GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

13-14 MARCH 2023
OECD HEADQUARTERS | PARIS, FRANCE

OECD
BETTER POLICIES FOR BETTER LIVES

2023 OECD Global Forum on Digital Security for Prosperity Session Themes

Theme 1: As policymakers move to implement security policies, how can we ease the implementation of better practice across the Internet of Things?

The Internet of Things (IoT) is a rapidly growing area of emerging technology. Estimates vary, but there are expected to be over 75 billion connected devices worldwide by 2030. In many cases, the level of security within these devices is lower than their end users expect, and the presence of basic security flaws leaves individuals, businesses and organisations vulnerable to a range of harms.

The Mirai DDOS attack helped to focus the attention of policymakers, and a range of policy initiatives are underway in the European Union, Japan, the United Kingdom, the United States, Australia, Singapore, India, Finland, Germany and many other jurisdictions.

There is a great deal of consensus already. All approaches agree that universal default passwords in products add needless risk, and that products are more secure when their manufacturers abide by strong and coordinated processes to manage vulnerabilities. There is also agreement on the importance of software updates and 'patching' to address these vulnerabilities, as well as a number of globally applicable Technical Standards in this sector, from ISO 29147 and 27402/4 to ETSI EN 303 645, and a range of mapping options, that show consensus between these Technical Standards.

2023 is a landmark year, as many of these policies are now implemented into law and consumer-facing approaches, including labelling, which is taking place in Finland, Singapore and Germany, and work is underway in the United States and Japan. There is a risk that the slightly differing approaches in each country are increasingly viewed as 'fragmentation', and that this will cause confusion among businesses and introduce inefficiency into the economy.

Key questions for discussion at the Global Forum:

1. What can my organisation do now to support better security practices for the IoT?
2. How can we better amplify the consensus between technical standards and legislative approaches?
3. How can we move 'beyond the baseline' and support the future development of products and services with quality security, embedded in the design?

Theme 2: How can a 'secure by design' approach be embedded within Artificial Intelligence policies?

Artificial Intelligence is one of the most exciting and fast paced areas of technology, with the potential to revolutionise virtually all aspects of economies and societies. As this technology is being embraced around the world, there are important security considerations.

Whilst AI can be used as a tool within security, other important questions are how policy makers can apply the lessons learned from the broader security policy work in emerging technologies, and how a 'secure by design' approach can be embedded across AI technologies.

Put simply, 'secure by design' is an approach within policymaking that seeks to protect end users from harm whilst protecting innovation within the emerging technology and maintaining the capacity to adapt to an ever-changing threat landscape.

The potential threats facing AI are numerous, one example being the poisoning of the data, which has great potential for harm. This session will seek to identify key considerations for policymakers, as well as identify a working model for how international consensus can quickly be delivered in the area of security risks in AI.

Key questions for discussion at the Global Forum:

1. What lessons can we apply from the development of security policies across other elements of emerging technology to better embed security into AI? What are the key challenges?

2. How can a 'secure by design' policy-making approach, that seeks to find the proportionate balance between protecting users and enabling innovation, be embedded within AI policies?

Theme 3: How can we better promote collaboration between the technical and policy making communities to address future security challenges within new and emerging technologies?

Digital security within new and emerging technology is not just a technical issue, but a social, economic and fundamentally human concern. Developing effective policy within this space is a team effort that requires effective partnerships between policy makers, academia, industry, civil society groups and the technical community.

As the security and policy space has grown in recent decades, the criticality of that last community has become more and more evident. And yet, historically, it has not been easy for the security community to engage directly with policymakers. Established elements of the security community, such as the Def Con conference, have been increasingly focusing on the role of security within policy, and how this community can be more present in supporting policy makers.

Key questions for discussion at the Global Forum:

1. How can my organisation better engage with security agencies or the security community?
2. What have I seen work well in previous interactions or working relationships between the security and policy community?
3. What opportunities are there to deepen this partnership, at a domestic or international level, so as to promote more effective policy responses to future challenges in new and emerging technology?