Organisation for Economic Co-operation and Development

DSTI/CDEP/SDE(2022)5/FINAL

Unclassified

English - Or. English

9 May 2023

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Security in the Digital Economy

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 - Virtual Event Hosted by Israel – 7-9 June 2021

This report provides a summary of the third annual event of the OECD Global Forum on Digital Security for Prosperity, hosted virtually by Israel, on 7-9 June 2021. Moderators, speakers and delegates of the Working Party on Security in the Digital Economy (SDE) reviewed the draft. SDE delegates then agreed by written procedure to its transmission to the Committee on Digital Economy Policy. This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy on 24 February 2023 and prepared for publication by the OECD Secretariat.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Andras MOLNAR andras.molnar@oecd.org
Laurent BERNAT laurent.bernat@oecd.org

JT03518397

This document, as well as any data and 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.

Foreword

This report provides a summary of the third annual event of the OECD Global Forum on Digital Security for Prosperity, hosted virtually by Israel, on 7-9 June 2021.

It was drafted by Andras Molnar and Laurent Bernat of the OECD Secretariat and reviewed by speakers and moderators. Recordings of the event are available on YouTube.

This event was sponsored by the Israeli National Cyber Directorate (INCD) and TÜV SÜD.

The organising team included Matthew Nuding, Marion Barberis, Ghislain de Salins, under the supervision of Laurent Bernat, of the OECD Secretariat.

The Secretariat wishes to thank all the moderators and speakers, as well as the entire INCD team who helped organise the event, including in particular Michal Cremer and Aviram Atzaba.

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://oe.cd/gfdsp.

Table of contents

BOXES

Executive Summary

The third annual event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum") was held on 7-9 June 2021 and hosted virtually by Israel. It brought together 280 invited experts from 50 countries, representing governments, business, civil society, and academic and technical communities, to share views on "Local challenges, global solutions: Building cyber resilience together in a post-COVID-19 world". Participants discussed the following policy challenges where international co-operation is essential and OECD could build on its longstanding digital security expertise to facilitate a multistakeholder dialogue:

- **Digital security of consumer IoT devices.** Speakers highlighted the insufficient level of security and safety of many IoT products, the need for a rethink of consumer product safety regimes in relation to IoT devices and the market failure at the root of this issue. They discussed policy options to address it, such as Japan's technical initiatives (NICTER and NOTICE projects), as well as Singapore's cybersecurity labels scheme, noting that the speed of IoT innovation frequently outpaces policy making. They also discussed the pros and cons of voluntary versus mandatory policy measures.
- **Cyber insurance's readiness for digital catastrophes.** Speakers stressed that the current growth in risk and losses undermines insurance's role as a business and digital transformation enabler. They identified the systemic characteristics of the digital economy challenging the insurance sector (e.g. cloud computing, monoculture) and the importance of quantification and disaster scenarios to better understand the risk. As in other areas, public-private partnerships could help insurers overcome potential losses from cyber events that would surpass the insurance industry's financial capacity. An international multi-stakeholder dialogue, potentially hosted at the OECD, could help address this issue.
- **Supervision and enforcement of digital security policies.** Speakers recognised that digital security regulatory supervision and enforcement aim to improve security by changing organisations' behaviour rather than punishing them for not complying. While there is no one-size-fits-all supervision and enforcement model across countries, some approaches provide better results, such as those that are more flexible, based on multi-stakeholder co-operation, and that create trust in and among them.
- **Digital security challenges raised by the rapid digitalisation of public services**. A speaker from INCD explained how the Israeli cybersecurity agency took the opportunity of the COVID-19 crisis to boost the digital security risk management culture of the public sector leadership and top management.
- **Risk raised by managed service providers (MSPs)**. Speakers underlined that these companies have become a target of choice for malicious actors, as a single incident affecting one of them can compromise thousands of their customers (e.g. SolarWinds and Kaseya incidents). This represents a systemic risk for our economies, but MSPs' security can improve. For example, if policies foster the adoption of a "zero trust" approach and support the creation of independent digital security rating agencies to enable firms to differentiate MSPs on the market based on cybersecurity, better security would follow.
- **The relevance of standardisation and certification in a globalised and interconnected world.** Speakers underlined the limited adoption of and certification against key digital security standards. Together with the standards themselves, digital security standardisation and certification processes face several challenges. For example, standard setting processes generally have a very slow life cycle, which is not adapted to the dynamics of cybersecurity. To improve the situation, several options are envisioned, such as shifting from a "standard as a product" to "standard as a service" model, as well as bringing together the conformity assessment and standard setting communities.

Introduction

This document provides a summary of the third annual event of the OECD Global Forum on Digital Security for Prosperity, hosted virtually by Israel, on 7-9 June 2021, which brought together 280 invited experts from 50 countries' governments, businesses, civil society organisations, and academic and technical communities.

Each section of this report summarises the discussions held among speakers and panellists at the event.

In addition to these discussions, the following high-level speakers welcomed participants and provided scene-setting remarks: **Mathias Cormann**, OECD Secretary-General[1]; **Alon Ushpiz**, Director-General, Ministry of Foreign Affairs, Israel; **Haim Assaraf**, Ambassador, Permanent Representative of Israel to the OECD; **Yigal Unna**, Director-General, Israel National Cyber Directorate (INCD), Israel; and **Audrey Plonk**, Head of the Digital Economy Policy Division, OECD, who moderated the session.

Furthermore, the concluding panel brought together high-level representatives who provided an update on their countries' priorities for digital security policy and underlined the key role of the OECD to strengthen international co-operation in this area. This session was moderated by **Yigal Unna**, Head of Israel National Cyber Directorate, INCD, and included **Petr Novotny**, Director of Cyber Security Policies Department, NÚKIB, Czech Republic; **Yves Verhoeven**, Head of the Strategy Department, National Cybersecurity Agency (ANSSI), France; **Rajesh Pant**, National Cybersecurity Coordinator, Prime Minister's Office, India; **Tomoo Yamauchi**, Deputy Director-General, NISC, Cabinet Secretariat, Japan; **Jin-bae Hong**, Director-General for Cyber Security and Network Policy Bureau, Ministry of Science and ICT (MSIT), Korea; **David Koh**, Chief Executive, Cyber Security Authority (CSA), Singapore; **H.E Mohamed Al-Kuwaiti**, Head of Cyber Security, United Arab Emirates; and **Brandon Wales**, Acting Director of the Cybersecurity and Infrastructure Security Agency (CISA), United States.

The introductory and concluding sessions are available on YouTube with the other sessions.

How can policy makers address the IoT digital security challenge?

