Recommendation of the Council on Digital Security of Critical Activities

OECD Legal Instruments

OECD
BETTER POLICIES FOR BETTER LIVES

This document is published under the responsibility of the Secretary-General of the OECD. It reproduces an OECD Legal Instrument and may contain additional material. The opinions expressed and arguments employed in the additional material do not necessarily reflect the official views of OECD Member countries.

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

For access to the official and up-to-date texts of OECD Legal Instruments, as well as other related information, please consult the Compendium of OECD Legal Instruments at http://legalinstruments.oecd.org.

Please cite this document as:
OECD, *Recommendation of the Council on Digital Security of Critical Activities*, OECD/LEGAL/0456

Series: OECD Legal Instruments

Photo credit: © Adobe Stock/mumemories

© OECD 2024

This document is provided free of charge. It may be reproduced and distributed free of charge without requiring any further permissions, as long as it is not altered in any way. It may not be sold.

This document is available in the two OECD official languages (English and French). It may be translated into other languages, as long as the translation is labelled "unofficial translation" and includes the following disclaimer: *"This translation has been prepared by [NAME OF TRANSLATION AUTHOR] for informational purpose only and its accuracy cannot be guaranteed by the OECD. The only official versions are the English and French texts available on the OECD website http://legalinstruments.oecd.org"*

Background Information

The Recommendation on Digital Security of Critical Activities was adopted by the OECD Council on 11 December 2019 on proposal of the Committee on Digital Economy Policy (CDEP). It replaces the 2008 OECD Recommendation on the Protection of Critical Information Infrastructure (hereafter the "2008 CIIP Recommendation") [OECD/LEGAL/0361].

Critical activities are increasingly exposed to digital security risk

Most economic and social activities are digital dependent. Among these activities, some are critical because their interruption or disruption could have a serious impact on the health, safety, and security of citizens; or the effective functioning of services essential to the economy and society; or economic and social prosperity more broadly.

The 2008 CIIP Recommendation was a pioneering international standard that played a key role in raising awareness about the need to develop policies to better protect information systems and networks that support critical activities (so-called "critical information infrastructures" or CII).

However, since 2008, the digital reliance of critical activities has increased and is now accelerating with digital transformation and the generalisation of technologies such as big data, artificial intelligence, and the Internet of Things. In parallel, digital security threats have been growing in number and sophistication. Many governments are anticipating a greater occurrence and severity of digital security incidents affecting critical activities in the coming years, potentially leading to large-scale disasters.

The combination of increased digital dependency of and threats to critical activities pushes governments to adopt policies that strengthen digital security of critical activities. However, such policies should not undermine the benefits from digital transformation in critical sectors through constraints that would inhibit innovation or unnecessarily restrict the use, dynamic nature and openness of digital technologies.

A modernised framework to enhance digital security of critical activities

CDEP's Working Party on Security and Privacy in the Digital Economy (SPDE) monitored the implementation of the 2008 CIIP Recommendation and agreed on the need to update and replace it in order to take into account changes since 2008, as well as the experience acquired by Adherents in implementing policies in this area.

The 2019 Recommendation:

- focuses on the critical economic and social activities that rely on the information infrastructures rather than on the information infrastructures themselves. This evolution promotes an economic and social – rather than purely technical – risk management approach to digital security. In so doing, it ensures coherence with the 2015 Recommendation on Digital Security Risk Management for Economic and Social Prosperity [OECD/LEGAL/0415].
- helps clarify where this policy area stands within the broader landscape of digital security policy and national risk management / critical infrastructure protection policy.
- sets out a range of policy recommendations to ensure that policies targeting operators of critical activities focus on what is critical for the economy and society without imposing unnecessary burdens on the rest. These recommendations also support Adherents in: (i) adapting their overarching policy framework; (ii) promoting and building trust-based partnerships; and (iii) improving co-operation at the international level.

A two-year process for developing of the 2019 Recommendation

The review process of the 2008 CIIP Recommendation lasted more than two years with inputs received from more than eighteen countries, civil society and business representatives on the basis of a survey questionnaire. The analysis of responses indicated a need to update the CIIP Recommendation and provided key material to guide the development of the 2019 Recommendation.

In 2018, an informal group composed of experts from governments, business, civil society and the internet technical community was created to guide the Secretariat in the development of the 2019 Recommendation.

Implementation and dissemination tools

To support the implementation of the Recommendation, the CDEP will serve as a forum for (a) exchanging information on digital security of critical activities to identify good practices in coordination with other international fora and (b) developing analytical work to support the Recommendation's implementation.

For further information please consult: www.oecd.org/sti/ieconomy/security.htm.

