INAUGURAL EVENT

Governance of Digital Security in Organisations and Security of Digital Technologies

Paris
13-14 DECEMBER 2018
Roles and Responsibilities of Actors

GOVERNANCE OF DIGITAL SECURITY IN ORGANISATIONS AND SECURITY OF DIGITAL TECHNOLOGIES

13-14 December 2018 – OECD Conference Centre, Paris, France

Global Forum Web Site: oe.cd/gfdsp

“All stakeholders should take responsibility for the management of digital security risk.”

OECD 2015 Recommendation on Digital Security Risk Management for Economic and Social Prosperity

The OECD Global Forum on Digital Security for Prosperity

- Aims to consolidate a global network of experts and policy makers by fostering regular 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.
- Is an international multilateral, multi-stakeholder and multidisciplinary setting for all communities of experts to meet, dialogue, network and influence public policy making on matters related to digital security for prosperity.
- Feeds OECD policy discussions. Its output can lead to the development of analytical work, principles and international policy recommendations.

Purpose of the event

This inaugural event of the Global Forum will examine the roles and responsibilities of actors for digital security, with a focus on good practice for the governance of digital security risk in organisations, and improving digital security of technologies throughout their lifecycle.

It will bring together businesses and organisations using digital technologies, suppliers of these technologies, suppliers of security solutions, experts from civil society and academia as well as government policy makers interested in encouraging the adoption of best practice to reduce digital security risk.

Who should participate?

Public policy makers from governments in OECD member and non-member countries; Chief Information Security Officers (CISOs), risk managers and other experts in charge of digital security in businesses and public sector organisations; digital security experts from firms offering digital products and services (hardware and software products, network and cloud services, etc.) or digital security services; experts from civil society, academia and the technical community.

Format

Organised around 6 plenary sessions, the event will interactively engage speakers and participants. The final session will lay out main findings and possible future work to enhance international co-operation.

Contact

For more information, please contact: OECD Secretariat - digitalsecurity@oecd.org
DRAFT AGENDA  

as of 12 November 2018

Chair: Jørgen Abild Andersen, former Chair of the OECD Committee on Digital Economy Policy (CDEP)

DAY 1: Thursday 13 December 2018

8:30 Registration

9:00 Welcome remarks
   Keynote: Guillaume Poupard, Director General, French Cybersecurity Agency ANSSI

PART I: DIGITAL SECURITY RISK GOVERNANCE IN ORGANISATIONS

This part will explore roles of actors within organisations (session 1), and their responsibilities with respect to others (session 2) and regarding how far they can go in protecting themselves (session 3).

9:30 Session 1 - Changing the Culture at the Top and Breaking Corporate Silos

A clear chain of responsibility starting at the highest level of leadership is essential to manage digital security risk. A governance framework is also necessary to clarify who is responsible for what, and how collaboration can take place, including across silos. This session will discuss how to make digital security a priority for CEO, Board and C-Suite. It will also discuss good practice for digital security risk governance, including co-ordination, chains of reporting, incentives, evaluation, etc.

Moderator: tdb

Speakers and Panellists: speakers and panellists from business / government / civil society / tech community in OECD member and non-member countries, including:

- Dato’ Dr. Haji Amirudin Bin Abdul Wahab, CEO, Cybersecurity Malaysia
- Pascal Andrei, Chief Security Officer, Airbus
- Andrea Bonime-Blanc, GEC Risk Advisory
- Sebastian Bregning, Senior Risk Manager, A.P. Møller – Mærsk
- Philippe Cotelle, Board Member, Federation of European Risk Management Associations (FERMA)
- Hudi Zack, Israel National Cyber Directorate (INCD)
- Ministry of Economy, Trade and Industry, Japan (tbc)

11:00 Break
11:30  Session 2 - How Can Value Chain Partners Trust Each Other’s Digital Security Governance?

In hyper-connected economies, digital security threats can come from anywhere, including from partners along the value chain. How can partners trust each other in a business ecosystem and value chain? Are there particular mechanisms or measures that can achieve trust between partners (e.g. standards, certification, information sharing). This session will discuss good practice and incentives schemes to foster trust between partners.

Moderator: tdb

Speakers and Panellists: speakers and panellists from business / government / civil society / tech community in OECD member and non-member countries, including:

- Evangelos Ouzounis, Head of Unit, European Network and Information Security Agency, ENISA
- John Salomon, Director, Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Yuval Segev, Israel National Cyber Directorate (INCD)
- Michiel Steltman, Director, Digital Infrastructure Netherlands Foundation (DINL)
- Henry Young, Senior Technology Policy Advisor, Department of Commerce, United States

13:00  Lunch Break

14:00  Session 3 - "Active defence": how far can businesses go in proactive security?

The private sector has been exposed to an increasing number and variety of attacks and businesses are dependent on their governments if they wish counter-offensive action to be taken against attackers. Today practices known as "hacking-back" are within governments' prerogative only. Should public policy evolve in order to clarify whether and how private sector could take proactive defensive measures (also called "active cyber defence")?