Moderator: **Tarah Wheeler**, International Security Fellow, New America

Panellists:

- **Ursula Pachl**, Deputy Director-General, BEUC The European Consumer Organisation
- **Atsushi Umino**, Director of the Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications (MIC), Japan, and Vice-Chair of the OECD Working Party on Security in the Digital Economy (SDE)
- **Neville Matthew**, General Manager, Risk management and Policy, Australian Competition and Consumer Commission (ACCC), Chair of the OECD Working Party on Consumer Product Safety
- **Stephen Pattison**, VP Public Affairs, ARM Holdings
- **Lim Soon Chia**, Cyber Security Engineering Centre Director, Cyber Security Authority (CSA), Singapore

Short summary[2] – *While Internet of Things (IoT) devices have become widespread and can provide considerable benefits, they also frequently have an insufficient level of digital security and can raise safety concerns. IoT devices are forcing a rethink of consumer product safety regimes, in particular as they increase the risk of "hasardisation", blur the current notions of liability and responsibility, and even affect public safety in some cases. In general, market dynamics fail to ensure a sufficient level of IoT security. For example, IoT producers are not appropriately incentivised to design secure products, IoT-based Distributed Denial-of-Service (DDoS) attacks reveal negative externalities in the IoT market, and there are significant information asymmetries related to digital security. A mix of information and education to empower consumers as well as well-designed regulation can help address the market failure. From a consumers' advocate perspective, mandatory requirements would be necessary to incentivise suppliers to develop safer IoT products. However, while regulation is an option, it could disrupt the market and inhibit innovation. This is why some countries prefer a mixed and "soft touch" approach, such as Japan's (cf. Box 1), and Singapore's (cf. Box 2) with its voluntary cybersecurity labelling initiative. In general, international co-operation is essential to reduce the prospect of a fragmented IoT security technical and legal standards' landscape that would increase the cost of doing business without necessarily enhancing cybersecurity.*

Internet of Things (IoT) devices have become widespread and can provide considerable benefits. According to some estimates, there will be 75 billion IoT devices worldwide by 2025. These devices range from healthcare products, connected toys, and connected vehicles to smart home applications such as cameras and sanitary ware. IoT devices can enable new business models, services and applications, ranging from remote surgery and airplane engines optimisation. ***However, IoT products often have an insufficient level of digital security.*** More than half of the IoT products that the European consumer organisation BEUC tested across the European Union came with no or very insufficient digital security measures. A security test of smart home products by a Belgium consumer organisation showed connected door locks, smoke detectors and cameras could be easily hacked. As the IoT connects the online and offline environments, digital security incidents can lead to physical damages and may affect personal safety.

Fast moving IoT-related innovation and technologies are forcing a rethink of consumer product safety regimes. Such regimes across the world are generally focusing on products rather than on the broader notion of consumer safety. However, recent evolutions increase the risk of "hasardisation" and blur the current notions of liability and responsibility. For example, products such as a cooktop stove designed to be used by a human locally can now be triggered remotely, with the risk of starting a fire or other accident. The safety of a product may be reduced if software updates are not received, whether expected by the consumer or not. Malicious actors can also trigger hasardisation, for example to threaten a victim by disrupting her home security cameras or indoor temperature control system. Attacks can affect public safety if malicious actors target a country's critical public service such as power grids. Another challenge is when consumers continue to use products that become more dangerous because they no longer receive security updates. This is a complex issue due to consumers' information overload which can make them insensitive to warnings and notices. They can also be overly optimistic about risk and reluctant to surrender a product they enjoy if there is no replacement. Overall, IoT-related innovation and technologies are moving so fast that governments are struggling to implement effective regulatory frameworks in this area.

Market dynamics fail to ensure a sufficient level of IoT digital security. IoT producers are not sufficiently incentivised to design products with an appropriate level of digital security. Digital security may be at odds with other market incentives, such as price and usability. In the rapidly evolving IoT market, innovators often prefer to minimise time-to-market rather than include robust digital security measures. IoT producers may also fail to adopt best risk management practices due to a lack of digital security awareness and culture. For instance, many IoT producers do not have clear and transparent policies or guidance on security updates, vulnerability disclosure and/or products' end-of-life. Furthermore, ***there are significant information asymmetries*** related to digital security in the IoT market. For example, consumers are unlikely to distinguish products based on security in absence of usable and trustworthy information about their level of digital security that would enable cross-products comparisons. Furthermore, it is not realistic to expect that consumers would appropriately identify, understand, and manage the consequences of vulnerabilities in the increasing number of IoT products they own. Lastly, distributed denial-of-service (DDoS) attacks reveal ***negative externalities in the IoT market***. As the producers of IoT devices do not take financial responsibility for such attacks, they lack the incentive to develop their products with digital security in mind.

While ***educating and empowering consumers is essential to address the market failure***, consumers also have a role to play, for example by maintaining cyber-hygiene. Moreover, changing consumers' mindset and educating them about IoT products' digital security may help them better understand digital security risk, and over time drive them to make more informed product choices. Governments can play a role, for example by launching education programmes and awareness raising campaigns, and forming public-private partnerships to support consumers and other stakeholders, including IoT producers. ***From a consumers' advocate perspective, mandatory requirements would be necessary*** to incentivise suppliers to develop safer IoT products. Consumers are reluctant to pay more to have a safe and secure IoT product. They expect these products to have a minimum level of security and safety, and to be designed and manufactured with security in mind, just like most other physical products. IoT products that do not include baseline security and safety measures should not be on the market. Regulation establishing minimum requirements for security and safety would both create a level playing field and legal certainty for suppliers and foster consumer trust. It could require suppliers of IoT devices to adopt security-by-design development processes and to put products on the market with security-by-default settings to simplify a consumers' choice of devices.

However, while regulation is an option, it could disrupt the market and inhibit innovation, which is why some countries prefer a "soft touch" approach. For example, the Japanese approach is based on a mix of proactive awareness raising and technical requirements. This "soft touch" approach aims to support market mechanisms, knowing that developers and users of IoT devices in Japan generally follow

recommendations from the government without the need for strong mandatory requirements. This approach includes initiatives to raise awareness of suppliers and developers about IoT security and provide them with specific IoT security guidelines. It also includes several technical initiatives to inform users and suppliers about the security of their IoT devices, as illustrated in Box 1. It also includes legislation and ministerial ordinances requiring all IoT devices sold in Japan to embed minimum technical security features, such as access control and firmware update mechanisms.

Box 1. The Japanese government's technical initiatives to inform users about digital security risk to IoT products

The Japanese Ministry of Internal Affairs and Communications (MIC) launched several technical projects in co-operation with the national research institute (NICT) aiming to alert users who own vulnerable IoT devices:

- The "NOTICE" project investigates IoT devices to detect those that are vulnerable to malware infection and alert their users through their Internet Service Provider. In practice, NICT tries to log into devices with weak passwords and triggers and alert mechanisms upon success.
- The "NICTER-Alert" project detects malware infected traffic and provides related information to the relevant ISPs with an invitation to alert the IoT user.
- A third project focuses on the digital security of critical IoT devices such as rivers' water gauges. It detects such devices online, tests them against known vulnerabilities or the presence of sensitive information which should not be available online (e.g. geolocation of the device) and contacts the operators for remediation.

Source: Atsushi Umino, Director of the Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications (MIC), Japan

International security standards can foster a trusted and sustainable global IoT market. The industry needs to build IoT products that are sufficiently "secure by design" because it is what consumers expect when they buy a physical product. A situation where consumers cannot really trust the products they buy is unlikely to be sustainable. One avenue is to make it easy for developers to design safer and more secure IoT products, for example by encouraging the development and adoption of standards that they can use to provide minimum levels of safety and security. Several guidelines and specific technical standards already exist such as ETSI's technical specification as well as the voluntary guidance issued by the United States' National Institute of Standards and Technologies (NIST).

