”), and distribute them to other actors across the value chain towards end-users. Organisations should monitor their information systems to ensure that these mitigations are appropriately applied and avoid product misconfigurations. These are complex and expensive endeavours, especially when vulnerabilities are located in code components developed by third-parties in the supply chain, including open source software, or affect numerous products, under-resourced organisations, or businesses with low digital maturity such as traditional manufacturers entering the Internet of Things (IoT) market. They are also never-ending tasks because malicious actors continuously discover and exploit new vulnerabilities. In addition, in many cases, stakeholders need to disclose information about vulnerabilities they discovered, for example to facilitate threat detection. Vulnerability treatment refers to the overarching process encompassing the discovery of a vulnerability, how the vulnerability is handled by suppliers (“code owners”), managed by system owners, and publicly disclosed.

Over the last few years, the technical community has made progress in developing good practice for treating vulnerabilities, including through co-ordinated vulnerability disclosure (CVD). However, significant economic and social challenges prevent stakeholders from adopting good practice. For example, software

developers and system owners are often insufficiently aware that it is their joint responsibility to address vulnerabilities. They often lack resources and skills, and misaligned market incentives may disincentivise them to take action. Many of them can ignore vulnerability researchers, and may even threaten them with legal proceedings. Vulnerability researchers, also known as "ethical hackers", discover and report vulnerabilities to the software developers and system owners who can mitigate them, thereby reducing cost and users' "window of exposure" to digital security risk. When ignored or threatened, vulnerability researchers may be tempted to disclose the vulnerability information publicly without co-ordinating with other stakeholders, which may create risk for all users and the economy. They may also turn to the black market to monetise vulnerability information, thereby feeding the criminal ecosystem.

Public policies aimed at removing these obstacles and encouraging vulnerability treatment have the potential to significantly reduce digital security risk for all (OECD, 2021[36]; OECD, 2021[37]; OECD, 2021[38]). The complexity of this key area is the first obstacle that policy makers face when they consider addressing it at the domestic level. Therefore, they first need to establish a dialogue with the technical community (e.g. vulnerability researchers, system owners, developers, academia, etc.) to get rid of common misconceptions, such as those introduced in Box 4.

Box 4. Common misconceptions about digital security vulnerabilities

Vulnerability treatment is a complex area that policy makers need to be approach in co-operation with the technical community in order to avoid ineffective and counterproductive policy measures. Examples of common *misconceptions*, based on OECD analytical work on vulnerabilities, include the following:

You may think that …	… When in reality
Developing secure products will eliminate all vulnerabilities and solve this problem.	Security-by-design is essential (cf. 3.2), but where there is code, there are always vulnerabilities. There is no such thing as a fully secure product that contains code. There is no silver bullet against vulnerabilities and it is impossible to eliminate them all, because attackers' techniques evolve. Products and services require constant monitoring of vulnerabilities.
Developing mitigations (e.g. "patches") for zero-day vulnerabilities –i.e. newly discovered vulnerabilities in products– is the most urgent priority.	Developing mitigations for zero-days is key, but if system owners do not implement these mitigations, they are worthless. Vulnerability treatment is a shared responsibility of suppliers and system owners, together with vulnerability researchers who can help both of them.
All security updates should be automatic, so vulnerabilities would be easily fixed when mitigations are available.	Security updates themselves may carry security risk. Applying them blindly to complex systems, such as in large organisations, can create security incidents. Therefore system owners often need to test them prior to applying them. Vulnerability management is a risk-based process that generally excludes one-size-fits-all approaches.
Governments can help because they are always neutral in this technical area.	Stakeholders do not necessarily trust governments because some may actually buy vulnerabilities to exploit them. Governments are part of the solution, but also part of the problem. This shows that while this area is quite technical, many obstacles are cultural, social, economic, legal and even political.
Bug bounties, whereby organisations pay researchers to report vulnerabilities to them, will solve the problem.	Bug bounties can be very valuable tools, but they are no panacea. They are suited for sufficiently resourced and mature organisations that already have a well-organised vulnerability management or handling process. They should be used as one tool among others to reduce risk, such as software code reviews, audits and network penetration tests.