Moderator: tdb

Speakers and Panellists: speakers and panellists from business / government / civil society / tech community in OECD member and non-member countries, including:

- Stewart Baker, Steptoe & Johnson
- Théodore Christakis
- Leandro Ucciferri, Asociación por los Derechos Civiles (Argentina)
- Yves Verhoeven, French National Cybersecurity Agency (ANSSI)

15:30  Break
PART II: MAKING DIGITAL TECHNOLOGIES MORE SECURE THROUGHOUT THEIR LIFECYCLE

This part will explore roles and responsibilities of actors to make technologies more secure at technology design and integration stages (session 4) and once the technology is in customers’ hands (session 5). It will also discuss how increase the responsible discovery and disclosure of vulnerabilities (session 6).

16:00 Session 4 – How to Achieve Security by Design?

Providers of digital technologies are increasingly aware of the need to take digital security into account in the design of their products and services. However, technologies are developed in more complex environments involving large numbers of partners such as designers, integrators, distributors, etc. This is particularly the case with the Internet of Things (IoT) and cloud computing. Trade-offs need to be made between security, functionality, cost, time-to-market, and other factors affecting competitiveness. In addition, technologies are deployed by customers in very different ecosystems, also involving many actors and partners. This session will discuss the roles and responsibilities of actors for making technologies more secure from the outset, the incentives and disincentives they face, the need for baseline and other security standards, their implementation throughout the value chain, and the possible need for third party evaluation.

Moderator: tdb

Speakers and Panellists: speakers and panellists from business / government / civil society / tech community in OECD member and non-member countries, including:

- Pascal Andrei, Chief Security Officer, Airbus
- Audrey Plonk, Government and Policy Director, Intel
- Diane Rinaldo, Deputy Administrator and Deputy Assistant Secretary for Communications and Information, US Department of Commerce, NTIA
- Jeff Wilbur, Technical Director, Online Trust Alliance (OTA)
- Siemens (tbc)
- Andy Schweiger, Managing Director Cyber Security Services, TÜV SÜD

17:30 End of Day 1 - Cocktail
DAY 2: Friday 14 December 2018

9:00  Session 5 – Maintaining Security once Technologies are on the Market

Despite efforts to make technologies more secure from the outset, vulnerabilities are often found once products and services are used by customers. This session will discuss the challenges related to the management of vulnerabilities, including the roles and responsibilities of different actors in the development, integration and application of security updates, and with respect to products’ end of life, i.e. when they are no longer supported.

**Moderator:** tdb

**Speakers and Panellists:** speakers and panellists from business / government / civil society / tech community in OECD member and non-member countries.

- Nimbe Ewald Aróstegui, General Director of Technical Regulation, Instituto Federal de Telecomunicaciones, Mexico
- Cristine Hoepers, General manager, CERT.br
- Angela McKay, Microsoft
- Mr. Chaichana Mitrpant, Deputy Executive Director, Electronic Transactions Development Agency (ETDA), Thailand
- Ministry of Internal Affairs and Communications, Japan (tbc)

10:15  Break

10:45  Session 6 - Encouraging responsible vulnerabilities disclosure

To make technologies more secure, so-called “zero day” vulnerabilities must first be discovered and disclosed for mitigation measures to be developed and implemented. However, many vulnerabilities are discovered by researchers and “hackers” and have a lot of value for technology suppliers and security firms who want to improve products’ security, and for criminals and other actors who want to exploit or sell them. Coordinated disclosure of vulnerability processes are easier to implement in a finder-vendor relationship but become more complex where they involve a variety of companies and complicated supply chains. This session will discuss how to reduce zero-day vulnerabilities’ lifetime, encourage responsible disclosure of vulnerabilities and ethical hacking (“white hat”), and how coordinated disclosure of vulnerability can be implemented in increasingly complex environments and supply chains.

**Moderator:** tdb

**Speakers and Panellists:** speakers and panellists from business / government / civil society / tech community in OECD member and non-member countries, including:

- Rodolphe Harand, Associate Director, Yes We Hack
- Cedric Laurant, Civil Society
- Lorenzo Pupillo, Head of the Cybersecurity Initiative, Centre for European Policy Studies (CEPS)
- Marietje Schaake, Member of European Parliament
- Bruce Schneier, Security Technologist and Author
Conclusion

12:00 Public policy discussion

This session will bring together policy experts from OECD and non-OECD governments, private sector, civil society and technical community for a high-level policy discussion on the main findings from the event, possible avenues for future work and international co-operation.

Moderator: Katarina de Brisis, Chair of the OECD working Party on Security and Privacy in the Digital Economy (SPDE)

Panellists: high-level experts from business / government / civil society / tech community in OECD member and non-member countries.

- Henri Verdier, Ambassador for Digital Affairs, France (tbc)
- Thomas Fitschen, Special Representative for Cyber Foreign Policy and Cybersecurity, Germany (tbc)
- United States (tbc)
- Carlos da Fonseca, Brazil
- Suso Baleato, Civil Society Information Society Advisory Council (CSISAC) (tbc)
- Nigel Hickson, Internet Technical Advisory Committee (ITAC) (tbc)

13:15 End of the event

Global Forum Web Site: oe.cd/gfdsp

Global Forum Partners