

OECD work on digital security policy

As the digital transformation accelerates, our economies and societies are increasingly vulnerable to cyberattacks that can harm organisations' assets, reputation and competitiveness. Such attacks may even result in companies shutting down and, with the development of the Internet of Things (IoT), threaten human safety. The surge of ransomware attacks is the most recent illustration of this trend, affecting in 2021 operators of critical activities such as gas distribution (Colonial Pipeline in the United States) and healthcare (Health Service Executive in Ireland). The global cost of cyberattacks is estimated from USD 100 billion to USD 6 trillion annually, and is rising every year.

Effective digital security policies are essential for growth and well-being

The OECD provides a unique forum to develop and promote evidence-based policy analysis and advice to **strengthen security and trust, without inhibiting the benefits of the digital transformation** and its potential to increase well-being, innovation and growth. The OECD has been at the forefront of facilitating international co-operation on digital security policy since the 1990s. The OECD focuses on the economic and social aspects of cybersecurity, as opposed to aspects that are purely technical, directly related to criminal law enforcement or national security.

The OECD approach to digital security is grounded in **risk management** and focuses on **identifying the most effective policy tools** to address the economic and social challenges that often limit the ability of stakeholders to optimally manage digital security risk. These challenges include, for instance, a shortage of skills and talent, a lack of digital security innovation, unclear assignment of roles and responsibilities to economic actors, misaligned market incentives, information asymmetries as well as the cultural and legal barriers to effective co-operation across borders and stakeholder groups. OECD's work on digital security policy:

- Is carried out through the **Working Party on Security in the Digital Economy (SDE)**;
- Builds on the outcomes of the **Global Forum on Digital Security for Prosperity**; and
- Supports the development of **OECD Recommendations** on digital security policy.

The Working Party on Security in the Digital Economy (SDE)

The SDE was established in 2019 as a working party of the OECD Committee on Digital Economy Policy (CDEP). Since January 2022, it is chaired by Florian Schütz (Switzerland).

The SDE develops **evidence-based policy analysis and advice** through discussions amongst delegates from the 38 OECD Member countries. It also gathers **multi-stakeholder input** from various communities, including informal expert groups and the following stakeholder groups: Business@OECD, the Internet Technical Advisory Committee (ITAC), and the Civil Society Information Society Advisory Committee (CSISAC). The SDE current work programme focuses on:

- Enhancing the **security of products and services**, including **supply chain** and the **IoT**.
⇒ Two [reports](#) and a [policy brief](#) (also available in [French](#)), published in 2021.
- Encouraging **vulnerability treatment**, including the protection of security researchers responsibly disclosing vulnerabilities (e.g. **safe harbours**).
⇒ Two [reports](#) and a [policy brief](#) (also available in [French](#)), published in 2021.
- Enhancing the **security of communication networks**, at the infrastructure (e.g. **5G security**, open RAN and virtualisation) and protocol levels, including the security of **routing** and of the Domain Name System (**DNS**). This work is carried out jointly with the CDEP Working Party on Communication Infrastructures and Services Policy (CISP).
⇒ Three reports are due to be published in 2022.

The Global Forum on Digital Security for Prosperity



Launched in 2018, the OECD Global Forum on Digital Security for Prosperity holds international multi-stakeholder events gathering **policy makers and experts** from the private sector, the technical community and civil society.

Outputs from these thematic discussions influence international public policy discussions and can lead to the development of analytical work, principles and policy guidance, both at the OECD and in other international fora. Since 2018, Global Forum events focused on:

- **Roles and responsibilities of actors** (hosted by **France** in 2018);
- **Encouraging digital security innovation** (hosted by the **United Kingdom** in 2019);
- **Building cyber resilience together in a post-COVID-19 world** (hosted by **Israel** in 2021);

Japan will host the next Global Forum event in 2023, focusing on “**Artificial Intelligence and other emerging technologies: a new frontier for digital security**”, followed by **Korea** in 2024.

More about the [Global Forum on Digital Security for Prosperity](#).

OECD Recommendations on Digital Security

Since the 1990s, the OECD has developed a set of [legal instruments](#) (*OECD Recommendations*) on digital security – with others currently being developed:

- Guidelines on [Cryptography Policy](#) (1997), to be reviewed in 2022-23;
- Recommendation on [Digital Security Risk Management](#) (2015);
- Recommendation on the [Digital Security of Critical Activities](#) (2019);
- Draft Recommendation on the **Digital Security of Products and Services** (expected Q4 2022);
- Draft Recommendation on **Vulnerability Treatment** (expected Q4 2022);
- Draft Recommendation on **National Digital Security Strategies** (expected Q4 2022);

The forthcoming OECD **Policy Framework on Digital Security** will provide a concise and coherent overview of the OECD’s approach and standards in this area (Q4 2022).

About the OECD

Founded in 1961, the Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organisation whose purpose is to promote “better policies for better lives”. It gathers 38 Members around shared values, in a commitment to democracy, human rights and market economy.

The OECD works towards establishing evidence-based international standards and finding common solutions to key global challenges. OECD committees and working parties bring together delegates from its Member countries to discuss emerging trends on a variety of topics, from taxation regimes and insurance policies to climate change and the digital transformation. This “whole-of-government” perspective is unique in the international landscape.

More about the [OECD](#).