2 Digital security in SMEs

This chapter covers the key issues surrounding digital security in small and medium enterprises (SMEs). It discusses the challenges raised by the changing nature of incidents, the prevalence and costs of cyberattacks and human errors, and their incidence on SMEs. It highlights the growing exposure of SMEs as digitalisation increases the economic value of data, and their reliance on software code and connectivity. It identifies how the COVID-19 pandemic gave opportunities for hackers to intensify attacks. It looks into SME practices in terms of securing systems and data, and gaps vis-à-vis large firms. Finally, this chapter presents the rationale for better digital security policies, and how governments have attempted to improve risk management amongst SMEs. Initiatives include legislation; certification schemes and education and awareness campaigns to encourage uptake; incentives to develop business solutions and "security by design"; and the mainstreaming of SME policy considerations in national digital security strategies.

In Brief

Highlights

- **Cyber-attacks are a constant threat to enterprises**, with criminal organisations likely to be responsible for over half of the incidents reported in 2020. Financial profitability is the main motive for these criminals.
- **Most products or services that contain software code contain vulnerabilities**. Nowadays, all enterprises, regardless of size or sector, can be exposed to malicious attacks that seek to exploit these vulnerabilities in web applications, devices or servers.
- **The ideal target is a vulnerable organisation with valuable data** (e.g. credentials or personal data). Some sectors tend to be more exposed and are more targeted than others, i.e. those that are digitally intensive, process sensitive or large volumes of data and have large cash reserves.
- **SMEs tend to be less digitally intensive** (and possibly have lesser ability to detect security incidents) but some factors increase their probability of suffering an incident, e.g. the nature of their business, their sector of activity or immaturity in their digital security practices.
- **The digital transformation increases SME exposure to digital security risks and likelihood to be victims of cybercrime** by making them more exposed to digital security incidents and making them more reliant on digital technology. The Internet of Things increases digital connectivity, the number of vulnerabilities to exploit and the potential frequency or probability of attacks. Cloud computing is resulting in increased migration of sensitive data to external parties to the enterprise in question, which means that security and protection of that data are technically managed by an external party. Artificial intelligence can enhance the capacity of digital security teams but also be undermined by data poisoning and leveraged by cybercriminal organisations.
- **The COVID-19 crisis has made more businesses reliant on digital technology than before**. This is an opportunity for malicious actors to intensify cyber-attacks e.g. phishing then fraud. Some of these attacks targeted sectors where social distancing and disruptions in supply chains imposed a rapid shift towards digitalisation and working from home, e.g. retail trade, professional services. This increased reliance also makes the potential impact of disruptions more serious (i.e. business interruption).
- **Threat actors increase their sophistication over time as detection and mitigation measures improve**. Malicious techniques therefore evolve continuously requiring more advanced risk management capacities that smaller firms are less likely to have first. Phishing, ransomware, and denial of service attacks continue to be the most prevalent methods.
- **Economic damages from malicious and non-malicious incidents add up to large amounts** and can include hidden costs or under-stated losses. Absolute costs increase with firm size and a small proportion of enterprises incur the lion's share of total economy-wide incidents and losses. When affected by rare but very costly incidents, SMEs can incur costs that add up to several months of revenues. In addition, weak digital security practices may become a barrier to them to building networks with larger enterprises, multinationals and business partners.
- However, **measuring the prevalence and costs of digital incidents remains a challenge due to a lack of international standards and comparable data**. Therefore, the data available need to be interpreted with caution.