The COVID-19 crisis highlighted our dependence on certain critical activities, as well as the growing digitalisation of their operators, which increases their exposure to digital security risk. For instance, many hospitals have been the target of digital security attacks such as Distributed Denial-of-Service (DDoS) or ransomware. In fact, the pandemic has been a stress test for the digital security risk management practices of many of our critical infrastructures. This Recommendation provides governments with timely guidance on strengthening the digital security of such critical activities, without undermining the benefits of digital transformation.

For more information, see:

- Dealing with digital security risk during the Coronavirus (COVID-19) crisis

Contact information: digitalsecurity@oecd.org.

Implementation

OECD Going Digital Toolkit Policy Note "Enhancing the digital security of critical activities"

The digital transformation of critical activities such as the delivery of water, energy, healthcare, telecommunications, and banking services increasingly exposes them to cybersecurity threats, which can affect the health, safety, and security of citizens, the functioning of essential services, or economic and social prosperity more broadly.

Approved by the Committee on Digital Economy Policy on 31 August 2021, the Policy Note is based upon the Recommendation and supports its implementation. It introduces key concepts, such as critical activities, critical information infrastructure (CII), cybersecurity and digital security risk management, and helps policy makers identify what needs to be protected and what types of measures operators of critical activities should take. It further discusses the institutional framework to develop and supervise policies to enhance the digital security of critical activities, including trust-based partnerships, and provides a selection of policy approaches from a range of jurisdictions in the Annex.

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

HAVING REGARD to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188]; the Recommendation of the Council on Principles for Internet Policy Making [OECD/LEGAL/0387]; the Recommendation of the Council on the Governance of Critical Risks [OECD/LEGAL/0405]; the Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity [OECD/LEGAL/0415] (Digital Security Risk Recommendation) and the Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration) [OECD/LEGAL/0426];

HAVING REGARD to the experience and best practices that emerged from the implementation of the Recommendation of the Council on the Protection of Critical Information Infrastructures [OECD/LEGAL/0361], which this Recommendation replaces;

RECOGNISING that

- Digital transformation affects all economic and social activities, spurring innovation and generating significant benefits, but also exposes these activities to increasing digital security risk;
- Digital security risk results from potential intentional or unintentional threats that are cross-border in nature, exploit vulnerabilities and produce incidents affecting the availability, integrity and confidentiality of the data, hardware, software and networks on which these activities rely;

RECOGNISING that the multiplicity and complexity 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; that each actor is therefore dependent upon and responsible towards all others to manage digital security risk;

RECOGNISING that partnerships within and across the public and private sectors are essential to approach digital security risk to critical activities in a coherent and holistic manner;

RECOGNISING that the Digital Security Risk Recommendation provides a robust framework to strengthen digital security of economic and social activities without reducing the opportunities offered by digital transformation;

RECOGNISING that critical activities run by different operators in different sectors and countries depend on the same digital technologies and therefore can be simultaneously disrupted by threats exploiting common vulnerabilities; that digital security incidents can propagate extremely quickly across operators, sectors and borders; and that disruptions in the delivery of critical activities caused by digital security incidents in one place can cascade onto other operators, sectors and countries, potentially affecting regions and international stability;

RECOGNISING that the consequences of digital security incidents affecting critical activities run by public and private operators may extend beyond the interests of these operators, affect a whole society and others beyond borders; and that, as a consequence, any residual risk taken by these operators may affect all those who depend on such activities as well as society as a whole;

RECOGNISING that enhancing the digital security of critical activities is a priority for national policy; that discrepancies in public policies across countries increase the complexity of managing the digital security of interdependent critical activities across borders; and that international co-operation is therefore essential to reduce such discrepancies and maximise the global effectiveness of domestic policies;

MINDFUL that the management of digital security risk to critical activities has to respect privacy and personal data protection;

MINDFUL of the variety of cultures, as well as legal and institutional frameworks in Members and non-Members adhering to this Recommendation (hereinafter the "Adherents") and of the possible use of different terminology in Adherents' policies to enhance digital security of critical activities;

On the proposal of the Committee for Digital Economy Policy:

I. **AGREES** that the purpose of this Recommendation is to provide guidance on how to implement the Digital Security Risk Recommendation to maintain the continuity, resilience and safety of critical activities without inhibiting the benefits from digital transformation.

II. **AGREES** that, for the purpose of this Recommendation:

- **Critical activities** refer to economic and social activities the interruption or disruption of which would have serious consequences on:
  - the health, safety, and security of citizens;
  - the effective functioning of services essential to the economy and society, and of the government; or
  - economic and social prosperity more broadly.

  Critical activities are identified on the basis of a national risk assessment.
- **Operators** are the public and private entities that carry out critical activities.
- **Critical functions** refer to the processes without which operators could not effectively carry out their critical activities.
- **Digital ecosystem** refer to the digital environment that supports an operator's critical functions along the value chain of critical activities. It includes digital assets such as hardware, software, networks and data, operational technologies that detect or cause changes in physical processes, as well as the internal and external entities, persons and processes that design, maintain and operate them, and the relationships between them.