***Labels can also play a key role to enhance IoT security while supporting innovation*.** Singapore, Japan, Germany and Finland launched digital security labelling schemes. Launched in October 2020, Singapore's labelling scheme is designed to enhance cybersecurity without stifling innovation, gently driving the market towards higher levels of security without disrupting it (cf. Box 2). Singapore developed this scheme as part of its strategy to become a "smart nation" and after developing a report with the Dutch cybersecurity agency on the IoT security landscape. The report highlighted that traditional security and certification mechanisms are not relevant in the rapidly evolving IoT market, where products need continuous maintenance and support throughout their lifecycle. Higher IoT security assurance requires a common baseline which can be achieved through international standards or interoperability of domestic and regional standards. For example, the Japanese labelling scheme makes use of ETSI 303 645. Experience from other areas shows that labels have to be simple, straightforward and global. This may be challenging as IoT security is a complex area where many factors have to be taken into account. The adoption of new labels may require time and advertising campaigns to be effective.

International co-operation is always necessary. In general, industry players are concerned with the prospect of a fragmented standards landscape that would increase the cost of doing business without necessarily enhancing cybersecurity. Mutual recognition of conformity assessment is key to foster the international market and collectively grow a more secure digital industry. International co-operation is essential to address this challenge.

Box 2. Singapore's IoT security approach and digital security labelling scheme

Singapore's approach is based on the assumption that if consumers change attitude towards security, developers will have appropriate incentives to build more secure products and that security will become a market differentiator. Furthermore, the government aims to increase international collaboration with like-minded partners to facilitate mutual recognition of standards and conformity assessment with a view to reduce the duplication of products tests across borders and reduce the cost of compliance.

To implement this approach, Singapore established a cyber security labelling scheme (CLS) consisting of four levels, from basic hygiene (with self-evaluation) to high assurance (with third-party assessment). Devices receive a label based on their risk profile, which depends on factors such as market demand, technology maturity and product readiness. Level one of the scheme requires an open vulnerability disclosure framework to allow vulnerabilities to be reported to the developer who can subsequently fix the problem. It also ensures that there are no universal passwords. Level two provides digital security risk assessment and critical design reviews. At level three, the product undergoes an assessment by a third-party test lab which evaluates its vulnerabilities. Level four focuses on resilience against common attacks and provides testing against specific used cases or devices that may pose a threat.

The scheme is voluntary, to enable fast implementation by the government, as well as continuous fine-tuning and improvement. However, labels can be required in some areas. For example, the Cyber Security Authority (CSA) selectively collaborates with sector regulators to mandate the adoption of the labelling scheme in their area. For example, all home Wi-Fi routers in Singapore have met CLS level one requirement by November 2021 as a result of a cooperation between CSA and Singapore's telecommunications regulator.

Source: Lim Soon Chia, Cyber Security Engineering Centre Director, Cyber Security Authority (CSA), Singapore

Preparing for digital catastrophes: Is cyber insurance ready?

Moderator: **Itai Benartzi**, Director of Policy Advancement, INCD, Israel

Panellists:

- **Roberta (Bobbie) Stempfley**, Vice President and Business Unit Security Officer, Dell Technologies
- **Peter Armstrong, Director**, Cyber Risk Insights Limited
- **Maya Bundt**, Head Cyber & Digital Solutions, Swiss Re
- **Leigh Wolfrom**, Policy Analyst, Directorate for Financial and Entreprise Affairs, OECD
- **Ariel Eli Levite**, Non-resident Senior Fellow, Carnegie Endowment for International Peace (CEIP)

Short summary – *Cyber insurance is playing an increasingly important role to support trust and resilience in the digital economy. However, as the losses have increased, cyber insurers are re-evaluating their strategies. The current trend in risks and losses has implications for insurance's general role of business and digital transformation enabler. Major recent incidents and the multiplication of ransomware has negatively affected the availability of insurance coverage and increased premium costs. In addition, due to high insurance payouts, certain systemic digital security risks are excluded from cyber insurance policies or have limited insurance coverage, forcing governments and businesses to bear the risk alone. Several interrelated characteristics of the digital economy are at the root of the systemic risk that undermines insurers' confidence to cover this risk. They include increasing business reliance on third-party services and networks, the reliance on cloud computing, aggregation risk through concentration and monoculture, and overall complexity. To unlock the potential of cyber insurance, insurers need disaster scenarios to understand the risk and its systemic dimension, and make decisions about capital requirements and capacity models. Better quantification is also needed, as it is difficult for insurers to quantify catastrophic and cascading cyber events and to meaningfully diversify the risk based on differences in policyholder characteristics. As in other areas, Public-Private Partnerships could help insurers overcome cyber events that surpass the insurance industry's financial capacity. An international multi-stakeholder dialogue that would include governments, digital security experts and insurers would be useful to address challenges related to cyber insurance.*

Cyber insurance is playing an increasingly important role to support trust and resilience in the digital economy. Through risk transfer, cyber insurance coverage allows businesses to accept risk and recover faster from cyberattacks. The cyber insurance market can incentivise businesses to adopt better digital security risk management practices, and facilitate the harmonisation of norms. Furthermore, insurers can also act as a depository of data and source of data analysis. However, despite take up rates doubling over the past five years, cyber insurance is currently facing a number of key challenges.

As the risk increases, cyber insurers are re-evaluating their strategies. Major incidents and the multiplication of ransomware negatively affected the financial resources of cyber risk insurers and the amount of capacity (insurance coverage) that they are willing to provide. Some cyber insurers have reached the limits of their financial capacity to cover the growing number of ransomware attacks over the last two years, at least one insurance giant declared ransomware uninsurable, and some others raised premiums by over 20 percent. Loss ratios have deteriorated, forcing insurers to re-evaluate their strategies, adjust underwriting standards, re-assess their capacity, or even exit the cyber insurance market altogether. For some insurers, the magnitude of potential losses is simply too large relative to the amount of premiums

they collect. Furthermore, they cannot meaningfully diversify the digital security risk based on differences in policyholder characteristics such as location, sector or size, which is the essence of the insurance.

The current trend in risk and losses undermines insurance's general role of business and digital transformation enabler. The growth of the economy may be in jeopardy if cyber insurance cannot play its role. If the risk and losses continue to rise and insurers continue to increase premiums or withdraw from the market insurance could become unattainable for many businesses. As a result, they may have to reduce the scale, scope and speed of their digital transformation. Because insurance allows businesses to run and innovation to happen, this would seriously impact the economy, echoing for example the 1980s liability crisis in the United States. While lack of cyber insurance coverage is not yet preventing businesses from having access to finance, it may happen in the future.

