OECD Global Forum on Digital Security for Prosperity

Main points from the Inaugural Event (14-15 December 2018): Key areas for international co-operation

The OECD Global Forum on Digital Security for Prosperity ("Global Forum") was launched in 2018. It brings together policy makers and experts from all stakeholder groups to foster regular sharing of experiences and good practice on digital security risk and its management, as well as mutual learning and convergence of views on digital security for economic and social prosperity.

The Global Forum holds thematic events the outputs of which aim to feed international public policy discussions and inform analytical work, principles and international policy recommendations, both at the OECD and in other international fora. The Global Forum is not an OECD formal body but rather a flexible vehicle to engage all countries in the discussion of digital security from the economic and social perspective. The Global Forum does not address international security and cybercrime.

The Inaugural Event of the Global Forum took place in Paris on 15-16 December 2018. Over 250 experts from government, business, civil society and the technical community coming from 35 countries[1] examined the roles and responsibilities of digital security actors**,** a theme proposed by France.[2] They discussed good practice for the governance of digital security risk in organisations and for improving digital security of technologies throughout their lifecycle.

The following three challenges emerged as priority areas in need of further international multi-stakeholder dialogue and analytical work:

1. Strengthening digital security of products and services throughout their lifecycle

One avenue to reduce digital security risk is to encourage businesses to increase digital security in products and services throughout their lifecycle. This includes promoting "digital security by design" including through third party evaluation, maintaining digital security of products and services once they are in the hands of customers (for example through timely security updates and by ensuring that these updates reach end users), and addressing the security challenge of the end of their commercial life, when products are still in use but no longer maintained. Furthermore, if customers could meaningfully assess the level of digital security of products and services on the marketplace, market forces would probably better reward "digital security by design" and other good digital security practices on the part of products manufacturers and services providers.

Enhancing digital security of products and services remains however a challenging task that requires to take into account market conditions, the complexity of ICT design ecosystems and the multiplicity of actors involved along products and services' value chains.

International cooperation in this area would be helpful to explore incentives, challenges, policies and other means to enhance digital security of products and services without inhibiting innovation. Connected physical devices (IoT) could be one focus as digital security breaches can potentially create physical damages to their users (connected homes, automated vehicles, health devices, etc.).

[1] Austria, Belgium, Brazil, Canada, China, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Israel, Italy, Jamaica, Japan, Korea, Latvia, Luxemburg, Malaysia, Mexico, Netherlands, Norway, Poland, Slovak Republic, Russia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States, European Union

[2] The agenda and more information is available at http://oe.cd/gfdsp

2. Encouraging responsible and co-ordinated disclosure of vulnerabilities and protecting security researchers

A pre-condition to making digital products and services more secure is the discovery of vulnerabilities and their disclosure to relevant stakeholders who can fix them in order to reduce potential malicious exploitation by third parties. However, businesses may not all have appropriate processes in place to act on vulnerabilities reported to them by security researchers, and may even discourage or threaten them of legal proceedings. Practices that discourage responsible disclosure of vulnerabilities by security researchers are feeding the underground market for so-called "zero day" vulnerabilities that can be acquired by malicious actors. Nevertheless, some stakeholders have established good practice to encourage the responsible and co-ordinated disclosure of vulnerabilities.

International cooperation in this area would be helpful to explore existing good practice across countries to protect and encourage security researchers to disclose vulnerabilities in a responsible and coordinated manner. Outcomes of this work would help identify principles that could be supported at international level.

3. Clarifying the limits of what businesses can do to protect themselves in response to an attack ("hack back")

Businesses currently face uncertainty with respect to the legality of a number of technical digital security measures that could be taken in response to attacks. For example, some digital security measures targeting devices involved in an attack, often located in other jurisdictions, could potentially increase digital security risk to legitimate third parties ("hack back", "active defense", "offensive response", etc).

International cooperation, strictly focused on private sector response to attacks, would be helpful to begin clarifying the "grey zone" between legal and illegal digital security measures. Better policies and good practice in this area would prevent businesses from unintentionally becoming an additional source of digital disruptions while empowering them to best defend themselves.