Organisation for Economic Co-operation and Development

DSTI/DPC/DS(2024)8/FINAL

Unclassified

English - Or. English

27 January 2025

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
DIGITAL POLICY COMMITTEE

Cancels & replaces the same document of 23 January 2025

Working Party on Digital Security

Summary of the Fifth Event of the Global Forum on Digital Security for Prosperity: 10 – 11 July 2024

This document presents a summary of the fifth event of the Global Forum on Digital Security for Prosperity, which took place on 10-11 July 2024 in Seoul, Korea.
Moderators, speakers and delegates of the Working Party on Digital Security reviewed the draft. The Digital Security delegates then agreed to its transmission to the Digital Policy Committee. This paper was approved and declassified by the Digital Policy Committee on 21 November 2024 and prepared for publication by the OECD Secretariat.

Bénédicte Schmitt: benedicte.schmitt@oecd.org
Bora Kim: bora.kim@oecd.org
Jeremy West: jeremy.west@oecd.org
Marion Barberis: marion.barberis@oecd.org

JT03558725

Note by the Secretariat

This report provides a summary of the fifth event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum"), which took place on 10-11 July 2024 in Seoul, Korea. The report was drafted by the OECD Secretariat and reviewed by moderators and speakers.

This event was hosted by the Ministry of Science and ICT of Korea (MSIT) and sponsored by the Korea Internet & Security Agency (KISA).

The Secretariat wishes to thank MSIT, KISA, and all the moderators and speakers, as well as the Korean delegation to the OECD, who helped organise the event.

The Global Forum was launched in 2018 to foster sharing of experiences and good practice on digital security risk and its management, mutual learning, and convergence of views on core thematic issues related to digital security for economic and social prosperity. Its outputs feed OECD policy discussions and can lead to the development of analytical work, principles, and international policy recommendations.

Events are proposed by OECD delegations and organised by the Secretariat in co-operation with the host.

More information about the Global Forum and its events is available at https://www.oecd.org/en/networks/global-forum-on-digital-security-for-prosperity.html

Table of Contents

Executive Summary

The fifth event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum") was held on 10-11 July 2024 in Seoul and hosted by the Korean Ministry of Science and ICT (MSIT) and the Korea Internet & Security Agency (KISA). It brought together 158 invited experts from 16 countries, representing governments, business, civil society, and academic and technical communities, to share views on "Joining policymaking and technical communities to strengthen digital security: open-source, supply chains and zero trust". Participants discussed the following policy challenges, for which international cooperation is essential and the OECD built on its longstanding digital security expertise to facilitate a productive multistakeholder dialogue:

- **Security-by-design and open-source software (OSS).** Speakers noted that OSS security is often underexplored and highlighted the need to critically assess the viability of a security-by-design approach to OSS. Due to its transparent and collaborative nature, the traditional challenges related to the treatment of vulnerabilities and supply chain security require a new form of cooperation. The lack of resources to support the community of software engineers maintaining the OSS ecosystem is another challenge. Governance is crucial for OSS security, which may require an alignment of technical support and wider industrial policies. One of the policy options discussed was the adoption and further integration of Software Bill of Materials (SBOM) to increase the visibility of software components and to enhance the vulnerability management of their dependent components.
- **Leveraging open-source software for vulnerability treatment**. Speakers reaffirmed the importance of regular service monitoring to measure and observe the performance of a system, as well as automated vulnerability detection in ensuring digital security. Governments have published guidelines and guidance documents, both domestically and internationally, to establish procedures on vulnerability treatment, such as Japan's new SBOM guidance document that includes guidelines on vulnerability management, and the Quad cybersecurity senior group's "Joint Principles for Security Software". However, challenges remain, for instance, with regard to the protection of ethical security researchers. Speakers suggested that countries implement safe harbours with the support of international organisations such as the OECD.
- **Strengthening the role of managed service providers (MSPs) in the supply chain**. Despite the growing presence and integration of MSPs in the digital security of supply chains, they remain largely under-regulated so there is little oversight on these businesses. Speakers underlined that it is important to constantly educate and train MSPs to create buy-in from them to adopt appropriate security standards. Governments and non-profit organisations prepare a variety of tools beyond certifications that can help MSPs and their clients to increase their security. Regulations can also contribute to fostering a security mindset among MSPs.
- **Usefulness of the zero trust model for supply chain security**. The zero trust security model embodies the principle "never trust, always verify," rejecting the traditional perimeter-based approach to security in favour of a more granular and adaptive approach. Speakers mentioned that the zero trust approach offers clear advantages to both government entities and private companies

on a practical level. For governments, it is a more secure way to protect a country's critical assets by imposing more stringent rules and procedures. Companies can also employ zero trust principles to assess their digital security preparedness, for instance, during merger and acquisition processes. Nevertheless, the zero trust model is a paradigm rather than a single solution. Considering the model's restrictive nature, speakers advised that its application should be considered within limitations. A paradigm shift to zero trust cannot take place without sufficient support from governments. Public policies should address the potential changes in business models in companies as well as the accompanied costs.