Systemic digital security risk challenges insurers. Due to the potential for extreme losses, certain systemic risks are excluded from cyber insurance policies or have limited insurance coverage, forcing governments and businesses to bear the risk alone. Systemic risk includes events that insurers might not cover given the magnitude of potential losses as a result of simultaneous impacts across many policyholders. While there has not been a large scale catastrophic cyber event yet, large incidents affecting critical infrastructures such as the Colonial Pipeline attack, or many sectors, such as NotPetya, give an idea of what might happen. Several interrelated characteristics of the digital economy are at the root of the systemic risk that undermines insurers' confidence to cover this risk:

- *Cloud computing*. Ultimately, cloud technologies are expected to be everywhere, in response to increasing demands to accelerate digital transformation. According to one analysis, every entity on the planet will be at least somewhat reliant upon cloud computing by 2030. However, cloud services, which have been called the "biggest single point of failure in human history"[3], are not immune to security failures, as illustrated by recent outages.
- *Aggregation through concentration and monoculture.* An ever-growing number of businesses increasingly depend on a small number of suppliers, technologies or products ("monoculture"), with little or no interoperability or redundancy.
- *Increasing business reliance on third-party services and networks*. The proportion of business interruptions associated with third party services and networks is increasing significantly. Businesses' reliance on extremely complex third party networks shifts their risk profile and makes it difficult or even impossible to assess the related risk. As a result, some insurers exclude them from their insurance policies. If this trend continues, by 2030 "when every entity is reliant upon third party networks and services, there will be no cyber insurance being written and no cyber risk capital available".
- *Complexity.* The sheer complexity of information systems and networks supporting the digital transformation increases the likelihood of unintentional errors and the magnitude of their consequences, and challenges our ability to model possible catastrophes. Overall, highly complex and interdependent value chains with many vulnerable points pose a multi-faceted challenge to insurers who cannot get close enough to the risk, assess and underwrite it.

Disaster scenarios are needed for the insurance market to develop. For insurers, disaster scenarios are essential to understand the risk and its systemic dimension, and to make decisions about capital requirements and capacity. A typical disaster scenario is a prolonged and widespread power outage, which could result in up to one trillion dollars losses. According to models developed by the Israeli National Cyber Directorate (INCD), a "cyber epidemic" scenario based upon mass distribution of malware similar to NotPetya could cost up to ten percent of the country's national budget. Other models based on similar scenarios reach up to USD 200 billion of economic losses of which only about 15 percent would currently be insured, a scenario which would wipe out the current affirmative cyber premium four times over. In comparison, Hurricane Katrina generated USD 160 billion in losses and 65 billion in insurance payouts in 2005. However, payouts included publicly insured losses by the national flood insurance programme (FEMA), raising the question of public-private insurance schemes (see below).

However, it is difficult for insurers to quantify catastrophic and cascading cyber events and to meaningfully diversify the risk based on differences in policyholder characteristics, e.g. by location or sector. It has been easier to enable digital transformation than to acknowledge that the likelihood of failures and understand the scope and scale of their consequences. Digital security risk quantification is not yet mature and most scenarios are based on breaches of availability and neglect the possible consequences of breaches of integrity which may arise with the rapid adoption of automation and artificial intelligence. The limited trust in existing models and analytical tools for quantifying digital security risk limits the capacity that insurers and reinsurers are willing to provide. This creates a threshold in capacity with reinsurance. There are relatively low insured limits applied to cyber insurance policies, significant use of reinsurance, and very little excess of loss reinsurance available in the market. The same lack of confidence in alternative reinsurance markets reinforces the "capital crunch".

The insurance industry, businesses and governments have a role and responsibility to better address digital security risk. In particular, the insurance industry has to better understand and assess digital security risk, which requires better quantification, including perhaps pooling of data. Better mapping of critical choke points can be used to dilute their likelihood and reinforce assurance, for example through redundancy and interoperability of cloud provision. Insurers need to put on the market products that price the risk adequately and foster good risk management practices. Business leaders need to acknowledge the strategic and operational nature of this risk, enhance their organisation's resilience and preparedness. Governments can also positively influence the environment, for example through appropriate legislation to reduce the threat level (e.g. cryptocurrencies), and by supporting standard-setting or awareness.

Public-private partnerships (PPPs) could help insurers to overcome the risk of financial losses due to cyber events that would surpass the insurance industry's financial capacity. In other risk areas, such PPPs have demonstrated that they can provide protections enabling insurers and re-insurers to put out large amounts of risk capacity without endangering their financial status or risk insolvency. Catastrophe risk insurance programs, loss sharing arrangements, or public-private partnerships exist in half of OECD countries and have successfully broadened the availability of affordable coverage for the perils that they target. Many types of insurance, reinsurance or co-insurance arrangements mutualise exposure to catastrophe risk, always with some government moral backing and sometimes with financial backing through a government backstop or guarantee. Most of these arrangements have been designed in such a way to ensure that government backing has been triggered only in very few instances. Often established in the aftermath of a catastrophic event that led to the withdrawal of private insurance coverage from the market (e.g. 9/11, Marmara Earthquake in the Republic of Türkiye), these arrangements cover natural disasters (e.g. floods and earthquakes), and terrorist attacks. These programs, which target businesses and/or households, exist in places that accounted for approximately 40 percent of all "wind and storm" and flood losses, and about 80 percent of all earthquake losses in OECD countries.

A multi-stakeholder and international dialogue that includes governments, digital security experts and insurers would be useful to address the challenges related to cyber insurance.

Increasing cyber resilience in the private sector: Towards smart(er) supervision and enforcement?

Moderator: **Rami Efrati**, Managing Partner, MSF Partners Innovation AG

Panellists:

- **Florentin Blanc**, Senior Policy Analyst, OECD
- **Lawrence Tay**, Director of Regulations Division, Cyber Security Agency of Singapore
- **Kay Tidten**, Senior Policy Officer, Federal Ministry of the Interior, Building and Community, Germany
- **Danielle Kriz**, Senior Director, Global Policy, Palo Alto Networks

Short summary – *Over the last few years governments have adopted policies to increase digital security in the private sector. In this area, regulatory supervision and enforcement need flexibility to take the diversity of stakeholders into account. In most cases, digital security regulatory supervision and enforcement aim to improve security by changing organisations' behaviour rather than punishing them for not complying. Overall, there is no one-size-fits-all digital security supervision and enforcement model across countries. However, some approaches are likely to provide better results. For example, supervision and enforcement strategies need flexibility to overcome the heterogeneity of organisations' profiles. Co-operation among all stakeholders is crucial to enhance digital security, as neither the government nor the private sector can reach a sufficient level of security alone. Yet trust between organisations and regulatory agencies is essential to establish such co-operation. Some lessons can be learned from other policy areas such as food and aviation safety, where the environment is also very dynamic and information sharing is key. Measuring digital security policy effectiveness can be challenging and incident reporting is not a panacea to address this challenge.*

Over the last few years, governments have adopted policies to increase digital security in the private sector. For example, the United States' government encouraged the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework including through public procurement. In the European Union, the NIS Directive requires operators of critical activities to enhance their digital security risk management. Nevertheless, it can be challenging for governments to assess and ensure the effective adoption and enforcement of their policies. For instance, certain businesses may resist regulation perceived as contrary to their short-term financial or other interests.