OVERARCHING POLICY FRAMEWORK

III. **RECOMMENDS** that Adherents develop a **strategic approach** to the management of digital security risk to critical activities by:

1. Adopting at the highest level of government, and as part of a national digital security strategy, **clear objectives** to strengthen digital security and resilience of critical activities, and ensure consistency with national risk assessment and other risk and sector-specific strategies.
2. Adopting and publicly releasing a **domestic governance** mechanism that allocates authority and responsibility to specific government bodies for developing and implementing with relevant stakeholders policies to enhance digital security of critical activities within and across sectors. The domestic governance mechanism should also identify, where appropriate, any supporting role played by government bodies in charge of national security and defence.
3. Ensuring a whole-of-government **domestic co-ordination** in order to:
   a. Establish intra-governmental co-operation, taking full account of the importance of a dialogue between digital security and sectoral experts;
   b. Ensure consistency of the measures adopted across sectors, where appropriate, and resolve potentially competing policy objectives;

c. Allocate resources effectively across responsible government bodies and create a critical mass of expertise and skills; and

d. Facilitate cross-border co-operation.

IV. RECOMMENDS that Adherents **build capacity** to support digital security risk management and resilience of critical activities by:

1. Developing a new or strengthening their existing **incident response capability**, such as through one or more Computer Emergency Response Teams (CERT), Computer Security Incident Response Teams (CSIRT) and/or Security Operation Centres (SOC), in charge of monitoring, warning, alerting and carrying out recovery measures, as well as mechanisms to foster closer co-operation and communications among those involved in incident response;
2. Facilitating **co-operation among CERTs/CSIRTs/SOCs and operators**, including incident reporting and analysis, to promote swift and effective operational cooperation;
3. Applying best practice for digital security risk management related to the provision of **critical digital activities by the government**.
4. Promoting **international digital security standards**, methodologies, baseline security manuals, best practice and tools;
5. Providing **support to operators**, as appropriate, including by:
   a. sharing information on threats, vulnerabilities, and risk management practice,
   b. supporting operators in assessing risk and establishing appropriate risk treatment measures,
   c. providing assistance and/or guidance in case of incident or crisis; and
   d. providing toolkits, methodologies, best practice and tools;
6. Fostering the **development of the global market** for a variety of trusted security services and products, including managed services, audit and response services, including where appropriate through a range of mechanisms for credible signalling of the nature and degree of security;
7. Supporting the development of a **skilled workforce** that can manage cross-sector and sector-specific digital security risk;
8. Adopting and encouraging the adoption of **responsible and co-ordinated vulnerability disclosure and management** processes, as well as encouraging and protecting security researchers; and
9. Sharing, as appropriate, with operators and other actors, appropriately **aggregated statistical data** from incident reporting;

V. RECOMMENDS that Adherents establish evidence-based **monitoring and supervision** cycles to *i)* evaluate and appraise implementation of requirements by operators, and *ii)* enable continuous improvement of policies, legal frameworks and self-regulatory schemes in order to meet the expected level of protection.

VI. RECOMMENDS that Adherents **integrate digital security risk to critical activities in national risk management** such that:

1. National risk assessments enable identification of critical activities and their operators, taking into consideration the critical activities' value chain; and
2. Operators are encouraged to conduct a cyclical enterprise risk assessment to identify critical functions necessary to ensure provisioning of critical activities.

MEASURES FOR OPERATORS

VII. **RECOMMENDS** that Adherents ensure that operators:

1. are responsible to manage digital security risk to critical functions with a view to protecting the continuity, resilience and safety of critical activities that they enable; and
2. effectively reduce the digital security risk to critical functions to a level acceptable for society, consistent with national risk assessment, by encouraging or requiring, where appropriate, that they take governance, protection, detection and response, and resilience measures. Such measures should include:

a. Governance – establishing an organisational framework for cyclical digital security risk assessment and treatment

i. Assigning responsibility for digital security risk management to the highest level of leadership;

ii. Integrating digital security risk management and digital security governance within their overall cyclical enterprise risk management framework;

iii. Adopting an internal digital security risk management policy that defines:

a) Responsibilities and modalities for accountability with respect to digital security risk ownership, assessment and treatment, residual risk acceptance, and processes to review digital security risk-related decisions; and

b) Modalities to ensure that digital security risk management is systematically integrated into strategic and operational decisions related to the use of digital technologies; and that leaders and decision makers are informed and supported by digital security experts;

iv. Mapping the operator's digital ecosystem, including internal and external dependencies to identify the components that are essential to the critical functions;

v. Conducting cyclical digital security risk assessments of critical functions, taking into account the operator's digital ecosystem and the potential impact that digital security incidents could have on the critical activities of the operator itself, on third parties, in particular other operators in the same and in other sectors, and on the economy and society as a whole;

vi. Determining, on the basis of the digital security risk assessment, the level of digital security risk to be reduced, transferred, avoided, and accepted (risk treatment);

vii. Performing periodical digital security audits;

viii. Investing in digital security training and skills development; and

ix. Fostering best digital security risk management practice along the supply chain.