- **Balancing regulation and flexibility to support security and innovation.** OECD countries are addressing digital security through a variety of regulatory frameworks, each tailored to their unique contexts and challenges. The discussion demonstrated that robust digital security requires a mix of regulatory measures and adaptable policies, not only to accommodate different levels of risk and resources across industries, but also to support industry dynamism and innovation.
- **Policy approaches to stimulate and enhance collaboration.** The discussions highlighted the importance of cross-sector and international collaboration for building a resilient digital environment. The effectiveness of such collaboration requires comprehensive and coordinated efforts across all levels of the private sector and government, including the regional and local levels, underpinned by trust, shared goals, and effective communication. The OECD could play a pivotal role in enhancing collaboration by setting unified goals, aligning policies and strategies across Member countries, promoting best practices, identifying legal barriers to information sharing, and reframing digital security as a broader risk management issue rather than a technical concern.

Introduction

This document provides a summary of the fifth event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum"), which took place in Seoul, Korea on 10-11 July 2024 with the support of the Korean government. The Global Forum brought together 158 experts from 16 countries' governments, businesses, civil society organisations, and academic and technical communities.

The event focused on three themes, each introduced by a keynote speech followed by two panels. These themes were:

- Open-source software: opportunities and challenges
- Collaboration for more secure and resilient supply chains
- Regulatory approaches in digital security

Each section of this report summarises the keynote speakers' presentations and the discussions held among panellists. The report does not necessarily reflect the views of the OECD Secretariat or of Member countries.

In addition to the summarised discussions, **Mathias Cormann**, OECD Secretary-General, and **Je-Myung Ryu**, Deputy Minister of the Office of Network Policy at the Ministry of Science and ICT, Korea, opened the Global Forum and welcomed participants with some scene-setting remarks. **Sang-Joong Lee**, President of KISA, welcomed the participants to the reception. **Audrey Plonk**, Deputy Director of Science, Technology, and Innovation, OECD, delivered closing remarks.

Open-source software: opportunities and challenges

Keynote speech

Christopher Hockings, Chief Technology Officer, IBM Security Asia Pacific

The keynote speech traced the Internet's evolution from an unsecured platform in the 1990s to a secure, commerce-enabled web. This transformation was driven by initiatives such as the development of open-source standards while managing software vulnerabilities and supply chain threats and exploring new security models such as zero trust.

Collaboration in open-source projects has been crucial to accelerating technological advancements, allowing experts to solve shared problems collectively. Open source is integral to enterprise software, with the private sector contributing significantly to open standards and open-source initiatives, which led to the development of widespread tools such as online authentication systems.

However, there are inherent risks in software development, including vulnerabilities in both open-source and proprietary systems. IBM launched a threat research team in the early 2000s to track them. A total number of 23,964 vulnerabilities were tracked in 2022 by the research team, compared to 21,518 in 2021. High-severity vulnerabilities, such as Heartbleed in 2018 and Log4J in 2021, pose significantly greater risks when embedded in widely used open-source software, requiring urgent resolution to prevent exploitation.

Mr. Hockings also considered supply chain threats that arise from vulnerabilities within the software components of a product. Attackers may exploit these weaknesses, leading to severe consequences like ransomware. The importance of tracking and managing these risks is underscored by industry's efforts to find adequate solutions such as the development of SBOM standards to manage risks across complex, multi-vendor technology environments. Public-private open project initiatives such as Protobom, an open-source tool to facilitate the development of SBOMs, or the Secure by Design Pledge supported by 17 public and private organisations, demonstrates a global commitment to enhance supply chain security (Open Source Security Foundation, 2024[1]), (CISA, 2024[2]).

Additionally, Mr. Hockings addressed the importance of implementing zero trust principles in modern, distributed technology architectures. Zero trust is a security model that assumes no implicit trust and requires verification at every stage. Implementing zero trust involves strong protection measures, real-time analytics, and immediate response mechanisms to detect and mitigate threats. Adopting an "assume breach" mindset is essential for successfully applying the zero trust model.

Security-by-design and Open-source software

Moderator: **Jeremy West**, Head of the OECD's Digital Security and Safety Unit

Panellists:

- **Rasma Araby,** Chief Operating Officer, Atsec Information Security AB
- **Allan Friedman**, Senior Advisor and Strategist, U.S. Cybersecurity and Infrastructure (CISA)
- **Robin Ginn,** Executive Director, Open JS Foundation
- **Heejo Lee**, Professor of computer science, Korea University
- **Elina Machefer**, Open source security programs lead, French Cybersecurity Agency (Agence nationale de la sécurité des systèmes d'information ANSSI)

The panel highlighted the importance of integrating security by design and leveraging OSS to enhance innovation and security. The discussion focused on the benefits and challenges of open-source software development, as well as the necessary steps for strengthening its security and resilience.

Security-by-design emphasises anticipating risks and incorporating security measures from the outset of product and service development, rather than addressing security problems post-development. Open-source software relies on collaboration and transparency to drive innovation, but these same qualities can present security challenges, including for the security-by-design approach.

The model behind security-by-design was conceived around large commercial, proprietary software and does fit the open-source domain very well. The high-level secure-by-design concept was originally spelt out in a joint document by 17 government agencies around the world and includes three pillars (CISA, 2023[3]). First, embracing radical transparency is essential, as it is impossible to secure what we are not aware of. Second, users should take ownership of security outcomes, meaning that they should understand the security risks of their devices. Last, leadership for increasing digital security should come from policy makers, who should devote time, expertise, and resources to it.

OSS security is often underestimated and misunderstood. Most users assume that open source equates to security and safety. Governance is crucial for OSS security, requiring adaptation of industrial policies to address open-source challenges. Technical support and industrial policies should be aligned to foster a consultative approach with the ecosystem.