There is no one-size-fits-all digital security supervision and enforcement. Their effectiveness depends in part upon whether organisations' differences are taken into account. Companies and other organisations have variable sizes and degrees of digital maturity, security awareness, capacity and sophistication. Those who already perform audits can provide their results, while others may not audit their security at all. Some organisations may be very agile while others, despite having significant capacity, may be difficult to change. Organisations face different constraints according to their sector and scope of action (e.g. local, national, regional, international). Some may deliver critical activities to the economy and society

by operating a nation's most critical assets, and others may not. For example, Germany identified 1 700 critical operators that require stricter digital security regulation because of their national importance.[4]

Supervision and enforcement need flexibility to take the diversity of stakeholders into account. In most cases, digital security regulatory supervision and enforcement aim to improve security by changing organisations' behaviour rather than punishing them for not complying. Organisations do not want to be harmed by a cyberattack, therefore the role of the government is to help raise their awareness, educate them, and encourage them to improve their digital security skills and share threat information. Effective supervision and enforcement is based on several characteristics. Carried out carefully, it is based on existing and well recognised standards (e.g. ISO/IEC 27001) and good practices, and it is realistic from the perspective of the organisation. For example, it does not request the provision of confidential information (e.g. source code or customer data) or the duplication of processes that are already in place such as specific audits. Governments can define target groups based on key differences to tailor their regulation, supervision and enforcement accordingly, striking the balance between regulation and self-regulation, on a case-by-case basis, for example depending on sectors, criticality, size, maturity, etc. In addition, they can leave broad discretion to enforcement agencies to take into account the unique circumstances of organisations. They can also use a toolbox of instruments ranging from awareness, education and incentivisation, to legal requirements and enforcement, generally as a last resort. With respect to operators of critical activities, many countries have adopted specific regulation, such as Singapore (cf. Box 3) and Germany.

Box 3. Singapore's approach to supervision and enforcement

Singapore recognises both the importance of supervision and enforcement to enhance digital security, and that it is not possible to rely only on enforcement. Everyone has to take responsibility, play their part, and collaborate to enhance the security of the country.

Singapore places a strong emphasis on prevention and preparedness, in particular with respect to Critical Information Infrastructure (CII). In 2018, Singapore enacted a Cybersecurity Act providing a framework for the protection of CII operated by public and the private sector actors. It requires the CII owners to establish security measures in their systems, conduct regular digital security risk assessments and audits, and participate in digital security exercises led by the Cyber Security Agency (CSA). Audits and digital security risk assessments received by CSA enable to identity key areas for improvement and systemic risk that may require CSA's attention or intervention. The Cyber Security Act also mandates operators of CIIs to report digital security incidents and empowers the CSA to investigate, take remediation actions and share alerts with other stakeholders to prevent further damages. In case of incidents, CSA works with the victim organisation to mitigate impact, and determine the root cause. It does not immediately blame or punish the organisation. The objective is to "take a look" in order to help the operator rather than disrupt business operations.

CSA also takes a consultative approach to ensure that policies are calibrated, visible and practical. It holds regular consultations with digital security stakeholders to seek feedback on the feasibility of the agency's various digital security initiatives. In addition, it conducts nationwide digital security exercises, whereby the agency works with sectoral regulators and CII operators to test and validate operational plans in case of complex digital security attacks. These exercises require participants to attend digital security scenario planning sessions and workshops in order to identify areas for improvement in CII policies. They provide CSA with insights about the readiness of operators.

Source: Based on Lawrence Tay, Director of Regulations Division, Cyber Security Agency of Singapore

Co-operation is crucial to enhance digital security, as neither the government nor the private sector can reach a sufficient level of security alone. Such co-operation can take place when developing regulation and legislation, to optimise their applicability. Formal and/or informal consultations can inform governmental action and ensure its appropriateness to the targeted organisations. Co-operation can also take place between the cybersecurity agency and sectoral regulators (e.g. energy, finance, health, etc.) who are best placed to understand the unique context and complexity of their sector. For example, CSA-led digital security exercises involving sectoral regulators help increase their security capabilities (cf. Box 3). They also enhance trust and facilitate co-operation between agencies when incidents happen. In addition, Singapore holds sessions with industry players, sectoral regulators and insurers to discuss challenges and gather feedback on policies.

Trust between organisations and regulatory agencies is essential. For example, organisations need to have confidence that the agency will respect the confidentiality of information it may access to perform its mission. In Germany, for example, many organisations used to hesitate to share risk information with the government in the early days of digital security policy, to prevent leaks and exposure to the media and related reputational harm. Therefore, regulatory agencies need to demonstrate that they will protect the confidentiality of shared information. Furthermore, organisations also need to get some benefits from sharing information with the government, such as analysis and trends based on other reports. Simply publishing the number of incident reports received per year is unlikely to be sufficient. Fear of prosecution may also impede collaboration and information sharing between organisations and enforcement agencies. In Germany, a public-private partnership gathering operators of critical activities and the government helped overcome these obstacles. Stakeholders can share risk information collectively knowing that it will be kept strictly confidential by other participants.

Digital security supervision and enforcement share characteristics with other policy areas. For example, aviation safety deals with extremely complex systems operating in very dynamic environments where failure can create serious damage and there are many near misses. Therefore, sharing risk information and best practices is extremely important, within organisations, with the private sector, as well as with the government. Another example is food safety. Thirty years ago, the food industry had to educate every employee about the consequences of failure, a cultural challenge similar to digital security awareness raising and the education of all stakeholders in their daily use of digital devices.

Measuring policy effectiveness can be challenging and incident reporting is not a panacea. For example, quantitative indicators based on incident reports can be misleading. An increasing number of incidents may reflect increased security awareness or the effect of incentives to report incidents rather than a higher risk level. In addition, statistics may not adequately reflect differences in incidents severity, as stakeholders may be motivated to report all incidents, including near misses. Nevertheless, such information may be useful, for example to inform other stakeholders and enhance their situational awareness. Even audit reports can be difficult to compare when their context is not similar. Detailed analysis is generally needed to extract meaningful information and enable comparison, in particular to draw conclusions regarding regulatory effectiveness. More generally, effective incident reporting requires realistic timeframes, and clarity on the reporting thresholds in terms of severity or impact as regulators have limited capacity to digest information. Ex-post incident reporting, aiming at understanding what happened, needs to be distinguished from ongoing threat information sharing, aiming at enhancing situational awareness. Mandatory incident reporting requires significant multistakeholder consultation to ensure calibration and effectiveness.

Is the rapid digitalisation of public services compatible with digital security risk management?

Speakers:

- **András Hlács**, CDEP Vice-Chair, and Hungarian Delegate to SDE
- **Amit Ashkenazi**, Head of the Legal Department, INCD, Israel

Short summary – *Over the last few years, governments have accelerated the pace of their digitalisation. The COVID-19 crisis further increased the pressure on governments to rapidly develop and deploy new digital tools. In a keynote dialogue with András Hlács, Vice-Chair of the OECD Committee on Digital Economy Policy and delegate to the OECD Working Party on Security in the Digital Economy, INCD's Head of the Legal Department Amit Ashkenazi explained how his agency successfully supported the hyper-accelerated digitalisation of the Israeli government during the COVID-19 crisis and took that opportunity to boost the digital security risk management culture of the public sector leadership and top management. While this was a timely effort, there are still many challenges ahead, from ensuring appropriate budget allocation for security across agencies, to empowering security professionals as part of decision making processes, as well as migrating digital government services to the cloud in a secure manner.*

In the public sector, ICTs are often viewed as a technical issue primarily led by technical people, and do not always attract senior management's attention. However, when COVID-19-related lockdowns severely disrupted brick-and-mortar public services, senior public sector management immediately realised the importance of digitalising as many public services as possible, as quickly as possible, to ensure continuity in the delivery of government services to businesses and individuals. In this context, the Israeli National Cyber Directorate (INCD) had to ensure that such new digital government services deployed in crisis mode were sufficiently secure, while acknowledging that ministries and agencies' leaders and decision makers were primarily focused on the public safety and health, and on business continuity rather than digital security.