- **SMEs tend to have less comprehensive and sophisticated digital security risk management practices**. They often do not have a dedicated person in-house, they tend to seek less information from external sources and do not tend to have formal procedures in place to detect intrusions. They also tend to invest less in digital security, due partly to their lower relative size by revenue, although this varies between sectors and countries.
- **SMEs tend to delegate responsibility for their digital security** either explicitly to implicitly to external third parties. In the former case, this might involve hiring external security consultants. The latter case involves purchasing digital products or services where the security design choices are made by the designer. This limits the control that SMEs have over the security of their products and services and makes them reliant on the choices made by other stakeholders.
- **SMEs have to integrate digital security risk management into their business decisions and processes** in order to sufficiently reduce the risk they incur and the risk they may pose to others. They also have to see digital security as an investment rather than a cost centre. As SMEs go digital, an early change in culture and practices is increasingly critical.
- **Governments increasingly aim to encourage the adoption of better digital security practices in SMEs** through certification schemes, security standards, or by enforcing personal data protection regulation, or raising awareness and building business competences on digital security. Governments' initiatives are often not specific to SMEs, or not specifically designed towards this segment of the business population.
- **Governments also support the supply-side**, through incentives for developing business solutions that could help SMEs improve digital security risk management, or for producing more secure digital products ("security by design").
- **The mainstreaming of SME policy considerations in national digital security strategies is emerging as a key topic**. The OECD Recommendation in the area insists on considering SMEs in strategy design and implementation, especially because of governance failures between digital security agencies and SME policy instances.
- **The challenges at stake call for enhanced co-operation and knowledge exchange between stakeholders**. Within industries where actors share similar business models; between SMEs and large firms that share similar threats with different and potentially complementary response capacity; across jurisdictions that face no-border attacks; etc.

Introduction

We are at dawn of a new industrial era. Emerging digital technologies, such as artificial intelligence (AI), 5G or The Internet of Things (IoT), are opening tremendous market opportunities and creating entirely new industries, but, in turn, raise new - or amplify existing - digital security risk. As small and medium-sized enterprises connect to the digital world and move towards new digital practices, they will need to effectively manage digital security risk so as to be able to reap the benefits of the digital transition.

Yet, some SMEs do not have the awareness, resources or expertise to effectively assess their digital risk exposure and to implement appropriate prevention and remediation measures. Relatively poor or inadequate digital security risk management practices could have far-reaching consequences since smaller firms may not have the capacity to weather – even temporary - losses of reputation, consumer trust or revenues following serious incidents. The risk is particularly pronounced in sectors where SMEs tend to rely on sensitive or valuable data, or process significant volumes of data, such as professional services, healthcare and retail trade.

This document discusses the challenges raised by digital (in)security, the changing nature of incidents, the prevalence and costs of attacks and human errors, and their incidence on SMEs. It highlights the growing exposure of SMEs as digitalisation increases the economic value of data, and their reliance on software code, data and connectivity. It identifies some of the ways that the COVID-19 pandemic gave opportunities for malicious actors to intensify attacks. It also looks into SME practices in terms of securing systems and data and gaps vis-à-vis large firms. Finally, it presents the rationale for digital security and data protection policies towards SMEs and provides examples of such government policies across the OECD area.

Digital security: Challenges for SMEs

Nature and evolution of digital security risk

Digital security incidents harm businesses, governments and individuals by undermining the availability, integrity and/or confidentiality (the so-called "AIC triad") of their data, information systems and networks. A data breach is a specific sub-class of incident affecting the confidentiality of data that results in the disclosure of data to an unauthorised party. As a consequence of digital security incidents, victims can face tangible and intangible damages, ranging from monetary losses, reduced competitiveness, reputational damages, interruption of operations, privacy breaches, etc. (OECD, 2020[1]).

Digital security risk results from incidents caused by threats exploiting vulnerabilities. Threat sources include governments, groups and individuals with malicious or ill-intentioned and/or criminal purposes. Their motivations vary, but typically include geopolitical goals for governments, profit making for criminals, ideology for hacktivists, violence for terrorists, personal aims for thrill seekers, and discontent for insider threats.

Incidents can also result from unintentional events such as human error, system bugs or external non-malicious causes (e.g. power outage, lightning strikes, solar flares). These events might however be initiated by an external malicious actor through social engineering methods, like phishing (Box 2.1). However, due to the way in which digital systems and software are designed, users of these technologies might make mistakes and cause financial costs or losses. The systems themselves might fail due to a bug or other fault. Finally, non-malicious external forces might cause system failure e.g. power outage, lightning strikes, solar flares.