b. Protection – implementing appropriate security measures to reduce digital security risks to critical functions

i. Determining security measures related to the operator's digital architecture, system administration, personnel training, digital security maintenance as well as physical security;

ii. Maintaining appropriate identity management, authentication and access control measures;

iii. Determining measures related to data security, including the protection of data at rest and in transit; and

iv. Sharing with the government and experts, as appropriate, information about the economic and social impacts of incidents with a view to improving digital security public policy frameworks.

c. Detection and Response – putting in place processes and measures to defend against and respond to incidents

i. Setting up security information and event management, incident detection and monitoring operations, and carrying out appropriate analyses;

ii. Setting up incident management processes and measures as well as response capabilities (e.g. CERTs) and up-to-date procedures for handling response and analysis of incidents;

iii. Reporting, as appropriate, incidents, including near-misses according to their level of criticality, to a relevant government body and/or other relevant entities or fora (e.g. sectoral cooperation fora); and

iv. Communicating, as appropriate, incidents to the public as soon as possible.

d. Resilience – adopting appropriate preparedness and recovery measures to ensure the continuity of critical functions

i. Adopting strategic objectives and recovery plans for business continuity, crisis management, and disaster recovery which take safety into account;

ii. Testing and improving business continuity, crisis management and disaster recovery plans regularly, including by organising, co-organising and participating in internal, cross-operator, cross-sector and cross-border exercises; and

iii. Ensuring that the operator's business decision makers are leading crisis management planning and implementation, with the support of digital security technical experts.

TRUST-BASED PARTNERSHIPS

VIII. RECOMMENDS that Adherents promote and build trust in sustainable partnerships to ensure that digital security risk management of critical activities appropriately takes account of dependencies across sectors and borders. To that effect, Adherents should:

1. Develop **partnerships for policy development and implementation** through:

a. An open dialogue at the national level between operators and relevant government bodies to determine and implement the measures that operators should take, taking into account the specificities of each sector as well as the business, resources, regulatory, and market constraints of operators, including small and medium-sized enterprises;

b. Support for private-private cooperation and structured dialogue among operators within and across sectors, as well as with other relevant private actors (e.g. vendors), to foster exchanges on digital security expertise, threats and risk management;

c. Ongoing dialogue between digital security and sectoral experts to improve mutual understanding of their respective specificities and constraints; and

d. Bilateral and multilateral co-operation to share knowledge and experience with respect to domestic policies, practices and co-ordinating models with operators, and to facilitate collective action to:

i. manage digital security risk to critical activities with cross-border dependencies and interdependencies; and

ii. address cross-sector and sector-specific digital security vulnerabilities, threats, incidents and impacts on critical activities.

2. Strengthen **operational co-operation** by:

   a. Fostering partnerships for co-operation among operators within and across sectors and borders, on incident prevention, detection, and response with a view to encouraging information sharing and exchange on threats, vulnerabilities, incidents, impact and risk management practice;

   b. Creating the conditions for formal and informal co-operation between operators when it does not already exist, including without government participation if it could impact trust relationships among partnerships' participants;

   c. Creating the conditions for digital security exercises to take place with relevant operators, within and across sectors and borders, in order to strengthen digital security preparedness, test and improve strategic decision making and co-ordination mechanisms;

   d. Encouraging operators to participate in international or regional networks for watch, warning and incident response to enable information sharing and co-ordination at the operational level, as well as to better manage crises in case of an incident developing across borders;

   e. Supporting cross-border collaboration for, and information sharing on, public-private research and development for digital security of critical activities, including on methodologies for impact assessment of digital security incidents; and

   f. Supporting advanced research, fostering innovation and working together to develop digital security risk management skills and knowledge that will help create a skilled workforce for the future.

3. Set up **trust conditions** for sustainable partnerships by ensuring that:

   a. the aims and values of partnerships are shared by partners and transparent to the public;

   b. the roles and responsibilities of the various parties involved are clear;

   c. partnerships are based upon clear rules accepted by all partners so that partners' actions are reliable, predictable, and consistent over time;

   d. partners mutually benefit from the partnership over time, including by creating the conditions for operators to share information with and receive information from the government; and

   e. the information shared by operators and the government:

      i. is disclosed on a voluntary basis, only to the appropriate audiences, and subject to information sharing protocols;

      ii. is managed in a responsible manner, according to a set of rules governing its receipt, retention, use and dissemination consistent with privacy and personal data protection regulations, and other regulations protecting the confidentiality of information (e.g. trade secrets). Such rules should in particular ensure that personal data unrelated to a digital security threat is removed prior to any exchange of information; and

      iii. will only be used for defensive purposes.

   f. the confidentiality of risk and risk management-related information shared by operators with the government is protected so as not to unnecessarily expose the operator's reputation and commercial interest.