Because the government provides key services to the population, it needs to maintain the same level of accountability online as offline. In Israel, many ministries and agencies already had plans before the crisis to digitalise key procedures involving significant security challenges (e.g. checking citizens' identity with a high level of assurance), but they were waiting for appropriate digital transformation reforms to come to reality. The COVID-19 crisis accelerated that digitalisation process, with the risk that sensitive and essential public services requiring a comprehensive security check be deployed for the long term with insufficient security.

To address this challenge, INCD leveraged a so-called "triangle of accountability", targeting each agency and ministry's Director-General who has overarching responsibility, Chief Information Officer who is in charge of delivering the public digital service, and Legal Director or advisor, who has to make sure that the risk is managed. INCD sent a letter to each of these three senior officials to remind them of their responsibility with respect to digital security risk management. These letters required

prior coordination with the Attorney General's Deputy for private law, and generated discussions in the executive branch. Security was sometimes viewed as an impediment, leading to negotiations regarding the breadth and depth of risk management requirements and, accordingly, appropriate level of digital security measures.

In addition, when the government introduced a fast-track legislation to enable digital transformation, parliamentarians asked INCD to join the discussions to ensure that digital security risk management would be included in the new COVID-19 e-government legislation. Ultimately, a clause was inserted to require heads of agencies to have a documented risk management procedure.

One of the major assets supporting rapid and secure digital transformation was Israel's e-Government unit. The e-Government unit works to establish government-wide infrastructures in order to help ministries provide public services through a variety of channels, while reducing bureaucracy and streamlining work processes within ministries. It develops and operates secure technology infrastructure, and provides solutions for customers and partners in government bodies, in order to make government services available to citizens, businesses and the general public, and to connect ministries to online services. The unit develops and manages the government's outward facing internet infrastructure, including citizen facing services, such as payments. As such it was designated as "critical information infrastructure", overseen for cybersecurity aspects directly by the INCD. The e-Government unit had mature technological and cybersecurity capacities developed before the crisis. These were leveraged for a smooth and secure digital transformation. Thus, the e-Government unit provided secure solutions that enabled agencies to provide new digital services while doing so in a secure and accountable manner.

This approach was successful and effectively moved the digital security risk management discussion from the server room to the boardroom, which is the public sector is the director-general's level. This raised digital security risk management awareness across the government and triggered an evolution of senior civil servants' cybersecurity culture. It raised awareness on both the very concrete nature of digital security risk and that the fact that they are the primary risk owners, rather than ICT staff.

From this perspective, the COVID-19 crisis was a great opportunity because integrating digital security risk management among organisations' leadership is more challenging in the public sector than in private firms. Typically, the civil servants' culture is less accustomed to risk-based thinking than in the entrepreneurial world. Furthermore, public sector agencies face more constraints than firms when digitalising services. For example, they have to respect public law requirements such as procurement and budgeting rules and other legal obligations. These measures are necessary to protect public interests but they can slow down acquisition processes that are necessary for new services. In addition, organisational changes are part of the normal management toolset in the business world, whereas in the public sector they often require more formal procedures and even a change in legislation that applies to the service.

There are still many challenges ahead for INCD, which reflect the challenges of developing ICT governance, a relatively new area in the field of public administration. Indeed, ICT itself is a fast paced technological area that affects the way organisations operate and compete. As organisations embrace digital change, they need to adapt their governance structures to consider and manage relevant benefits and risks. This means for example to empower cyber security professionals within ministries and doing the groundwork to ensure that they are effectively embedded in the decision-making processes. Furthermore, digital security also requires appropriate resources and therefore while legal and procedural requirements are key to set the basis for change, budget considerations are also essential to make it happen in practice.

Another important challenge lies in the migration of digital government services to the cloud. In Israel, the increasing use of cloud computing in the public sector will bring many benefits, including to facilitate and accelerate digital transformation, as well as enhance security. For example, it will allow for

leaping over legacy systems that do not embed enough security controls, thereby enhancing the security of the public services that rely on them. However, there are also complex security issues, such as how to make sure that the agencies utilise the controls and tools available in the cloud environment to carry out their responsibility. Even more complex issues, which require a comprehensive approach, include how to perform incident response in the cloud in the public sector, for example. To ensure that cloud migration is done appropriately in the public sector, Israel is developing a secure cloud infrastructure and disseminating instructions and recommendations on how agencies should use it most appropriately. This follows the model chosen by the government many years ago to create a robust centralised e-government infrastructure for ministries and agencies, in the e-Government unit, with the critical mass to address security in a very professional manner and under direct supervision by INCD.

Managed service providers: A target of choice for supply chain attacks?

Moderator: **Irfan Hemani**, Deputy Director for Cyber Security, Department for Digital, Culture, Media and Sport (DCMS), United Kingdom

Panellists:

- **John Watters**, President, FireEye
- **Udi Mokady**, Co-Founder, Chairman & CEO, CyberArk

Short summary – *Malicious actors are undermining the global economy at an accelerating pace. The ransomware epidemic shows that they have already expanded their scope of attack to any weak enough entity that can pay, regardless of country, sector and size. Unless all stakeholders decide to jointly change their approach, malicious actors will significantly outperform and "out-innovate" digital security measures by 2030. To reach their ultimate targets, malicious actors are increasingly exploiting vulnerabilities in weak supply chains, including through managed service providers (MSPs) that are becoming both pervasive in every sector across the world and essential to economic resilience. As they have privileged access to their customers' networks, MSPs are attractive targets for malicious actors. They represent a systemic digital security risk for our economies as a single compromised MSP can affect many of its customers. While many MSPs invest in digital security, misaligned incentives tend to keep their digital security below an optimal level. For example, many SMEs and small organisations tend to lack the appropriate resources and expertise to ensure that the MSPs they choose implement appropriate cybersecurity measures. In contrast, MSPs are more likely to better manage security for larger customers, who are increasingly adopting a "Zero Trust" approach. Public policy could aim at aligning incentives to enhance MSPs' security, for example by fostering the creation of independent digital security rating agencies to enable firms to differentiate MSPs based on cybersecurity.*

Malicious actors are undermining the global economy at an accelerating pace. Whilst spending on digital security has significantly increased globally, losses due to digital security incidents are expected to grow even more substantially and at a fast pace. For instance, in 2013 global spending on digital security was estimated at USD 65 billion, whilst losses amounted to USD 300 billion. By 2020 global spending reached USD 130 billion against losses of USD 945 billion. It is expected that by 2030 approximately USD 300 billion will be spent whilst losses will amount to almost USD 4 trillion. By then, these amounts will jointly make up 3.5 percent of global GDP, a huge "global malicious tax". The ransomware epidemic shows that malicious actors have already expanded their scope of attack to any weak enough entity that can pay, regardless of country, sector and size. Unless all stakeholders decide to jointly change their approach to tackle this global challenge, malicious actors will significantly outperform and "out-innovate" digital security measures by 2030.