Panellists raised the importance of government and industry collaboration on creating standards and promoting the adoption of SBOM. Implementing SBOM for visibility into software components is essential. While visibility alone does not eliminate risks, it enables proactive risk management and response.

Panellists also mentioned vulnerability treatment as a key challenge. While the transparency concept in open-source codes and projects facilitates peer reviews and vulnerability patching, it can be exploited by malicious actors when penetrating a system with sub-components that sometimes remain unpatched for years. Panellists also identified the lack of standardised naming conventions for vulnerabilities, as well as the high cost of securing OSS projects to avoid vulnerabilities, as another key challenge. Therefore, ensuring regular code reviews and security updates, and understanding software dependencies, are essential to enable vulnerability treatment.

Another challenge is supply chain security. Conducting risk assessments, maintaining a list of third-party components, and performing regular scans are crucial. Similarly, the end-of-life and end-of-support challenges for software components need to be addressed either by regulation or anticipation. Governments are increasingly developing regulations affecting the development and maintenance of OSS, such as the EU Cyber Resilience Act, to strengthen digital security and safety.

In addition to the technical challenges, the panellists highlighted the human aspect of OSS, pointing to the community of maintainers who support the open-source ecosystem for free with little support and consideration. As software projects grow in complexity, automation is an important way to help maintainers manage security effectively. Developing automated tools and best practices could aid maintainers in navigating regulatory requirements and ensuring secure code. Additional funding and training would help cope with this infrastructure fragility, which could put the OSS ecosystem at risk.

Eventually the speakers recalled that OSS security requires an international community effort because OSS is used globally, and by governments as well as critical industries. Vulnerabilities in OSS can therefore affect crucial systems and infrastructures worldwide, making it essential for developers, researchers, and organisations from different countries to collaborate in identifying and addressing security risks.

Open-source software and vulnerability treatment

Moderator: **Harry Toor,** Chief of Staff, The Linux Foundation

Panellists:

- **İsmail Erkek**, Advanced Cybersecurity Operations Coordinator, TR-CERT of the Information and Communication Technologies Authority of Türkiye (BTK)
- **Kyoungae Kim,** Open-source task team leader, LG Electronics
- **Melanie Rieback,** Chief Executive Officer and co-founder, Radically Open Security
- **Taketo Yamada**, Director for Cybersecurity Strategy, Ministry of Economy, Trade, and Industry of Japan

This panel examined the digital security challenges and opportunities presented by the widespread use of OSS. The panel recognised the new risks this development can bring because of untreated vulnerabilities, such as cyberattacks, phishing, data breaches, or cyber espionage. These threats pose serious challenges not only to individuals but also to states, making digital security an essential element of national security.

Panellists focused on the role of Computer Emergency Response Teams (CERTs) in developing effective defence mechanisms, highlighting strategies that include bolstering resistance to cyberattacks, managing vulnerabilities, and employing innovative solutions like big data to protect national data, critical sectors, and public institutions.

Service monitoring and automated vulnerability detection are also crucial components of digital security. The process of assigning Common Vulnerabilities and Exposures (CVE) codes to identified vulnerabilities is managed globally by 240 CVE Numbering Authorities (CNAs), who are responsible for informing users about these vulnerabilities and providing guidance on how to patch them. In Türkiye alone, 276 vulnerability notifications have been published, underscoring the ongoing efforts to mitigate cyber risks.

The discussion also addressed the increasing complexity of software development, with code often sourced from multiple origins. Panellists highlighted the introduction of SBOMs, which detail every component and module in a software product, as a promising solution for enhancing transparency and security. The need for SBOMs has grown with the proliferation of OSS, which allows developers to freely assemble diverse components. However, the panel noted challenges in implementing SBOMs, such as high costs and resistance from suppliers. Additionally, the lack of standardisation in software IDs and SBOM formats hinders the use of automated tools that could streamline its management.

In Japan, the 2022 Proof of Concept (PoC) explored the efficient and cost-effective use of SBOMs across industries like medical equipment, automobiles, and computer software (METI, 2023[4]). Following this PoC, Japan published an SBOM guidance document and later revised it to make it more accessible to organisations, including SMEs. The updated version, which includes new guidelines on vulnerability management, is set to be translated into English.

The panel also noted collaborative initiatives, such as the Quad cybersecurity senior group, comprising Australia, India, Japan, and the United States, which released the "Joint Principles for Security Software" in 2023 (Quad Senior Cyber Group, 2023[5]). This document aims to improve software security by establishing minimum cybersecurity guidelines for governments to follow in software development, procurement, and usage.

Speakers further highlighted the role of private companies in enhancing the security of open-source components. For example, LG, a Korean multinational conglomerate, has an in-house toolbox, "Free/Open Source Software that Shines a Light on the World" (FOSSLight) (LG Electronics, 2021[6]). It is a scanner that automates the analysis of a project's source code, binaries, and dependencies to identify any open-

source components. It also detects the licenses associated with these open-source components ("open-source compliance") to ensure that organisations avoid potential legal risks and use open-source software safely and responsibly. Another component of the FOSSLight suite is the FOSSLight Hub, which is an integrated management tool for open-source projects, including the detection and regular monitoring of vulnerabilities.

