Fifth Event

# Joining policymaking and technical communities to strengthen digital security: open source, supply chains & zero trust

**10-11 July 2024 – Swiss Grand Hotel, Seoul, Korea (hybrid)**

**Hosted by Ministry of Science and ICT (MSIT)**

**Sponsored by Korea Internet & Security Agency (KISA)**

## The OECD Global Forum on Digital Security for Prosperity

- Aims to consolidate a global network of experts and policy makers;
- Facilitates regular sharing of experiences and good practice on digital security risk and its management, mutual learning and convergence of views on core thematic issues;
- Is an international multilateral, multi-stakeholder and multidisciplinary setting for all communities of experts to meet, network and influence digital security public policy making;

The Inaugural Event of the Global Forum took place in 2018. Summaries of that Event and others that have taken place since then can be found at https://oe.cd/gfdsp.

## Contact

This is an invitation-only event. For more information, please contact: digitalsecurity@oecd.org

# DRAFT AGENDA

All times are KST (Seoul)

## DAY 1: Wednesday, 10 July 2024

| | |
|---|---|
| **14:00** | Registration |
| **14:30 – 14:55** | Welcome remarks |

### Theme 1 – Open-source software: opportunities and challenges

Fundamentally based on collaboration, open-source software (OSS) has particular implications for digital security, in terms of both strengths and limitations. However, these are not sufficiently understood by policy makers. Recognising the considerable importance of OSS today, this theme will aim to inform policy makers about OSS security opportunities and

challenges and discuss how policy makers can best ensure that cybersecurity policies fully take OSS specificities into account to best reduce digital security risk.

This theme will offer an opportunity to engage in a dialogue between experts from open-source communities and digital security policy makers in which they share views on how open-source approaches can best contribute to addressing current digital security challenges.

| | |
|---|---|
| | **Keynote speech** |
| **14:55 – 15:10** | The keynote speech could introduce the importance of open-source software (OSS) in today's digital environment, explaining how OSS supports digital security and why the security of OSS is critical for trust across all our digitally dependent economic and social activities. |

| | |
|---|---|
| **15:10 - 15:55** | **Session 1 – Security-by-design and OSS** |

Security-by-design is an approach that seeks to build security in products and services from the outset and throughout their lifecycle rather than as an afterthought, while maintaining the capacity to innovate and adapt to an ever-changing threat landscape. Following OECD Recommendations in this area, policy makers encourage its adoption by industry to reduce digital security risk, building on existing methodologies and standards such as the Secure Development Lifecycle. However, it is unclear how OSS projects can implement security-by-design. This session will explore the opportunities and challenges related to security-by-design in OSS.

**Key guiding questions include:**

- What are the opportunities and limitations of OSS projects with respect to security-by-design?
- How does the OSS model mitigate software security lifecycle challenges such as the unmaintained and outdated products as they reach end-of-life or end-of-support?

| | |
|---|---|
| **15:55 – 16:10** | **Coffee break** |

| | |
|---|---|
| **16:10 – 16:55** | **Session 2 – Open-source software and vulnerability treatment** |

When it comes to vulnerabilities, both proprietary and open-source software face the same reality: the more complex the code, the more vulnerabilities there are, and despite all efforts to secure the code by design, some vulnerabilities still remain, as explained in recent OECD work. The solution to software vulnerabilities is their detection and resolution, including through vulnerability treatment and co-ordinated vulnerability disclosure (CVD), a collaborative process involving all stakeholders, from security researchers (detection, disclosure) to software editors (vulnerability handling and resolution) and users (patching and vulnerability management). In 2022, the OECD recommended the adoption of public policies to encourage vulnerability treatment. This session will explore the specificities of OSS with respect to vulnerability treatment, and the unique characteristics of its ecosystem.

**Key guiding questions include:**

- What opportunities does the open-source model create for vulnerability treatment?
- What challenges does the open-source model create for vulnerability treatment?

| | |
|---|---|
| **18:00 – 20:00** | **Reception hosted by Korea** |

# DAY 2: Thursday, 11 July 2024

## Theme 2 – Collaboration for more secure and resilient supply chains

Across all sectors, supply chains are increasingly relying on increasingly complex cross-border digital ecosystems to support their economic and social activities. All organisations taking part in supply chains are interconnected and therefore, from a digital security standpoint, they are also all interdependent. This means that the security of all partners is aligned with the security of the weakest of them.