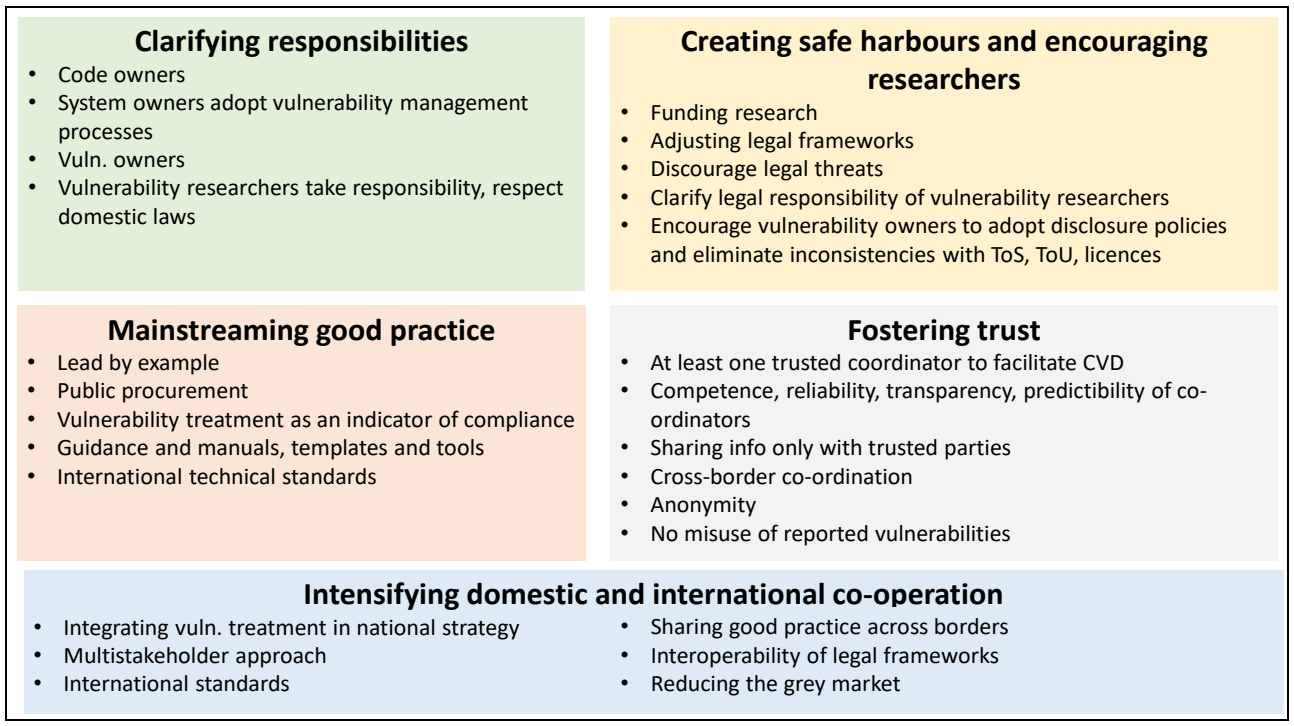
Governments should also use the *Vulnerabilities Recommendation* to ground their policies in internationally recognised good practice. The Recommendation focuses on five areas for policy action (cf. Figure 7):

- *Clarifying responsibilities* for each category of stakeholders such as software developers and owners of information systems, as well as vulnerability researchers. For example, software developers should not intentionally insert vulnerabilities in their products ("backdoors");
- *Creating safe harbours and encouraging vulnerability researchers*. Policies should establish safe harbours where researchers who follow good practice are protected against threats of legal proceedings from vulnerability owners, and such legal threats are discouraged;
- *Fostering trust*, by ensuring that stakeholders have access to at least one trusted co-ordinator who can assist in resolving issues between participants, and by ensuring that their institutional frameworks is trusted by vulnerability researchers;
- *Mainstreaming good practice*, including by implementing it within the government itself, leveraging public procurement, using vulnerability treatment as an indicator of contractual and regulatory compliance, as well as developing and disseminating guides and manuals;

- *Intensifying domestic and international co-operation*, by integrating vulnerability treatment in the national digital security strategy, leveraging the multi-stakeholder security community, reducing the grey market for vulnerabilities, sharing good practice across borders and ensuring the cross-border interoperability of legal frameworks to protect vulnerability researchers.

Operational principles focus on the implementation of digital security risk management in organisations. They are based on the digital security fundamentals introduced in 1.1. Policy makers can also use the OECD report on *Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities* (OECD, 2022[39]), which provides more details on vulnerability treatment in practice while avoiding technical jargon and detailed considerations. It may also help technical security experts to communicate with policy makers and non-technical experts in their organisation such as CEOs, board members, communication departments, lawyers, etc. on vulnerability treatment.