The session also touched on the challenges faced by security researchers, particularly the need for explicit permission to access and reverse-engineer codes. While penetration testing is valuable for improving security, obtaining the necessary permissions can often be time-consuming. The panel suggested that countries should implement safe harbours for ethical security researchers, providing legal safeguards for their work.

Additionally, speakers advocated the need for a shift in the business model of security companies towards the steward ownership model, which prioritises the companies' mission over short-term profits. Much of the current focus in cybersecurity is on profit generation rather than genuinely improving security. High costs of security devices also often prevent SMEs from accessing essential protections.

Despite the fact that OSS is often available for free, funding remains crucial for its development and maintenance. The European Commission's "Next Generation Internet" initiative is exemplary, having funded over 1,000 projects to date (European Commission, 2018[7]) The panel encouraged other organisations and countries to develop similar funding models to support open-source projects.

Finally, panellists emphasised the importance of rewriting code in memory-safe languages, which are designed to prevent various software bugs and security vulnerabilities, as a proactive measure to ensure more stable software development.

Collaboration for more secure and resilient supply chains

Keynote speech

Ryan Ko, Chair and Director, UQ Cyber, University of Queensland

The SolarWinds incident in 2020 elevated cybersecurity to a core consideration for many entities. The software update itself, which was supposed to prevent cybersecurity attacks and breaches, was the main factor that compromised much larger supply chains. Many countries responded by leveraging public-private collaboration to encourage reviews of cybersecurity systems within organisations and the adoption of relevant legislations. At the same time, this incident raised many critical questions such as: how do we prevent this from happening again? Is verifying every software update achievable in a dynamic environment? Is it viable for all kinds of organisations and businesses regardless of their size and maturity?

For SMEs, the situation appears more challenging. The SolarWinds incident and its impact involved only a small segment of the economy and given that 94.5% of companies in OECD countries are small or medium-sized, the lessons learned cannot be universally applied across all businesses. For example, suppliers often demonstrate compliance through certifications, which can require filling out extensive compliance spreadsheets that may need a full-time employee's dedication. However, not all companies have the resources to hire a dedicated staff member for this task.

Against this setting, Professor Ko identified several levers for change that can raise cybersecurity awareness among firms. One is effective regulation. The United States' Federal Information Security Modernization Act (FISMA) is an illustration of domestic regulations having a global impact. The Act sets the legal requirements for US federal agencies' compliance with policies developed by the National Institute of Standards and Technology (NIST). This Act creates a cascading effect, as the MSPs that have business relationships with these agencies must also comply with these requirements. Furthermore, as some of these providers are multinational, the increased use of NIST's compliance platform has contributed to raising the security maturity level across countries.

Professor Ko also emphasised the need for understanding the profitability incentives of SMEs, which typically outweigh security considerations. He referred to a study conducted by Mastercard of 1,000 Australian SMEs and their employees. The study found that their top three priorities are revenue-driving activity, client relationships, and growth. Cybersecurity is seen as a non-revenue-generating activity, often taking a backseat. According to the Australian Signals Directorate SMEs spend an average of AUD 500 per year on cybersecurity (ASD, 2023[8]). Increasing short term financial pressure sometimes forces SMEs to scale down their activity and reduce their spending on cybersecurity.

In an attempt to re-align SMEs' business priorities, policies should create incentives for businesses acting in their self-interest to inadvertently contribute to the public good, in this case, improving the levels of digital security. The speaker introduced the case of Cyber Security Certification Australia and its "SMB1001" standard, a multi-tiered cybersecurity certification standard comprising five levels to support the development of cyber hygiene. Uptake was slow until MSPs identified the certifications as an "independent triage" that could help them assess the security levels of their products and services more easily (CSCAU, 2024[9]). As MSPs quickly certified themselves, the standards adopted naturally helped raise their clients' cybersecurity levels at scale.

On the client side, security should be "made implicit". Businesses and individual customers often want to enjoy services without paying particular attention to the security aspects. Some may advocate the zero trust approach, a more granular and adaptive view towards security than the traditional perimeter-based model in which an organisation's network is protected by securing its edges or boundaries based on the assumption that there exists a clear distinction between internal, trusted networks and external ones. This again may raise the question of whether the zero trust approach is practical and applicable to all businesses.

Finally, policies and technologies should be "achievable". Businesses, especially smaller ones, should benefit from easy gains and achievable steps, and be catalysed by incentivised stakeholders.

Managed Service Providers (MSPs): the weakest link in the supply chain?

Moderator: **Allan Friedman**, Senior Advisor and Strategist, U.S. Cybersecurity and Infrastructure Agency (CISA)

Panellists:

- **Dan Yock Hau,** Assistant Chief Executive, Cyber Security Agency of Singapore
- **Young Hoon Kim**, Director of Public Policy for Japan and Korea, Amazon Web Services (AWS) Korea
- **Marissa Maldonado,** Chief Executive Officer, Proda Technology
- **Harry Toor**, Chief of Staff, The Linux Foundation

This session opened with a critical question: *why* cybersecurity should be a top priority for SMEs. This naturally sheds light on the role of MSPs, in which SMEs place their confidence by delegating technically complex security issues to them so that the SMEs can focus on creating revenues.