To reach their ultimate targets, malicious actors are increasingly exploiting vulnerabilities in weak supply chains, including through managed service providers (MSPs). Incidents such as NotPetya, Cloud Hopper, SolarWinds and Kaseya caused significant damage and led to malicious actors gaining unprecedented access to intellectual property and sensitive data. In the United Kingdom, only 12 percent of businesses have reviewed digital security risk posed by their suppliers and only five percent reviewed

their wider supply chain digital security risk. MSPs are key supply chain participants that provide businesses and organisations with essential ICT-based services such as network management, cloud and digital security services. They are becoming pervasive in every sector across the world, as well as essential to economic resilience. They bring huge benefits to small and medium-size enterprises (SMEs) and organisations lacking the skills and resources to perform such services in-house. Their customer base also includes most large businesses and organisations and is often spread across borders.

MSPs represent a systemic digital security risk. Because they have privileged access to their customers' networks, MSPs are attractive targets for malicious actors. With a single successful attack on one MSP, attackers can leverage such privileged access to breach that MSP's customers, including those operating in critical sectors or for governments. When successful, this one-to-many attack scheme can be remarkably effective, and allows attackers to expand their business model to small and medium organisations that would otherwise not be worth attacking. As MSPs are pervasive across all sectors' supply chains globally, they represent a global systemic risk.

While many MSPs invest in digital security, misaligned incentives tend to keep their digital security below an optimal level, in particular with respect to SMEs and small organisations. On the demand side, MSPs' customers who are not regulated, do not belong to critical sectors, or have a small or medium size, are looking for the cheapest service, often disregarding security. Small and medium size organisations buy managed services precisely because they do not have the resources, skills and scale to both carry out the service and manage the related risk themselves. Instead, they transfer the service to the MSP, without necessarily understanding the risk. Furthermore, they often believe that when they transfer the service they also transfer the associated risk and are relieved of managing it, an assumption that is not typically shared by the MSP itself. On the supply side, this may result in insufficient incentives for MSPs to invest in security and use security as a market differentiator. In lack of any oversight, MSPs can become the weakest point in the chain of security, leading to massive downstream incidents. While most MSPs do pay attention to digital security, this misalignment of incentives can contribute to limited investments. However, when they serve large customers or customers in critical sectors, MSPs are more likely to embed better security in their service, and sell products at a higher cost, because while these customers transfer a function to an MSP, they remain accountable to regulators or to shareholders for the related security risk. Furthermore, board members who are personally liable for security can also hold the leadership team accountable for implementing robust security that they can independently validate. These firms often have a Chief Information Security Officer (CISO) and buying power, thereby strengthening MSPs' incentives to invest in digital security. Larger firms may also be better placed to shift toward a "zero trust" security model, thereby incentivising their MSP's to follow this trend as well (cf. Box 4). More specifically, managed security service providers (MSSPs) generally have a higher level of digital security due to the nature of their business.

Box 4. "Zero trust": A solution to the disappearance of perimeters?

The widespread adoption of the Internet of Things, artificial intelligence, cloud technologies, and teleworking have created an infinite attack surface. Security perimeters have evaporated and it is becoming increasingly irrelevant to distinguish threats based on their internal and external nature. Malicious actors have a disproportionate advantage: they have to be right only one time whilst defense systems have to be right all the time. In fact, organisations have to assume that they are breached regardless of the robustness of their perimeter protections. As a result, it is no longer relevant to consider MSPs as external to their customers' information system from a digital security perspective.

Chief Information Security Officers (CISOs) who rely entirely on perimeter security may view the vanishing of perimeters as a nightmare. However, they could also view it as an opportunity to shift their

security model to a "zero trust" approach, which would simplify security by levelling up the types of controls that organisations have to implement.

Instead of trusting by default what is inside their increasingly hard to define perimeter, and struggling to block what is outside, it is more straightforward –at least conceptually- to trust nothing by default, and systematically verify permissions (zero trust approach).

Furthermore, a "tipping and cueing" system can also help detect and address malicious actors in a system. A first layer of controls may provide low-resolution evidence about something anomalous happening within an infrastructure, allowing then a second layer of controls to zoom-in at a higher resolution, investigate the intruder proactively, and prevent it from breaching assets.

The adoption of such a "zero trust" approach and "tipping and cueing" system will take time and significant investments. However, the combination of a digitally dependent global economy, ever more sophisticated threats, and geopolitical tensions, really call for a change of operational security model.

Source: Panel discussion.

***Public policy could aim at aligning incentives to enhance MSPs' security**, for example by:*

- *Educating organisations, in particular SMEs, on how to differentiate MSPs based on digital security and developing internationally supported baseline requirements for MSPs.* While small and medium organisations (and some larger ones) increasingly understand that they need higher security standards, including from their service providers, they struggle to differentiate MSPs based on digital security. Public policy could "help the buyers" by educating SMEs to better understand the minimum digital security requirements they should establish for their own activities ("cyber hygiene") and how these would translate into requirements for MSPs supporting their activities, including for example what they should hold an MSP accountable for in specific scenarios. In parallel, a set of baseline cybersecurity requirements which MSPs are expected to demonstrate, backed by a corresponding international effort to promote take-up/adoption by MSPs, could also be developed.
- *Promoting technologies that firms can use to measure their level of security.* Firms can't manage what they can't measure. While the extent to which a company could measure the effectiveness of its security used to be very limited, there are now maturing and increasingly usable technologies enabling firms to test their security against known threats relevant to their industry. These technologies allow firms to run security as a business function and validate their security posture, rather than measuring security efforts based primarily on their security expenditures.
- *Encouraging insurance in certain areas*. Insurance could provide a positive incentive system if firms with a higher level of security would be rewarded with a more attractive insurance offering, such as a reduced cyber insurance premium. As a firm's level of security depends on its suppliers' level of security, this positive incentive could trickle down to firms' MSPs. Facing increased demand for risk transfer, MSPs may be inclined for example to offer their service packaged with an insurance policy covering the risk related to the function they perform for their customers. Insurers could also require MSPs to enhance their security because of the systemic risk they entail.
- *Fostering the creation of independent digital security rating agencies to enable firms to differentiate MSPs based on cybersecurity.* Firms, including insurers, cannot just rely on MSPs' claims that they are following good security practices. Rather, they need to validate that security controls are effectively deployed, and test their operational effectiveness on an ongoing basis, because malicious actors continuously innovate and adapt their attack schemes. A thought-provoking, ambitious and long-term initiative could involve establishing an independent security rating mechanism, akin to credit rating agencies, to provide a neutral, consistent, flexible and evolving digital security maturity standard that would help firms, including insurers, validate MSPs' security claims on an ongoing basis. Such a

mechanism, which would require further analysis - for example, of how to take sectoral and customer variations into account - could increase transparency on the market, help customers choose their provider on the basis of security, and facilitate the provision of insurance to MSPs.