INTERNATIONAL CO-OPERATION

IX. RECOMMENDS that Adherents actively co-operate at international level by:

1. Sharing:

a. information regarding the roles and responsibilities of government bodies and other relevant stakeholders in charge of digital security risk management of critical activities with other Adherents' counterparts to improve timeliness of cross border co-operation;

b. experience on the development and implementation of policies to identify good practice and, insofar as possible, minimise differences across countries; and

c. aggregated statistical data from incident reporting, as appropriate, and work together to ensure the international comparability of such statistics.

2. Supporting capacity building efforts to assist other countries in the development and implementation of their policy on digital security of critical activities, as appropriate.

X. **INVITES** the Secretary-General and Adherents to disseminate this Recommendation.

XI. **INVITES** Adherents to the Digital Security Risk Recommendation to take due account of, and adhere to, this Recommendation.

XII. **INSTRUCTS** the Committee for Digital Economy Policy to:

a. Serve as a forum for:

i. exchanging information on digital security of critical activities to identify good practice in coordination with other international fora, and

ii. for developing analytical work to support the implementation of the Recommendation;

b. Monitor the implementation of this Recommendation and report to Council within five years of its adoption and at least every ten years thereafter.

Related documents

EXPLANATORY NOTE [1]

Digital technologies foster innovation, enhance productivity, and improve goods and services' effectiveness, to name a few of their benefits. They have become so pervasive across value and supply chains, deeply embedded in physical industrial and consumer devices, and at every stage of service delivery, that **most economic and social activities have become digital dependent**.

Among these activities, some are critical because their interruption or disruption could have a serious impact on the health, safety, and security of citizens; or the effective functioning of services essential to the economy and society, and of the government; or economic and social prosperity more broadly. These critical activities include, for example, the distribution of energy, the provision of health care and the delivery of key banking services. They also include the operation of major businesses or value chains supporting a significant share of a country's GDP, without necessarily being indispensable for the economy to function.

Digital reliance of critical activities started several decades ago and increased progressively, as public and private operators of critical activities increasingly used digital technologies to automate their business processes. This evolution reached a first milestone after the turn of the millennium with the general adoption of internet technologies, when previously isolated and closed information systems and networks became globally interconnected and open by default. While digital openness and interconnectedness multiplied the benefits from using digital technologies, they also exposed critical activities to new threats. Digital security incidents affecting critical activities became a new potential cause of catastrophes at the national, regional and international levels.

Over the last ten years, digital dependency of critical activities has continued to increase. In industrial environments, previously isolated Operational Technologies and Industrial Control Systems (ICS) that detect or cause changes in physical processes are no longer isolated from Information Technologies. Digital transformation is further accelerating critical activities' digital dependency, with the generalisation of technologies such as big data, artificial intelligence, and the Internet of Things to support, for example, "smarter" cities, power grids and health systems. Operators of critical activities manage increasingly massive amounts of data, hardware, software, and network infrastructures that can never be considered entirely secure. These complex and dynamic digital ecosystems increase operators' digital attack surface and exposure to digital security threats.

At the same time, **digital threats have grown in number and sophistication.** While robust quantitative evidence is scarce in this area, qualitative empirical evidence is clear. Malicious actors are increasingly innovative and have access to more sophisticated tools than ten years ago. Geopolitical tensions extend to the digital environment, adding States to the list of possible digital security threat sources. Security researchers repeatedly identify sophisticated new malicious code ("malware") specially designed to target critical activities, such as Havex, DragonFly, Black Energy, Grey Energy, Triton, and Industroyer[2], to name a few. The possibility for digital security incidents to create physical damages is no longer theoretical: the Stuxnet worm, discovered in 2010, destroyed nuclear centrifuges in Iran, and digital

1 This explanatory note was prepared by the Secretariat. The opinions expressed and arguments employed in this explanatory note do not necessarily reflect the official views of OECD Member countries.

2 www.techrepublic.com/article/how-the-triton-malware-shut-down-critical-infrastructure-in-the-middle-east/ and www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

security attacks generated massive physical damages in a German steel mill in 2014[3], as well as power outages in Ukraine in 2015 and 2017. Furthermore, the NotPetya incident in 2017 demonstrated the possibility for digital security attacks to significantly disrupt operations and supply chains for several days in areas such as global containers logistics (Maersk) and pharmaceutical production (Merck)[4].

This combination of increased digital dependency of and threats to critical activities presses governments to adopt **policies that strengthen digital security of critical activities without undermining the benefits** from digital transformation in critical sectors with constraints that would unnecessarily restrict the use and openness of digital technologies.