Trust is not security. Trust is earned by participating in the security ecosystem and adopting security tooling and best practices. The fundamental problem lies in the current market structure for MSPs, which largely remains unregulated with practically no controls on who can identify themselves as MSPs. This means that not all MSPs are created equal, and the quality and standards of services provided can widely vary. The point on trust becomes more apparent in comparisons between MSPs and cloud service providers (CSPs). CSPs provide essential infrastructure, platform, and software tools that organisations can access to support their IT environments whereas MSPs take on a more operational role. Besides, while CSPs are usually bound by more stringent regulatory standards, certifications, and requirements to provide transparent reporting and monitoring, MSPs are not obliged to adhere to certification standards or to earn accreditation.

The panellists noted several recent trends in the MSP market that can expand security loopholes or create new ones. The first trend is the rapid consolidation of the MSP landscape. The second trend is the rise of cybersecurity agendas among SMEs. Insurance companies have become a catalyst for more security due to the growing number of claims they received and the resulting sums they paid out due to cyberattacks since 2020. Consequently, they are strongly encouraging MSPs to take cybersecurity into consideration to continue benefiting from insurance coverage.

In this context, it is important to provide ongoing education and training for MSPs. Various initiatives aim to develop a security accreditation framework for MSPs by integrating established standards, such as the NIST and Centre for Internet Security (CIS) controls framework, with guidelines created by non-profit organisations and aligning with broader trends in government regulations. In addition, it is important to create buy-in from MSP communities in order for these accreditation frameworks to be useful.

Greater awareness of digital security can also be raised among MSPs by educating them with appropriate tools. A variety of such tools to ensure the security of software artifacts, products, and open-source repository already exist. These tools can also help to communicate security levels to consumers. MSPs can also leverage these tools to expand the security awareness of the SMEs with which they are engaging. Furthermore, the tools have to be complemented by mentioning and referencing of best practices, particularly in government documents, to be effective. Lastly, the use of tools should be complemented by other efforts to raise the overall security levels of MSPs.

Another way to infuse a security mindset into MSPs is through effective regulation. Regulation cannot be the lever of first resort since regulating the market from the very start may stifle its growth. When complemented by other means, regulation can help increase the level of cybersecurity in an organisation. For instance, chief information security officers (CISOs) often face substantial barriers when trying to

secure adequate cybersecurity resources since, by their very nature, such investments do not bear fruit until an incident occurs. In this regard, regulations can help them communicate the importance of cybersecurity by enabling them to refer to the compliance requirements.

Zero trust: a panacea to increase security of supply chains?

Moderator: **Melanie Rieback,** Chief Executive Officer and co-founder, Radically Open Security
Panellists:

- **Aviram Atzaba**, Executive Director for International Strategic Affairs, Israel National Cyber Directorate (INCD)
- **Eunsu Jeong,** Director of Cyber Security Industry Division, MSIT
- **Clément Rouault,** Chief Technology Officer and co-founder, ExaTrack
- **Florian Schütz**, Chair, OECD Working Party on Digital Security and Director, Federal Office of Cyber Security of Switzerland

The zero trust security model was mentioned during the 2021 Global Forum as one solution to the disappearance of security perimeters (OECD, 2021[10]). It was considered as a way both to level up and to simplify the types of security measures that are available to organisations.

The zero trust model compels digital security stakeholders to rethink the notion of "trust". The model calls for an allocation of additional resources for verifying everything that attempts to connect to a system, which may overshadow other business operations that require certain levels of trust, too. For instance, in the e-commerce industry, a 20-millisecond delay due to authentication requirement can lead to 1% less sales revenue. This means that some industries may consider trust as a lower priority.

On a practical level, the zero trust model offers clear advantages to government entities when considered within its limitations. For governments, it can be a more secure way to manage a country's critical infrastructure (CI) and supply chain as it forces constant adaptation. Over the last two decades, the Israel National Cyber Directorate (INCD), as the regulator of CI, has incorporated many security components that can together be considered as a zero trust approach, including network segmentation and screening of critical employees. At the same time, it acknowledges that the model can be implemented selectively for critical sections and that tailored risk assessment is crucial for sectorial business continuity.

From a supply chain point of view, zero trust principles can be useful for private companies when assessing their security levels. For instance, merger and acquisition processes are often abused by malicious actors, as the information is quickly made public and the information security side of it is often considered a minor detail that can be adapted months later. Therefore, the zero trust approach can help the acquirer determine whether the target company has a mature enough approach to digital security and whether its security has previously been compromised. However, the approach needs to be balanced with other considerations, such as the timing of the migration to the zero trust model and its affordability. Victims of ransomware attacks, for instance, are not advised to migrate to the zero trust model immediately, but rather to start upgrading their security level starting from the attackers' entry points. This is because the zero trust model requires a lot of resources that cannot always be tapped into within a few weeks during crises.

Paradigm shifts to the zero trust model cannot take place without sufficient government support. If an industry already has an established architecture, the zero trust model may mean changing fundamental aspects of businesses. Rather than proceeding directly to advocating the model, it is therefore crucial to first examine the companies' business processes and to conduct a risk analysis to determine whether introducing the zero trust model will significantly disrupt the existing business flow. On the other hand, if an industry sector is highly regulated, adopting zero trust principles can improve the companies' regulatory compliance, which in turn can be a more cost-saving way to run businesses. Policymakers can help businesses by providing national guidelines and tailored support. For instance, the Ministry of Science and ICT of Korea (MSIT) published its first national Zero Trust Guidelines 1.0 (MSIT, 2023[11])to help the public sector and corporate stakeholders understand the model's fundamental concept and ran pilot projects in which it funded consortia of supplier and customer companies in the cloud industry. Based on the lessons learned, MSIT plans to publish the Guidelines 2.0 this year.