Standardisation and certification: Are they fit for a globalised, interconnected world?

Moderator: **Dr Bushra Al Blooshi**, Head of Research and Innovation, UAE

Panellists:

- **Yuval Segev**, Director of Advanced Technology, INCD, Israel
- **Sudhir Ethiraj**, Global Head of Cybersecurity Office, TÜV SÜD
- **Lisa Carnahan**, Associate Director for IT Standardization, Information Technology Laboratory, National Institute of Standards and Technology (NIST), United States
- **Vladimir Radunovic**, Director for E-diplomacy and Cybersecurity, DiploFoundation

Short summary – *Standardisation and certification hold a great promise to increase the overall level of digital security, but also face challenges. For example, certification against the most well-known information security standard (ISO/IEC 27001) is not so common in comparison with other areas. Standardisation processes are facing several opportunities and challenges. In particular,* with *their very slow lifecycle digital security standards and conformity assessments are not sufficiently adapted to the dynamics of cybersecurity. Several options are being explored to adjust standards to the specificities of cybersecurity. For example: shifting from "standard as a product" to "standard as a service"; adopting a products & processes –rather than products only- approach; shifting from static paper attestations and labels to dynamic ongoing mechanisms; exploring easy-to-assess minimal requirements (e.g. for SMEs); striking the right balance between cost of conformity assessment and confidence benefit and bringing the conformity assessment and standards making communities together. Mutual recognition of conformity assessment is essential in a global market, but assessors need to meet certain conditions. From a public policy perspective, it is important to strike the right balance between voluntary and mandatory requirements related to the implementation of standards and certification.*

Standardisation and certification hold a great promise to increase the overall level of digital security, but also face challenges. Economic literature points to their positive effects on competition and innovation, in particular through increased interoperability and reduced information asymmetries. Many policy initiatives are underway in various regions to promote standardisation and certification as effective market mechanisms to mainstream digital security best practices. However, digital security standardisation and certification are currently facing a number of challenges. For example, certification against the most well-known information security standard (ISO/IEC 27001) is not so common in comparison with other areas. According to ISO survey data, only 40k valid certificates have been issued for ISO/IEC 27001, compared to 900k, 350k and 190k certificates issued respectively for quality (ISO 9001), environmental (ISO 14001) and health & safety (ISO 45001).[5] Participants in this session discussed challenges related to digital security standards.

Digital security standards and conformity assessments are not sufficiently adapted to the dynamics of cybersecurity. Despite the fact that digital security is an extremely dynamic area, security standards tend to have a very slow lifecycle. The typical time between each standard's iteration is too long, in part because the consensus-building process takes time. Standards typically have an 8 year review cycle whereas technologies, usages, threats, risks and mitigation techniques are constantly changing. In addition, product standards may be become vulnerable the day after receiving their attestation because of the changing environment, including updates in the product itself. Checklist-based standards are not fit for purpose in a continuously evolving risk environment. Furthermore, the assessment procedure is often suboptimal and quite subjective, and rarely uses technologies to produce an objective picture of an organisation's security maturity. Research in Israel showed that auditors are not always experienced and qualified enough to provide a truly informed and useful assessment. In general, the assessment process requires little evidence, addresses only the surface, is not performed often enough and, above all, assesses compliance rather than maturity and effectiveness.

Standardisation processes are facing several opportunities and challenges. For example:

- There are currently opportunities and interest for discussing the use of cybersecurity standards to foster the implementation of public policies and regulations, but policy objectives are often driven by different national agendas which may fragment global markets.
- Broader stakeholder participation (e.g. start-ups, SMEs, open source communities) in standards making processes could foster better and richer standards, but also make development processes more complex and increase time to reach consensus.
- There is currently interest in grounding standards in use cases, which may help develop better standards, but it may also ignore the fact that one product or technology may be used in a variety of environments and contexts (e.g. software libraries may end up being used in critical systems).
- New standardisation organisations are appearing, for example with respect to open standards, and corporate budgets are shrinking which means that firms tend to invest less in standards than in the past.
- The frontier between information technologies (IT) and operation technologies (OT) is increasingly blurred from a security perspective but the related standards are developed in different settings and groups, with different cultures and mindsets.
- Lastly, standards such as ISO 27001 are too complex for small organisations who primarily need to achieve baseline security.

Overall, the current standard and compliance model is not very effective with respect to digital security because standards making and assessment processes are not tailored to the pace of technological developments, as well as dynamics and complexity of cybersecurity.

***Several other options are being considered to adjust standards to the dynamics of cybersecurity*.** For example:

- S*hifting from "standard as a product" to "standard as a service".* In Israel, the government developed a free platform where organisations can get all the best practices and standards, and link them with their controls, risks, compliance requirements and regulations, all in a single dashboard. The platform helps organisations and their customers/partners to more easily get a real-time picture of where they stand against standards and regulations.
- *Adopting a products & processes –rather than products only- approach*. According to US Government Executive Order 14028, federal agencies purchasing products should consider whether developers followed a secure development methodology. As a result, the U.S. NIST is exploring what such software development requirements should look like, including in areas such as management and governance.

- *Shifting from static paper attestations and labels to dynamic ongoing mechanisms,* to enable ongoing assessment.
- *Exploring easy-to-assess minimal requirements, such as those that customers themselves can check* (e.g. ability to change a password).
- *Striking the right balance between cost of conformity assessment and confidence benefit*. Too many requirements add cost, but the goal should be to obtain the right level of confidence at the lowest cost.
- *Bringing the conformity assessment and standards making communities together.* Both communities can lean a lot from each other to improve their products and practices.
- *Changing the format of standards.* For example, light standards focusing on baseline requirements and recommendations may be developed to target SMEs and smaller organisations, and even large organisations who need more agility. The work carried out by the Charter of Trust is a good illustration of such an approach.

Mutual recognition of conformity assessment is essential in a global market, but assessors need to meet certain conditions. For all parties to trust each other's assessments, there needs to be a way to check that assessors' level of knowledge and experience is sufficient, which means that parties need to agree on what that level should be. Furthermore, the standards also need to address security at the right level of granularity and require appropriate evidence at that level rather than be too general.

From a public policy perspective, it is important to strike the right balance between voluntary and mandatory requirements *related to the implementation of standards and certification*. While mandatory requirements may be needed in some cases, it is essential that users and manufacturers see a real need for them. SMEs, for example, need more help than requirements. In addition, regulators can play a very important role to encourage the use of standards and align certification with them.

Notes

[1] Mr Cormann's speech is available at: www.oecd.org/about/secretary-general/oecd-sg-remarks-at-2021-global-forum-on-digital-security-for-prosperity-7-june-2021.htm

[2] This topic is also addressed in OECD (2021), "Enhancing the digital security of products: A policy discussion", *OECD Digital Economy Papers*, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en.

[3] www.networkdefenseblog.com/post/biggest-single-point-of-failure

[4] For more on the digital security of critical activities, see Bernat, L. (2021), *Enhancing the digital security of critical activities*, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf and OECD (2019), *Recommendation of the Council on Digital Security of Critical Activities*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456.

[5] https://www.iso.org/the-iso-survey.html