GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

OECD

Encouraging Digital Security Innovation

Report from event held in London, United Kingdom (14-15 November 2019)

The second annual event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum") was held on 14-15 November 2019 in London, United Kingdom. It gathered over 160 participants from 22 governments as well as experts from the business, technical, and civil society communities to discuss how to encourage digital security innovation. The event took place at Plexal, the East London innovation centre hosting the London Office for Rapid Cybersecurity Advancement (LORCA). The full report is available here.

Innovation is a key driver of digital transformation, fostering job creation and growth. However, malicious actors are also increasingly innovative, engaged in a race for new ways to launch digital security attacks against businesses, governments and individuals. To win this head to head race against malicious players, the market should provide more innovative digital security tools. Innovative products, including IoT and AI-enabled devices, should also be designed with enhanced security from the outset ("digital security by design"). The report of the event focuses on ways to encourage digitial security innovation.

We are at the early days of digital security innovation. All stakeholders still have a lot to learn about the role they should play to further stimulate innovation.

While there is a huge potential for digital security innovation, there are also many obstacles. Funding does not seem to be the major challenge as digital security innovation can attract a lot of capital, although this may vary across countries.

Governments can play a key role to remove obstacles and foster digital security innovation through a mix of policy tools ranging from tax incentives to acting as an early customer for innovative products.

Regulation can stimulate demand. However, it needs to be flexible and outcome-based.

Building a digital security innovation ecosystem is essential

The creation of one (or more) digital security innovation ecosystem is the most important component of a strategic approach to digital security innovation.

An ecosystem brings together different stakeholder groups, generally in a dedicated geographic location to facilitate synergies between them. Figure 1 illustrates the roles of each stakeholder in an ecosystem and how they relate to one another. A connector or facilitator is key to to bind them and keep them focused on responding to the market.

For example, Cyberspark in Be'er Sheva, Israel is a dedicated cybersecurity innovation ecosystem. The Israeli experience with Cyberspark shows that it takes time to build an ecosystem. It also requires an overarching strategic vision for digital security.

While governments can learn from successful models of innovation ecosystems, **it is not possible to simply copy an ecosystem** development strategy from one country to another and expect the same outcome.

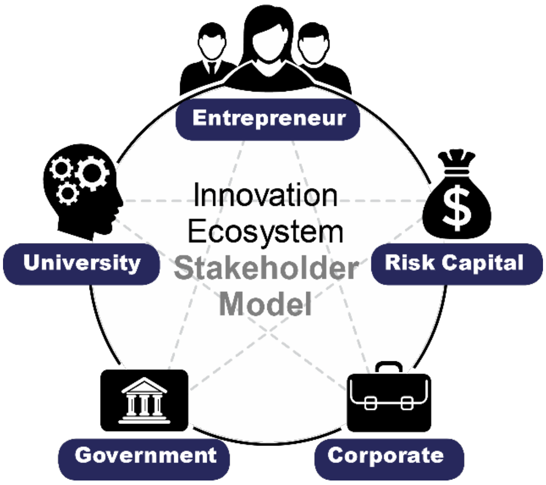

Figure 1 - MIT's Five Stakeholder Model for Innovation Ecosytems

Co-operation is essential for digital security innovation

Co-operation among stakeholders within an ecosystem and between ecosystems is crucial.

Global Epic logo

The Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global Epic) facilitates co-operation between digital security ecosystems across the world. This initiative began with leaders of ecosystems coming together to discuss best practices and, as of 2019, it had over 27 members from 15 different countries and 3 continents. Such partnerships can stimulate digital security innovation by the sharing and comparing of best practices.

The European Cyber Security Organisation (ECSO) is a three years old public-private partnership that coordinates the innovation roadmaps and investments in the EU, bringing many different voices in the discussion: academia, industry, SMEs and EU Member States. ECSO is an example of companies and other stakeholders coming together to enhance digital security. SMEs can learn a lot from ECSO's membership that would not have been available to them otherwise. Such initiatives show that it is possible to develop a common understanding of what different countries and stakeholders can do together.

Human capital and the role of government

Human capital is another major factor in fostering digital security innovation. To succeed as entrepreneurs, digital security experts need to venture outside their area of expertise and acquire business management, marketing and communication skills.

Further educational efforts, upskilling and reskilling can partly address the current digital security skill shortage.

Governments can also provide **support to disadvantaged groups** to take advantage of hidden talents, and **give underground "hackers" a chance** to move to the legal side and become innovative entrepreneurs.

Governments can encourage digital security by design in innovation more generally. Examples include Israel's integration of digital security at the core of its countrywide smart transports initiative, Japan's combination of Internet of Things (IoT) regulation and industry-based guidelines, and the United Kingdom's procurement policy which requires small- and medium-sized enterprises (SMEs) and supply chain actors to comply with the Cyber Essentials scheme to become a government supplier.

UK's Cyber Essentials scheme logo

The full report on Encouraging Digital Security Innovation is available here.

The OECD Global Forum on Digital Security for Prosperity

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

Outputs from these debates influence international public policy discussions and can lead to the development of analytical work, principles and international policy recommendations, at the OECD and in other international fora.

GLOBAL FORUM ON DIGITAL SECURITY FOR PROSPERITY

https://oe.cd/gfdsp