Regulatory approaches in digital security

Keynote speech

Benjamin Ang, Head, Centre of Excellence for National Security and Future Issues in Technology, Singapore

This keynote speech on cybersecurity regulation in Singapore highlighted the complexities and necessities of managing digital security in today's interconnected world. The discussion began with the OECD's definition of digital security, which is the economic and social dimension of cybersecurity. Similarly, digital security in Singapore involves creating a safe, secure, resilient, and trusted digital environment that improves consequences for society and the economy.

Singapore's Cybersecurity Act, passed in 2018, initially targeted 11 critical sectors, establishing obligations for them to adhere to certain cybersecurity standards, participate in regular checks, and allow government assistance during emergencies (CSA, 2018[12]). However, with the rise of sophisticated supply chain attacks, such as SolarWinds, and vulnerabilities in cloud services, the law was amended in 2024 to expand its scope. The amendments introduced three new categories:

- Systems of Temporary Cybersecurity Concern: These are systems that may not be classified as critical infrastructure but could pose significant risks during certain events. For example, during the Singapore Airshow, a high-ranking military official's call was hacked via hotel Wi-Fi, illustrating the need for enhanced security measures for systems of temporary concern during sensitive events.
- Entities of Special Cybersecurity Interest: This category covers institutions like universities that, while not traditionally seen as critical, house valuable research and data. A notable example is the breach of 52 staff accounts at four Singaporean universities by malicious actors, highlighting the need for special attention to cybersecurity in educational institutions involved in sensitive research.
- Foundational Digital Infrastructures: These are infrastructures that, while not critical on their own, are essential for the functioning of critical systems. For instance, the failure of air conditioning led to a major banking system outage in Singapore, underlining the broader concept of digital resilience beyond cybersecurity.

Mr. Ang also addressed how Singapore proactively approached the Internet of Things (IoT) by developing a cybersecurity labelling scheme. Rather than imposing fines, Singapore has incentivised manufacturers to enhance the security of IoT devices, such as IP cameras and smart home devices. The scheme has received mutual recognition from countries like Finland and Germany, with more countries potentially joining in the future, which would help raise global security standards.

Mr. Ang also discussed the effectiveness of self-regulation versus formal regulation. While companies and industry bodies have made efforts to enhance security, these measures often fall short when profitability is prioritised over societal impact. He argued that regulation is necessary to address market failures, drawing parallels to laws requiring seat belts in cars to ensure public safety.

The balance between regulation, self-regulation, and inaction varies by society, culture, and political context. While some fear that regulation stifles innovation, it can actually provide the certainty companies need to innovate securely. Trust among stakeholders is crucial, and it can only be built through transparent communication and equal information exchange between governments, companies, and civil society.

In conclusion, Mr. Ang emphasised that regulation is just one part of a broader cybersecurity strategy. Other essential elements include training, setting standards, and fostering a culture of self-regulation to ensure that digital security contributes to overall prosperity.

Is more digital security regulation inevitable?

Moderator: **Florian Schütz**, Chair, OECD Working Party on Digital Security and Director, Federal Office of Cyber Security of Switzerland

Panellists:

- **Benjamin Bögel,** Head of Sector for Product Security and Certification Policy, DG CONNECT, European Commission
- **Anne-Louise Brown,** Director of Policy, Cyber Security Cooperative Research Centre (CSCRC) of Australia
- **Keun Woo Lee,** Partner and Head of the New Project Group, Yoon & Yang LLC
- **Takashi Michikata,** Director for International Affairs, Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications of Japan
- **Murat Yazgan,** Head of Informatics and Cyber Security Department, Ministry of Industry and Technology of Türkiye

The aim of this session was to take stock of recent developments in digital security regulation in selected OECD Member countries. To shape the discussion, Mr. Schütz asked the panel whether more regulations are needed and to critically assess the impact they bring to stakeholders in the digital security ecosystem.

First, a panellist pointed out that in 2020 Australia introduced amendments to its Security of Critical Infrastructure Act, expanding its coverage from four sectors to eleven and thereby covering 80% of the companies in Australia (Australian Government Department of Home Affairs, 2021[13]). The Act mandates that entities within those sectors embrace Positive Security Obligations. The Obligations include providing operational and ownership information to government, encouraging voluntary cyber incident reporting to the Australian Cyber Security Centre (ACSC), and, for some entities like systems of national significance, complying with a Risk Management Program prepared by ACSC with boards submitting an annual report after the financial year. Overall, these reforms are expected to raise national digital security levels. The point of contention is that federal government entities are not fully captured by this Act.

Another strand of discussion focused on product security that, in a broader sense, closely relates to the secure delivery of services by CIs. CIs typically deploy products that are already available in the market. Therefore, by ensuring as much as possible that the products are developed with security by design in mind, governments can better manage the digital security risks that can manifest themselves during the service delivery phase. In this regard, the European Union is preparing the Cyber Resilience Act (CRA), which aims to ensure that the security risks of products with digital elements are managed throughout their entire lifecycle (European Commission, 2022[14]). There is a significant connection between the CRA and the European Union's Network and Information (NIS) Directive (European Union, 2022[15]). While the NIS Directive requires the use of fully patched and secure products, the CRA ensures that not only product manufacturers but also importers and distributors of those products are responsible for providing patches.

