Managing Digital Security and Privacy Risk for Economic and Social Prosperity
Objectives

The evolving digital economy, related innovation and emerging technologies present substantial opportunities for economic growth and enhanced societal benefit. To flourish, the digital economy requires effective digital security risk management and protection of privacy. However, digital incidents and threats to economic and social activities continue to grow in number and sophistication, with significant consequences. Public and private organisations, including those supporting critical infrastructures may suffer disruption of operations, direct financial loss, liabilities, damaged reputation, loss of competitiveness or of trust. Unauthorised access, destruction, use, modification or disclosure of personal data may also impact and violate individuals' privacy. With the ever more extensive large-scale collection and analysis of data, more attention must be given to addressing possible unanticipated and undesirable uses of personal data.

It is essential to address digital security and privacy risks as an economic and social risk at the highest level of leadership. The panel will identify strategies, policy measures and action plans to address these risks and strengthen trust while enhancing the benefits for the economy and society and taking into consideration the opportunities for innovation. It will discuss ways to develop national digital security strategies with a view to economic and social prosperity and to helping small and medium sized enterprises (SMEs) manage digital security risk. The panel will also discuss ways to leverage complementarities between digital security and privacy risk policies at national and international levels.

Key issues

Many countries have developed national digital security strategies, but too few of them are designed to manage digital security risk to support economic and social prosperity.

To optimise the economic and social benefits anticipated from an open digital environment, leaders and decisions makers should not treat digital security risk solely as a technical issue but adopt an economic and social risk management approach. Broad adoption of such an approach will require multi-stakeholder, interdisciplinary and international co-operation. Sharing of best practices and of robust evidence will facilitate the development of policies and their implementation.

Q1: How can national digital security strategies best foster economic and social prosperity?

Q2: How can co-operation across all sectors and stakeholders, including at the international level, facilitate the adoption and implementation of digital security risk management approaches for economic and social prosperity?
SMEs face distinct challenges for managing digital security and privacy risks and warrant particular attention.

SMEs, particularly high-growth innovative firms, are vital to economic growth, help drive competition and innovation, and make a strong contribution to job creation. The digital economy provides them with new opportunities to improve productivity and transform their business models. However, they often do not sufficiently understand how digital security and privacy issues can create economic risks, and have limited capacity to respond to and manage them. While different types of SMEs face different challenges, all would benefit from integrating digital security and privacy risk management into their business decision-making. In particular, SMEs that participate in value chains may inadvertently introduce vulnerabilities that may affect other participants. Greater awareness of these risks, development of scalable approaches to digital security and privacy risk management approaches, and effective SME-oriented guidance tools will be essential to increase accountability. In this regard, businesses and governments in developed and emerging economies might form formal and informal partnerships for greater awareness, education and skills. In addition, targeted incentives or mechanisms such as insurance can encourage the adoption of good practice.

Q3: What steps can be taken to help SMEs effectively manage digital security risk and protect privacy?

Digital security and privacy risks are inter-related but are still addressed at different policy levels and separately.

The relation between digital security and privacy risk has long been recognised, for digital identity management and cryptography policy, for example. However, stronger and better leveraged synergies between security and privacy policy approaches could be achieved, and co-operation among relevant actors could be increased. In contrast to digital security risk, which is addressed through national strategies, legislation continues to be the main response to digital privacy risk in many countries. While legal protection is essential, privacy in an increasingly data-driven economy would benefit from a multifaceted strategy, along the model of digital security strategies. This could strengthen protection and provide the flexibility needed to benefit from emerging technologies. Such strategies would also help support efforts by privacy enforcement authorities and others to foster privacy risk management. Interoperable privacy approaches and frameworks can enhance protection of personal data across jurisdictions and reduce uncertainty for trans-border data flows.

Q4: How can synergies between digital security and privacy risk policies at national and international levels best be leveraged?

Q5: How should privacy strategies be developed to respond to personal data protection challenges in a data-driven economy and society?

Q6: What economic and social benefits have been derived from national digital security strategies and what lessons can be learned for national privacy strategies?