In 2008, the OECD adopted the first international legal instrument addressing this issue, the *Recommendation on the Protection of Critical Information Infrastructure* (CIIP) ("CIIP Recommendation") [OECD/LEGAL/0361]. It complemented the 2002 OECD *Recommendation concerning Guidelines for the Security of Information Systems and Networks* ("Security Guidelines") [OECD/LEGAL/0312] which was updated and replaced in 2015 by the *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* ("Security Risk Recommendation") [OECD/LEGAL/0415].

The *Recommendation on Digital Security of Critical Activities* ("Recommendation") **updates and replaces the 2008 CIIP Recommendation**. It was developed to *i)* modernise the core concepts to ensure coherence with the 2015 Security Risk Recommendation; *ii)* clarify the scope of this policy area, including where it stands within the broader landscape of digital security policy and national risk management / critical infrastructure protection policy[5]; and *iii)* take into account changes since 2008 as well as the experience acquired by countries in implementing policies in this area.

Scope

The Recommendation provides guidance on how to implement the 2015 Digital Security Risk Recommendation to maintain the continuity, resilience and safety of critical activities without inhibiting the benefits from digital transformation. It also clarifies how this public policy area relates to broader national risk management/critical infrastructure protection policy.

The scope of the Recommendation represents an evolution from CII to "critical activities". The concept of CII was built upon the then relatively recent concept of critical infrastructure, a term used by governments since the late 1990s to describe assets that are essential to the functioning of a society and economy. Policies to protect critical infrastructure typically consider critical infrastructure sectors such as energy, finance or public health. In 2008, a key objective was to raise awareness of the need to develop policies to protect information systems and networks that support such critical infrastructure sectors. It seemed natural to call these ICT assets "critical information infrastructure", as if they formed an additional critical infrastructure sector. The 2008 CIIP Recommendation successfully achieved that objective.

The review of the 2008 CIIP Recommendation initiated in 2016 showed that, although useful at the international level and well recognised by subject matter experts, the concept of CII has however rarely been used to develop domestic policy frameworks. This may be due to the difficulty to delineate CII in practice. For example, the internet can be considered as being part of the CII because most operators of other critical infrastructures rely on it, such as banks, hospitals or energy distributors. However, these operators also rely on their internal critical information systems and networks, which therefore are also part of the CII. Such information systems and networks may be owned and managed by the operators of

3 www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/ and https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

4 www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ and www.fiercepharma.com/manufacturing/merck-has-hardened-its-defenses-against-cyber-attacks-like-one-last-year-cost-it.

5 Countries have different approaches to how they protect critical activities, which are often called critical infrastructure protection or national risk management policies.

critical infrastructure themselves. But they may also include building blocks which are "in the cloud", i.e. on the Internet, and owned and managed by third parties, potentially in other jurisdictions. This combination of shared and isolated, as well as internal and external technical components makes the critical information infrastructure difficult to represent and more complex than the more traditional "critical infrastructure" sectors upon which the CII concept was inspired.

Furthermore, the concept of CII gives the false impression that critical information infrastructure protection is a separate area from critical infrastructure protection. Most importantly, it is no longer aligned with the OECD approach to digital security which has evolved from the security of technical assets (i.e. information systems and networks) to the security of the economic and social activities that rely on them (i.e. the delivery of energy or emergency health services). This evolution was one of the main achievements of the 2015 Security Risk Recommendation. The shift from CII to critical activities ensures consistency of OECD guidance in this area with the 2015 Security Risk Recommendation.

Critical activities refer to economic and social activities the interruption or disruption of which would have serious consequences on the health, safety, and security of citizens; or the effective functioning of services essential to the economy and society, and of the government; or economic and social prosperity more broadly. The latter type of critical activities represent an important evolution from the 2008 concept of CII. It includes economic and social activities 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, car manufacturing or mining, in a country where such activities would represent a significant share of the GDP.

Terminology

The Recommendation provides a coherent semantic framework to understand how to approach digital security of critical activities. Using this terminology in domestic policies would likely facilitate international co-operation. However, the Recommendation recognises that Adherents may use different terminologies in their policies to enhance digital security of critical activities. This results from the observation that the terms used by governments in this area are often inherited from broader national risk management / critical infrastructure frameworks, which address all risks to critical activities. For example, some countries use the terms "function" instead of "activity", "essential" or "vital" instead of "critical", etc. Prescribing the Recommendation's terminology might therefore undermine consistency between domestic policies to enhance digital security of critical activities and domestic national risk management / critical infrastructure protection frameworks. This could increase confusion and contradict the very objective of the Recommendation to increase coherence between these highly related policy areas. Similarly, the scope of "critical activities" used in domestic policies is likely to be inherited from a broader national risk management / critical infrastructure framework and can be formulated differently from the Recommendation. For example, it may be broader, narrower, or include references to national security, and may be used for other purposes than digital security.[6]