Although such a comprehensive product security regime can help raise the overall cybersecurity level, it requires complementary measures to facilitate its implementation. The EU has planned a 3-year transition period for the rollout of the CRA. European standardisation bodies will develop product-specific standards during the first two of those years. Furthermore, in consideration of the budget constraints SMEs may face in complying with the new legislation, the CRA offers a simplified technical documentation process.

Similarly, in Türkiye, the Ministry of Industry and Technology has published the Regulation on the Authorization of Participants within the Scope of Public IT Service Procurement, primarily with an aim to enhance the overall cybersecurity posture of private IT service providers across the country. There are three types of authorisation certificates under the Regulation – 1) public IT; 2) software; and 3) penetration

test. The Public Procurement Authority determines the type of certificate that should be mandatory depending on the nature of public tenders. Likewise, the application process for private companies is significantly simplified and made available online.

Regarding IoT products, the Japanese Ministry of Internal Affairs and Communication (MIC) launched the National Operation Towards IoT Cybersecurity Enhancement (NOTICE) initiative to enhance the security measures and practices surrounding IoT devices (NOTiCE, 2024[16]). The initiative is mainly led by the National Institute of Information and Communications (NICT) upon MIC's approval and in collaboration with Internet service providers (ISPs). NICT regularly verifies the security of IoT devices by entering weak passwords, and once vulnerable devices are identified, NICT reports their IP addresses to ISPs, who then send alarms to the end users asking them to amend the issue. Currently, around 120 million out of the total of 190 million IP addresses are routinely monitored, and NICT finds 10k vulnerable IoT devices per month and 1k compromised devices per day.

Concurrently, since April 2024, MIC has decided to officially adopt a risk-based approach prioritising IoT devices that may have more impact on the Japanese telecommunications networks by leveraging the CISA's vulnerability database that is designed to track and manage vulnerabilities in IoT devices (NOTiCE, 2024[16]). Such an approach reaffirms that digital security is like a "team sport" that requires coherent collaboration with ISPs, IoT device manufacturers and other stakeholders.

Lastly, the speakers emphasised the importance of flexibility in designing regulations so as not to disrupt industry's dynamism or stifle innovation. An interesting demonstration can be found in Korea, where the digital security of some sectors is largely shaped by government regulations in the forms of certifications and standards, whereas other sectors are gradually moving towards corporate autonomy. The Cloud Security Assurance Program (CSAP) is an example of government-led digital security regulation (KISA, 2024[17]). Despite the benefits brought by its systemised approach in ensuring the safety and reliability of cloud services used by public entities, it has been a target of criticism due to the long time and high costs the process requires. Also, since CSAP is designed to support government entities, its widespread rollout may create challenges for big-tech companies that have overseas headquarters. On the other hand, the financial sector in Korea has seen a gradual expansion of corporate autonomy, mainly driven by rapid digital transformation. Considering the varying levels of digital security risks across sector, the government is encouraging companies to define their own regulations proportionate to their estimated levels of risk, thereby granting them more autonomy. Concurrently, the financial authority is moving away from its prior control approach with a prescribed set of rules and requirements to a goal- and principle-oriented approach that emphasises post-incident responsibility.

How to stimulate and enhance collaboration?

Moderator: **Audrey Plonk**, Deputy Director of the OECD's Directorate for Science, Technology and Innovation

Panellists:

- **Florian Kirchner,** Cyber coordinator, General Secretariat for Investment (SGPI), Office of the Prime Minister of France
- **Evangelos Ouzounis,** Head of Policy Development and Implementation Unit, The European Union Agency for Cybersecurity (ENISA)
- **Jennifer J. Quaid,** Executive Director, Canadian Cyber Threat Exchange
- **Shinya Tahata,** Vice-Chair, OECD Working Party on Digital Security, and Senior Director, Information Security, Tokyo Metropolitan Government

This session focused on strategies to stimulate and enhance collaboration in cybersecurity, emphasising the importance of cross-sector and international cooperation to build a resilient and secure digital environment. The speakers discussed various aspects of collaboration from the perspectives of the private sector, government initiatives, regional agencies, and local government actions.

Effective digital security requires cooperation not just between countries but also among diverse stakeholders, including private companies, researchers, government bodies, and civil society. Trust and open communication and shared goals among all participants are fundamental to these collaborations.

Collaboration within the private sector is crucial for improving resilience against cyber threats. It involves not only sharing indicators of compromise and attack patterns but also discussing prevention strategies and mitigation techniques. The Canadian Cyber Threat Exchange is an example of private-sector collaboration where companies from multiple industries share real-time threat intelligence. This collaborative approach allows them to support each other by identifying and responding to live threats, thereby building collective resilience. The primary challenges in expanding such cooperation are trust and active participation. Trust must be built over time, and companies need to see the tangible benefits of sharing information to actively engage in such initiatives.