Figure 7. Overview of the Vulnerabilities Recommendation



Source: OECD

Acronyms

AI – Artificial Intelligence

APT – Advanced Persistent Threat

CERT – Computer Emergency Response Team

CISA – Cybersecurity and Infrastructure Security Agency

CIIP – Critical Information Infrastructure Protection

CSIRT – Computer Security Incident Response Team

CVD – Coordinated Vulnerability Disclosure

ENISA –European Union Agency for Cybersecurity

ICT – Information and Communication Technologies

IEC - International Electrotechnical Commission

IETF – Internet Engineering Task Force

IoT – Internet of Things

ISAC – Information Sharing and Analysis Center

ISO - International Organization for Standardization

IT – Information Technologies

ITU-T - International Telecommunication Union (ITU) Telecommunication Standardization Sector

MNE – Multinational Entreprises

NCSC – National Cyber Security Center

NGO – Non Governmental Organisation

NIST – National Institute of Standards and Technologies

OECD –Organisation for Economic Co-operation and Development

OEWG – Open Ended Working Group

RBC – Responsible Business Conduct

SME – Small and Medium-sized Enterprises

UNDOC – United Nations Office on Drugs and Crime

UNGGE – United Nations Group of Governmental Experts

References

Bernat, L. (2021), *Enhancing the digital security of critical activities, OECD Going Digital Toolkit Notes, No. 17*, OECD Publishing, Paris, https://doi.org/10.1787/a91b818b-en. [33]

CISA (n.d.), *Information Sharing and Analysis Organizations (ISAOs)*, https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos. [30]

ENISA (2018), *Information Sharing and Analysis Center (ISACs) - Cooperative models*, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models. [29]

Gierten, D. and M. Lesher (2022), *Assessing National Digital Strategies and their Governance*, No. 324, OECD Publishing, Paris, https://www.oecd-ilibrary.org/docserver/baffceca-en.pdf. [26]

Krugman, P. (2009), *The Return of Depression Economics and the Crisis of 2008*, W. W. Norton & Company. [32]

NCSC-NL (2018), *Starting an ISAC: Sectoral Collaboration. Guide*, https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2019/juli/02/ncsc-guide-isac/ncsc_guide_isac.pdf. [31]

NIST (2018), *Cybersecurity Framework*, https://www.nist.gov/cyberframework. [3]

OECD (2022), *Good Practice Guidance on the Co-ordination of vulnerabilities*, OECD, Paris, https://one.oecd.org/document/DSTI/CDEP/SDE(2021)9/FINAL. [39]

OECD (2022), *Recommendation of the Council on Digital Security of Products and Services*, OECD/LEGAL/0481, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481. [7]

OECD (2022), *Recommendation of the Council on Digital Security Risk Management*, OECD/LEGAL/0479, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479. [4]

OECD (2022), *Recommendation of the Council on National Digital Security Strategies*, OECD/LEGAL/0480, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480. [5]

OECD (2022), *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities*, OECD/LEGAL/0482, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482. [8]

OECD (2021), "Digital security in SMEs", in *The Digital Transformation of SMEs*, OECD Publishing, Paris, https://doi.org/10.1787/cb2796c7-en. [28]

OECD (2021), *Encouraging vulnerability treatment - Overview for policy makers*, OECD, Paris, https://doi.org/10.1787/0e2615ba-en. [2]

OECD (2021), *Encouraging vulnerability treatment: background report - Responsible management, handling and disclosure of vulnerabilities*, OECD, Paris, https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf. [38]

OECD (2021), *Encouraging vulnerability treatment: How policy makers can help address digital security vulnerabilities*, OECD, Paris, http://www.oecd.org/digital/encouraging-vulnerability-treatment.pdf. [37]

OECD (2021), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers*, No. 307, OECD, Paris, https://doi.org/10.1787/0e2615ba-en. [36]

OECD (2021), "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. [35]

OECD (2021), *Recommendation of the Council on Broadband Connectivity*, OECD/LEGAL/0322, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0322. [14]

OECD (2021), *Recommendation of the Council on Children in the Digital Environment*, OECD/LEGAL/0389, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [16]

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, https://www.oecd.org/digital/smart-policies-for-smart-products.pdf. [1]

