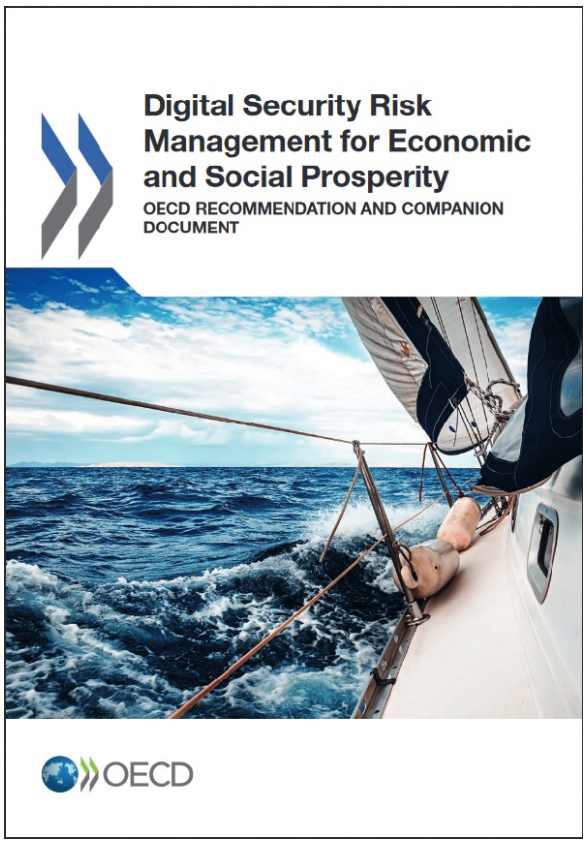
Digital security

Last update: 14 March 2017



While the digital world is a driver of innovation and productivity, it raises the issue of digital security, since online vulnerability can lead to financial, privacy and reputational damages.

Examples are not hard to find, whether among firms, government or individuals. In 2012, it took over two weeks for the oil company Saudi Aramco to recover from the erasure of over 30 thousands hard drives connected to its internal networks by digital intruders. Digital security incidents can have far-reaching consequences for private companies, for instance in terms of loss of competitiveness–in case of theft or trade secrets–or disruption of operations, through denial of service or sabotage. In 2007, massive cyberattacks against Estonia affected the parliament and ministries, along with banks, newspapers and broadcasters. People's personal data is constantly at risk of privacy breaches, from bank account to medical details, with potential material or moral damage. And people can also be victims of financial fraud.

The growing volume of incidents and their increased sophistication result mainly from the migration of organised transnational criminal groups' activities online. Other drivers include cyber terrorism, industrial digital espionage and "hacktivism"–the subversive use of computer networks to promote a political cause.

Although rare, digital security incidents could even cause loss of human life, considering the increasing reliance of transportation systems and hospitals on well-functioning information and communication technologies and infrastructures.

The OECD, whose last Recommendation on digital security was in 2002, offers eight principles to guide digital security risk management, including on the responsibility of different actors, cooperation between stakeholders and the role of innovation. It recommends that countries adopt national plans to identify measures to prevent, detect, respond to and recover from digital security incidents and to treat security as an economic risk.

See www.oecd.org/internet/ieconomy/

References

Digital Security Risk Management for Economic and Social Prosperity http://dx.doi.org/10.1787/9789264245471-en