Governments are also spearheading cybersecurity strategies to enhance national and local resilience. The French government has for instance launched a comprehensive innovation policy, called France 2030, with a dedicated budget for cybersecurity to address the profound technological changes affecting society (French Ministry of Economics, Finance and Industrial and Digital Sovereignty, 2023[18]). With €54 billion allocated, including €1 billion specifically for cybersecurity strategy, the program aims to secure small entities and large infrastructure providers while fostering innovation. Initiatives such as a €30 million cyber grant challenge have successfully funded innovative projects, showcasing the power of public-private collaboration in generating trust and stimulating innovation. France emphasises international cooperation and alignment with European strategies, participating in bodies like the European Cybersecurity Competence Centre in Bucharest and collaborating with international partners. This interconnectedness helps leverage international expertise and ensure a cohesive approach to cybersecurity across borders.

On the regional side, organisations such as the European Union Agency for Cybersecurity (ENISA) promote collaboration among EU member states to build capacity, respond to incidents, and harmonise policies. ENISA also facilitates collaboration through the CSIRT network, which connects national Computer Security Incident Response Teams (CSIRTs) for operational cooperation and information sharing. Another group, called CyCLONe, is dedicated to crisis management. These efforts ensure coordinated responses to cyber incidents across the EU. In addition, ENISA encourages the creation of Information Sharing and Analysis Centers, which operate on a sector-specific basis to foster information

sharing and operational collaboration. Trust, which is key to collaboration, is built gradually in small, physical communities rather than virtual ones.

Collaboration is also part of local government strategies. Tokyo, as a major economic and political hub, has prioritised securing its critical infrastructure, such as transportation and the water supply, against cyber threats. The Tokyo Metropolitan Government (TMG) has therefore developed specific cybersecurity guidelines and measures. It has also established GovTech Tokyo, a group of technical experts, to reinforce digital security and enhance collaboration on cybersecurity measures. This initiative reflects a proactive approach to strengthening local cybersecurity defences. In addition, TMG collaborates with private companies to exchange views and strategies on cybersecurity. TMG also seeks to expand its international collaboration with other municipalities globally, recognising the value of shared knowledge and joint efforts in enhancing cybersecurity.

Finally, the speakers provided several ideas on how the OECD could play a pivotal role in enhancing and fostering collaboration in digital security:

- Establish clear orientations and goals to foster a unified approach to innovation and collaboration among OECD members;
- Align policies and strategies across OECD countries to make it easier for organisations to operate across borders while maintaining robust security practices;
- Promote best practices to address the cybersecurity skills gap and promote capacity building;
- Identify and address legal impediments that hinder information sharing;
- Change the narrative around digital security to help policymakers and organisations shift their perspective on digital security from being purely an IT issue to recognising it as a broader risk management issue.

References

ASD (2023), *Cyber Security and Australian Small Businesses*, https://www.cyber.gov.au/sites/default/files/2023-03/2023_ACSC_Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results_D1.pdf. [8]

Australian Government Department of Home Affairs (2021), *Protecting Critical Infrastructure and Systems of National Significance*, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems. [13]

CISA (2024), "Secure by Design Pledge", https://www.cisa.gov/securebydesign/pledge. [2]

CISA (2023), *Principles and approaches for secure by design software TLP:CLEAR*, https://www.cisa.gov/sites/default/files/2023-10/Shifting-the-Balance-of-Cybersecurity-Risk-Principles-and-Approaches-for-Secure-by-Design-Software.pdf. [3]

CSA (2018), *Singapore Cybersecurity Act*, https://www.csa.gov.sg/legislation/Cybersecurity-Act. [12]

CSCAU (2024), *Our flagship Dynamic Standard SMB1001: Multi-tiered cyber security certification standard for small and medium-sized businesses.*, https://www.cscau.com.au/smb1001. [9]

European Commission (2022), *Cyber Resilience Act*, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. [14]

European Commission (2018), *Next Generation Internet initiative*, https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-initiative. [7]

European Union (2022), *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E*, https://eur-lex.europa.eu/eli/dir/2022/2555/oj. [15]

French Ministry of Economics, Finance and Industrial and Digital Sovereignty (2023), *France 2030 : un plan d'investissement pour la France*, https://www.economie.gouv.fr/france-2030. [18]

KISA (2024), *Cloud Security Assurance Program (클라우드 보안인증제)*, https://isms.kisa.or.kr/main/csap/intro/. [17]

LG Electronics (2021), *FOSSLight*, https://fosslight.org/. [6]

METI (2023), *Guidance on Introduction of Software Bill of Materials (SBOM) for Software Management*, https://www.meti.go.jp/english/press/2023/0728_001.html. [4]

MSIT (2023), *Ministry of Science and ICT of Korea publishes the national Zero Trust Guidelines 1.0 (과기정통부, 제로트러스트 가이드라인 1.0 발표)*, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=239&mPid=113&bbsSeqNo=94&nttSeqNo=3183279. [11]

NOTiCE (2024), *NOTiCE*, https://notice.go.jp/en/. [16]

OECD (2021), *Building Cyber Resilience in a Post COVID-19 World: Local Challenges, Global Solutions Summary of the Third Annual Event of the Global Forum on Digital Security for Prosperity* -, OECD Publishing, https://one.oecd.org/document/DSTI/CDEP/SDE(2022)5/FINAL/en/pdf. [10]

Open Source Security Foundation (2024), *Protobom*, https://openssf.org/projects/protobom/. [1]

Quad Senior Cyber Group (2023), *Quad Cybersecurity Partnership: Joint Principles for Secure Software*, https://www.pmc.gov.au/resources/quad-cybersecurity-partnership-joint-principles-secure-software. [5]