This theme will provide an opportunity for industry, policymakers, and stakeholders from civil society to highlight considerations regarding supply chains and Managed Service Providers and to discuss possible measures, including zero trust, that the international community can take to embed resilience within global supply chains that support economies.

| | |
|---|---|
| **9:30 – 9:45** | **A case study on digital security in the supply chain**<br><br>**Keynote speaker**: TBD. |

| | |
|---|---|
| **9:45 – 10:45** | **Session 3 – Managed Service Providers (MSPs): the weakest link in the supply chain?** |

The 2020 attack that leveraged vulnerabilities of the MSP SolarWinds showed how devastating a supply chain attack can be, including through cascading effects affecting other managed service providers down the supply chain, including some of the most well-known cybersecurity firms. This attack also showed that the weakest link is not necessarily the smallest or the least secure partner. MSPs play an increasingly important role in the maintenance and operation of today's information systems in organisations of all sizes. But at the same time, as MSPs are becoming critical in the supply chain, they are also becoming a prime target for malicious actors. MSPs can turn out to be the weakest point in the chain of security, leading to massive downstream incidents. This session will be an opportunity to discuss the criticality of MSPs and will bring together representatives from public and private organisations.

**Key guiding questions include:**

- What are the security challenges stemming from MSPs in supply chains?
- How do MSPs improve and, at the same, threaten digital security of supply chains?
- Should MSPs be regulated to enhance the digital security of supply chains?

| | |
|---|---|
| **10:45 – 11:05** | **Coffee Break** |

| | |
|---|---|
| **11:05 – 12:05** | **Session 4 – Zero trust: a panacea to increase security of supply chains?** |

Zero trust is increasingly being promoted as a new security paradigm to address the vanishing of digital security perimeters around organisations, including partners within supply chains. While in principle at least the migration to zero trust security offers a way to improve security quite radically, its cost/benefit is unclear, notably when considering usability, organisation, complexity, and other management aspects. Another issue related to zero trust is the extent to which it can enhance the security of supply chains in complex ecosystems with numerous partners, and how smaller partners who are not zero trust-ready (or cannot afford it) can nevertheless be included. This session will bring together technical and policy experts.

**Key guiding questions include:**

- Can the adoption of a zero trust approach improve security of supply chains?
- What challenges does a zero trust approach raise in supply chains?

| | |
|---|---|
| **12:30 – 14:00** | Lunch break |

## Theme 3 – Regulatory approaches in digital security

Many countries are developing digital security legislation and regulation, whether to protect critical activities and infrastructure, to enhance the security of products and services, or to improve vulnerability treatment.

These sessions would offer participants the opportunity to learn about approaches to developing and delivering security legislation that have proven successful. These can include the importance of monitoring and evaluation, how to generate legislative impact assessments and guidance on engagement or consultation on proposed legislative approaches.

This theme would present a unique opportunity for early adopter policymakers to share insight on their approaches, and the lessons that can be learned and applied by other policy makers seeking to deliver effective digital security laws.

| | |
|---|---|
| **14:00 – 15:15** | **Session 5 – Is more digital security regulation inevitable?** |

In an increasingly interconnected world, the need for robust digital security measures is undeniable. Yet the landscape is complex, with various sectors facing unique challenges. From critical infrastructure to the Internet of Things (IoT), cloud services, and the realm of certification and labels, the demand for regulation varies. This session will explore where regulation should become the norm to enhance digital security. It will also examine instances where self-regulation has shown promise, and yet sometimes faltered. Experts from governmental and private organisations will exchange views during the session.

**Key guiding questions include:**

- In which areas is digital security regulation already the norm? In which areas should it become the norm? (e.g., critical infrastructure, IoT, cloud, certification/labels)
- In which areas has self-regulation proven to be effective but sometimes ineffective, too?
- What is the right balance between compulsory regulation, voluntary regulation, and autonomy?

| | |
|---|---|
| **15:15 – 15:35** | **Coffee Break** |

| | |
|---|---|
| **15:35 – 16:20** | **Session 6 – How to stimulate and enhance collaboration?** |

Collaboration among countries, stakeholders, and sectors is paramount to effectively combat cyber threats, which are constantly increasing in intensity and complexity. The session will look at best practices and concrete examples from a variety of contexts. From government initiatives to industry partnerships and cross-sectoral collaborations, the session will analyse what works best to foster cooperation and strengthen digital security. This session will bring together representatives from governmental organisation, private companies, and civil society.

**Key guiding questions include:**

- What are the best practices and examples from different countries/ stakeholders/ sectors that could be put forward to enhance collaboration?
- What are the strategies for strengthening collective efforts in favour of digital security

| | |
|---|---|
| **16:20 – 16:30** | Closing remarks |

**Global Forum Web site:** oe.cd/gfdsp
**OECD works on Digital Security:** Digital security - OECD