8.6 Digital security in businesses

Why are indicators on digital security in businesses needed?

Digital security incidents expose individuals, businesses and governments to a variety of risks and attacks that target digital-dependent critical infrastructures and essential services such as energy, transport, finance and health. They can undermine business competitiveness, the ability to innovate and position in the marketplace and threaten the core functioning of economies and societies. Effective digital security risk management is essential for businesses to be able to minimise the frequency and negative impact of these incidents and thereby take advantage of and thrive during digital transformation.

Digital security threats and incidents continue to grow in number and sophistication, with significant consequences. For example, according to the 2017 Allianz Risk Barometer Survey, the perceived risk related to cybercrime and digital security incidents remained the third highest global business risk in 2017 for the second year in a row, up from 15th in 2013 (Allianz, 2016; 2017). Concurrently, the probability of a massive incident involving data fraud and theft was ranked fifth by the 2017 World Economic Forum Global Risks report, (WEF, 2017).

Digital security risk is a concern shared by the entire business community, but one that may have especially serious consequences for smaller businesses. While large businesses and organisations likely have the institutional and financial capacity to develop appropriate digital security risk management, studies in a number of OECD countries suggest that this is not the case for small and medium enterprises (SMEs), and particularly micro-enterprises, which can face managerial, skill, knowledge and financial constraints.

The scarcity of reliable evidence on which to base digital security risk management decisions and public policy actions calls for metrics and analytics to understand different digital security risk management practices, both in small and larger firms, within a context of rapid technological change.

What are the challenges?

While the frequency and severity of digital security incidents has grown, the ability to measure, analyse, understand and manage them efficiently has not kept pace. At a methodological level, there is a lack of consensus on definitions, typologies and taxonomy, as well as a paucity of historical data on digital security incidents, threats and vulnerabilities. Concepts such as threats, vulnerabilities, incidents and impacts are often used together under broad, all-encompassing terms. This lack of standard definitions has led to uncertainties regarding both the frequency and impact of digital security risk and has prompted calls for a more uniform approach.

The development of a more reliable and comprehensive dataset on digital security incidents and digital risk management practice requires a consensus on typology and taxonomy, a trusted public-private digital security incident repository and incentives to promote reporting of incidents and data sharing by organisations.

At an organisational level, improving information-sharing practices on digital security risk is a cornerstone of national digital security strategies of many OECD countries. In spite of the increasing numbers of collaborative information-sharing platforms and networks, how an organisation captures, stores and uses data, shares information and intelligence, and increases knowledge is frequently subject to substantial impediments.

Options for international action

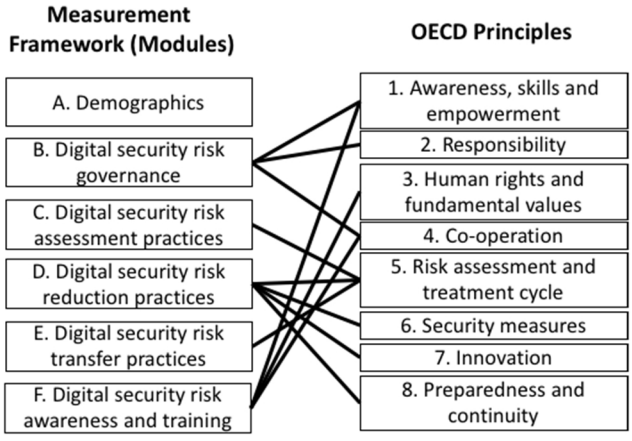
A number of different fora and initiatives by government, academia, the insurance sector and other private sector stakeholders are exploring ways to meet the requirements for establishing a typology of incidents, incentives for incidence reporting and data sharing. The value proposition of a data repository for information on digital security incidents, including possible data requirements and system attributes, is also being discussed by insurance companies and governments in a number of countries, such as France, the United Kingdom and the United States. The OECD has started to examine these various initiatives as part of its work on improving the evidence base on digital security and privacy policy-making following the 2016 Cancun Ministerial on the Digital Economy and in the context of an OECD project on the digital security insurance market.

In this context, the OECD first reviewed existing surveys that had sought to provide data related to digital security risk. It was found that past surveys typically included few questions on the digital security risk management practices of businesses and where they did, such questions were often limited to technical measures. This is not in line with the 2015 OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity ("Security Recommendation"), which emphasises the economic and social dimensions of digital security risk (OECD, 2015).

Once the deficiencies in the evidence base had been identified, the OECD sought to improve measurement in this area by developing a framework to assess the digital security risk management practices of businesses. This measurement

framework comprises six modules and 18 associated indicators. It draws heavily on the Security Recommendation, as shown in the figure below. Following the OECD model survey framework, national statistical offices or other organisations could adopt the individual modules, as necessary.

Mapping of the measurement framework with the OECD Principles on Digital Security Risk Management for Economic and Social Prosperity



Source: OECD (2019).

Finally, a survey instrument was designed with the goal of understanding the digital security risk management practices the specific population of risk managers. This survey instrument was subjected to cognitive testing in Brazil by Cetic.br in March-April 2018. It has then reviewed and piloted by the Federation of European of Risk Management Associations (FERMA) between July and September 2018. The outcomes of the pilot suggest that the measurement framework based on the OECD Security Recommendation is robust. However, improvements could be made to the design of the survey instrument. These changes primarily relate to the length of the survey in terms of the time required to respond and slight adjustments to the questions and their response options. A simpler version of the survey would allow for the collection of information from less data-intensive firms that may not necessarily have a dedicated person or unit responsible for digital security risk management (OECD, 2019).

The OECD has long supported co-operation on the management of digital security risk for economic and social prosperity, alongside other organisations that focus on defence and international security, criminal law enforcement and technical standards. The OECD has produced analyses and Recommendations since the early 1990s. This dialogue, inclusive of all stakeholders, has proved instrumental in developing digital security policies that build trust in the global digital environment, while preserving Internet openness, innovation and digitally driven growth.

In this respect, the recently launched Global Forum on Digital Security for Prosperity (http://www.oecd.org/internet/global-forum-digital-security) represents another milestone, as it engages stakeholders in a collaborative process to build partnerships and share experiences and good practice on digital security risk and its management. The Forum does also help to consolidate a network of governmental officials and non-governmental experts dealing with digital security for prosperity in OECD and partner countries and facilitate a convergence of views towards building a trusted and resilient digital environment.

References

Allianz Global Corporate & Specialty (2017), *Allianz Risk Barometer: Business Risks 2017*, Allianz Global Corporate & Specialty SE, Munich, https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf.

Allianz Global Corporate & Specialty (2016), *Megacities: Pushing the Boundaries of our Industry*, Allianz Global Corporate & Specialty SE, Munich, https://www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Megacities_The_future_risk_landscape.pdf.

OECD (2019), "Measuring digital security risk management practices in busineses", OECD unclassified document, DSTI/CDEP/SPDE/MADE(2018)2/FINAL.

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264245471-en.

WEF (2017), Global Risks Report 2016: 12th Edition, World Economic Forum, Geneva, http://www3.weforum.org/docs/GRR17_Report_web.pdf.