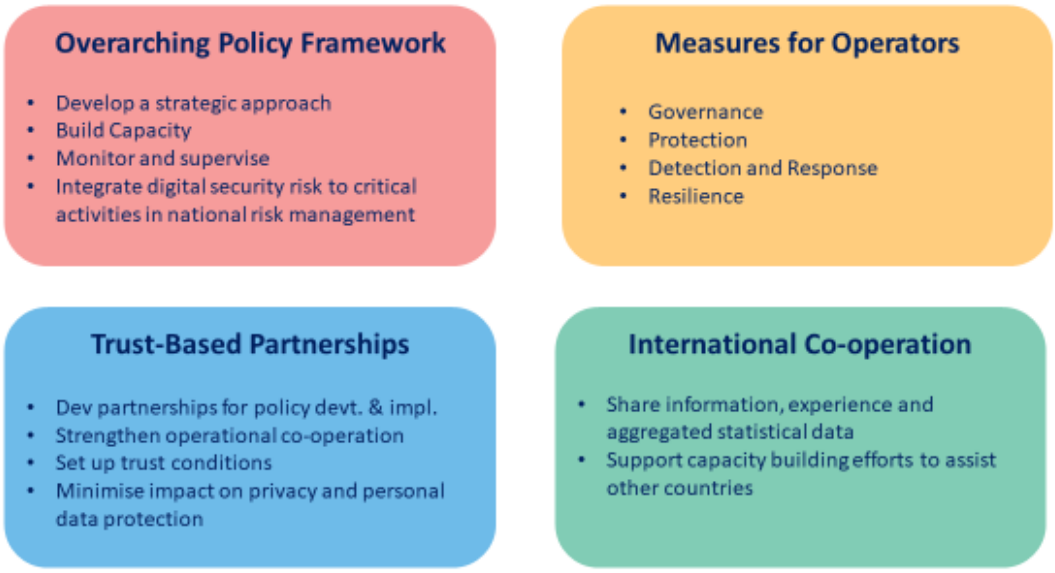
Consistent with the 2015 Security Risk Recommendation, the Recommendation uses "digital security" rather than "cyber security" in order to underline that digital security is an economic and social risk management challenge and to provide consistency with other expressions such as digital technologies, digital economy, and digital transformation.

6 For example, in the United States, "critical activities" are currently called "critical functions" and defined as "the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof". Executive Order on Coordinating National Resilience to Electromagnetic Pulses, 26 March 2019. www.whitehouse.gov/presidential-actions/executive-order-coordinating-national-resilience-electromagnetic-pulses/. See also www.dhs.gov/cisa/national-critical-functions.

Key building blocks

The Recommendation provides guidance on the overarching policy framework to enhance digital security of critical activities, the measures that governments should encourage operators to take, the establishment of partnerships and strengthening international co-operation (Figure 1).

Figure 1. Key building blocks of the Recommendation on Digital Security of Critical Activities



Source: OECD

The **overarching policy framework** should be rooted in both a national digital security strategy and a national risk assessment, and include a domestic governance mechanism. Domestic co-ordination is particularly important to ensure consistency of digital security policies with existing regulations in critical sectors (e.g. energy, bank or health regulation). As part of this overarching framework, governments should build capacity to support digital security risk management and resilience of critical activities. This includes developing a new or strengthening an existing incident response capability through a computer security incident response team (CERTs/CSIRTs) or Security Operation Centre (SOCs), or several of them operating for example by sector. It also includes enhancing digital security of critical digital services by the government, promoting international standards (including regional ones such as those of the European Union), and supporting operators, as appropriate.

Operators should be responsible for the management of digital security risk to critical activities that they operate.

A **funneling process**, based on a national risk assessment carried out as part of a critical infrastructure protection / national risk management framework, aims to ensure that policies targeting operators of critical activities focus on what is critical for the economy and society without imposing unnecessary burdens on the rest.

This process should take place as follows, on the basis of a national risk assessment covering all economic and social activities:

- The government, working with relevant public and private actors, identifies:
  1. *Critical activities*;

2. The *operators* of these critical activities;

- Operators of critical activities:

3. Conduct cyclical enterprise risk management to identify the functions without which they could not effectively carry out their critical activities ("*critical functions*");

4. Map their "*digital ecosystem*", i.e. the digital environment that supports their critical functions along the value chain of critical activities;

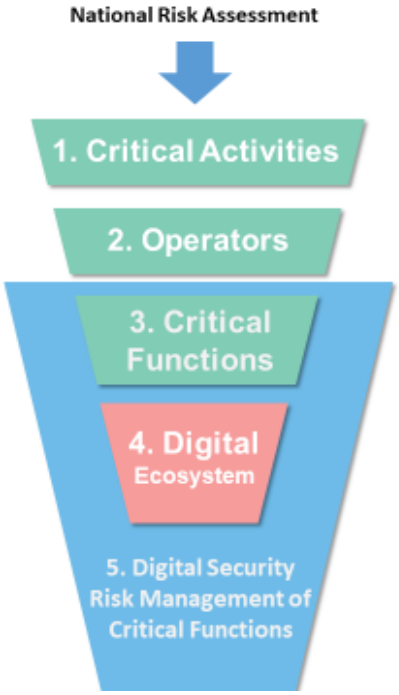
5. Conduct cyclical *digital security risk assessments of critical functions*, taking into account their digital ecosystem, and determine on that basis the level of digital security risk to be reduced, transferred, avoided, and accepted ("*risk treatment"*) and the digital security governance measures as well as those to protect the activities, detect and respond to incident and establish resilience.