OECD (2021), "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. [34]

OECD (2020), *Encouraging digital security innovation : Global Forum on Digital Security for Prosperity*, OECD Publishing, Paris, https://doi.org/10.1787/e65d02af-en. [27]

OECD (2020), *Going Digital integrated policy framework*, OECD Publishing, Paris, https://doi.org/10.1787/dc930adc-en. [11]

OECD (2019), "Policies for the protection of critical information infrastructure: Ten years later", *OECD Digital Economy Papers*, No. 275, OECD Publishing, Paris, https://doi.org/10.1787/efb55c54-en. [40]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [15]

OECD (2019), *Recommendation of the Council on Digital Security of Critical Activities*, OECD/LEGAL/0456, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. [6]

OECD (2018), "Digital security policy", in *OECD Reviews of Digital Transformation: Going Digital in Sweden*, OECD Publishing, Paris, https://doi.org/10.1787/9789264302259-en. [25]

OECD (2018), *OECD Due Diligence Guidance for Responsible Business Conduct*, OECD, Paris, https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf. [18]

OECD (2016), *Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration)*, OECD/LEGAL/0426, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0426. [21]

OECD (2016), *Recommendation of the Council on Consumer Protection in E-commerce*, OECD/LEGAL/0422, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422. [13]

OECD (2015), *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264236882-en. [20]

OECD (2015), *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415. [41]

OECD (2015), *Recommendation of the Council on Principles of Corporate Governance*, OECD/LEGAL/0413, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0413. [19]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [12]

OECD (2011), *Declaration on International Investment and Multinational Enterprises*, OECD/LEGAL/0144, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0144. [17]

OECD (2011), *OECD Guidelines for Multinational Enterprises*, OECD Publishing, Paris, https://doi.org/10.1787/9789264115415-en. [24]

OECD (2011), *Recommendation of the Council on Principles for Internet Policy Making*, OECD/LEGAL/0387, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0387. [22]

OECD (2008), *Declaration for the Future of the Internet Economy (The Seoul Declaration)*, OECD/LEGAL/0366, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0366. [23]

OECD (2007), *Recommendation of the Council on Electronic Authentication*, OECD/LEGAL/0353, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0353. [9]

OECD (1997), *Recommendation of the Council concerning Guidelines for Cryptography Policy*, OECD/LEGAL/0289, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289. [10]

Notes

[1] All OECD Recommendations are available on the online Compendium of OECD Legal Instruments.

[2] Available at https://oe.cd/security.

[3] Cf. Principle 3. Human Rights and Fundamental Values of the Digital Security Recommendation

[4] See also https://mneguidelines.oecd.org/ and (OECD, 2011[24]) for an edition of the MNE Guidelines with a commentary.

[5] The Due Diligence Guidance is referred to in the Recommendation on the OECD Due Diligence Guidance for Responsible Business Conduct (OECD, 2018[18]).

[6] From a pure risk management perspective, risk is the effect of uncertainty on objectives. This effect can be detrimental or beneficial.

[7] ISO/IEC standards define risk as « the effect of uncertainty on objectives ». When stakeholders assess risk, uncertainty is generally represented in terms of *likelihood* and the effect in terms of *severity*.

[8] Cf. ISO/IEC Guide 73:2009 "Risk Management Vocabulary. Management du risque – Vocabulaire", and ISO/IEC 27000:2018 "Information technology — Security techniques — Information security management systems — Overview and vocabulary".

[9] https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

[10] In addition to the full text of the Recommendation, the *Companion document of the 2015 Recommendation on digital security risk management for economic and social prosperity* provides further explanations of the principles.

[11] According to the MNE Guidelines, enterprises should "10. Carry out risk-based due diligence, for example by incorporating it into their enterprise risk management systems, to identify, prevent and mitigate actual and potential adverse impacts […]. 11. Avoid causing or contributing to adverse impacts on matters covered by the Guidelines, through their own activities, and address such impacts when they occur. 12. Seek to prevent or mitigate an adverse impact where they have not contributed to that impact, when the impact is nevertheless directly linked to their operations, products or services by a business relationship." (Chapter II, General Policies Section A) (OECD, 2011[24]).

[12] There may be other areas, not currently covered in the draft Policy Framework, where policy intervention might be needed to address other market failures.

[13] The rationale for this evolution is further detailed in (Bernat, 2021[33]) and (OECD, 2019[40]).