The first three steps of this process, which are part of a broader national risk management and critical infrastructure protection policy framework, are not addressed by the Recommendation, which focuses on digital security. Mentioning them however is essential to ensure that steps four and five are aligned with national risk assessment and do not generate unnecessary burden to operators.

Considering an activity as being critical according to this Recommendation will create additional constraints for its operators and could affect their competitiveness on the global market. Therefore governments often co-operate with these operators and other stakeholders in steps one and two, and more generally in the policy making process, to best balance progress in digital security with economic and social performance.

Step four introduces the notion of "digital ecosystem", which is broader than information systems and networks considered in the 2008 CIIP Recommendation, and includes digital assets such as hardware, software, networks and data, operational technologies that detect or cause changes in physical processes (often called "OT" as opposed to the more classic IT, i.e. "Information Technologies"), as well as the internal and external entities, persons and processes that design, maintain and operate them, and the relationships between them. Step four is a prerequisite for step five, where operators manage digital security risk as called for in the 2015 Security Risk Recommendation, i.e. as part of their broader enterprise risk management framework and overall economic and social decision making processes (Figure 2). The Recommendation provides however more detailed guidance on the governance, protection, detection and response, as well as resilience measures they should put in place, a categorisation which is consistent with both the United States (US) National Institute of Standards and Technologies (NIST) Cybersecurity Framework and the European Union (EU) Network and Information Security (NIS) Coordination Group Reference Document on Security Measures for Operators of Essential Services.

Figure 2. Funnelling process to focus strengthened digital security on critical functions



Source: OECD

The Recommendation recognises that the multiplicity and complexity 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 the benefit of all. Each actor is therefore dependent upon and responsible towards all others to manage digital security risk. To ensure that digital security risk management of critical activities appropriately takes account of such dependencies, the Recommendation calls for the establishment of sustainable **public-public, public-private and private-private partnerships** across sectors and borders, through which partners would share risk-related information, as well as experience and good practice on digital security risk management.

Considering the sensitivity of the information to be exchanged, **partnerships need to be based on trust**. The Recommendation provides a general list of conditions to establish trust with a view to enabling sustainable public-public, public-private and private-private partnerships. These conditions include the need for clear aims, values and rules, mutual benefits over time, respect for privacy and personal data protection regulation as well as other regulation protecting the confidentiality of information such as trade secret. In particular, it is important that partners ensure that the information they receive from other partners will only be used for defensive purposes and is managed in a manner consistent with regulations protecting personal data and other information such as trade secrets. Additional conditions, including for specific types of partnership (i.e. public-public, public-private, private-private) may also be needed.

Last, the Recommendation recommends that Adherents strengthen **international co-operation** by sharing information on government bodies and other relevant stakeholders in charge of digital security risk management of critical activities, experience on the development of policies and aggregated statistical data from incidents; as well as by supporting capacity building efforts of other countries, as appropriate.

About the OECD

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD Member countries are: Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Legal Instruments

Since the creation of the OECD in 1961, more than 500 legal instruments have been developed within its framework. These include OECD Acts (i.e. the Decisions and Recommendations adopted by the OECD Council in accordance with the OECD Convention) and other legal instruments developed within the OECD framework (e.g. Declarations, international agreements).

All substantive OECD legal instruments, whether in force or abrogated, are listed in the online Compendium of OECD Legal Instruments. They are presented in five categories:

- **Decisions** are adopted by Council and are legally binding on all Members except those which abstain at the time of adoption. They set out specific rights and obligations and may contain monitoring mechanisms.

- **Recommendations** are adopted by Council and are not legally binding. They represent a political commitment to the principles they contain and entail an expectation that Adherents will do their best to implement them.

- **Substantive Outcome Documents** are adopted by the individual listed Adherents rather than by an OECD body, as the outcome of a ministerial, high-level or other meeting within the framework of the Organisation. They usually set general principles or long-term goals and have a solemn character.

- **International Agreements** are negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.

- **Arrangements, Understandings and Others**: several other types of substantive legal instruments have been developed within the OECD framework over time, such as the Arrangement on Officially Supported Export Credits, the International Understanding on Maritime Transport Principles and the Development Assistance Committee (DAC) Recommendations.