Box 2.1. Digital security threats: Typology and trends

Distributed Denial of Service (DDoS) attacks are still common, but large-scale ones are rarer, signalling a reluctance of attackers to attract attention from law enforcement for attacks that are disproportionate in light of their benefits. DDoS attacks are a common type of incident that disrupts the availability of an online service by flooding it with illegitimate requests, most often to extort money from victims. To launch these attacks, malicious actors often leverage botnets, i.e. large networks of compromised devices called drones or zombies.

Phishing remains high and is increasingly difficult to detect by humans. Phishing is a method whereby an attacker disguises oneself as a trustworthy entity in an online communication to obtain sensitive information, e.g. usernames and passwords, or to deliver malicious code, i.e. "malware". There are different types of phishing attacks, from broad untargeted campaigns aiming to collect credentials by directing users to fake e-commerce or financial web sites, to more sophisticated spear-phishing emails targeting specific individuals to plant malware in their organisation's information system. Spear-phishing remained the most popular avenue for targeted attacks in 2018 and was used by 65% of all known cybercrime and State-sponsored groups ((Symantec, 2019[2]). Phishing was present in 78% of digital

security espionage incidents (Verizon, 2019[3]). Yet, the frequency of phishing attacks is unclear, due to the absence of common definitions and measurement techniques. In addition, phishing has become increasingly sophisticated. Messages can include links to malicious sites that are difficult for end users to detect without some automated protection. The presence of a Secure Sockets Layer padlock pictogram, a standard security technology for establishing an encrypted link between a server and a client, is no longer sufficient to trust a hyperlink, since an increasing number of phishing sites are hosted on sites using technically valid digital certificates (OECD, 2020[4]).

Ransomware attacks become more targeted. Ransomware is a type of malicious software that limits or disables the accessibility of data and demands a ransom for recovery. Ransomware can be delivered through a phishing attack. Ransomware attacks are a form of digital extortion (ANSSI and BSI, 2018[5]). In 2017, the Wannacry and NotPetya attacks hit media headline, as they caused billions of dollars of damage to large businesses such as Boeing, Beiersdorf (Nivea), Deutsche Bahn, DHL, FedEx (USD 400 million), Honda, Renault, Merck (USD 870 million), Mondelez, Petrobras, PetroChina, Saint Gobain (USD 384 million), and AP Moller Maersk (USD 300 million) (Greenberg, 2018[6]). In both cases, the malware was designed to rapidly spread inside and outside victims' networks, to encrypt files and to ask for a ransom in exchange for a decryption key. Public sector organisations such as the National Health Service in the United Kingdom and the Russian Interior Ministry were also affected (RT World News, 2017[7]). The impact on SMEs is unknown. To increase the likelihood of a ransom being paid, cybercriminals have been more and more choosing their victims among organisations that rely on ICTs and are known to pay less attention to digital security. As a result, ransomware attacks evolved to become more targeted. In 2018 and 2019, ports, airports, hospitals, healthcare organisations, and local governments were targeted with ransom claims ranging from USD 5 000 to USD 5 million, and around USD 1 million on average, depending on the size of the city (Kaspersky, 2019[8]). Plants and manufacturing installations can also be paralysed if attackers get access to the IT system and operational infrastructure that pilot physical installations.

Malware is malicious code that is always evolving to evade detection techniques and adapt to new targets and technologies. Techniques have considerably improved, from encrypted to polymorphic and metamorphic. Encrypted malware is the first step to evade signature-based detection. At each infection, the malware is encrypted with a different key, making each file unique. However, security tools can still detect the decryptor included in the code that remains the same across infections. Polymorphic malware can create a countless number of decryptors using a mutation engine. As more sophisticated anti-malware software can still detect polymorphic malware, attackers have developed metamorphic malware that can completely rewrite its code so that each new version of itself propagated elsewhere no longer matches its previous iteration without using encryption (You and Yim, 2010[9]). In 2017 and 2018, according to Webroot (2019[10]), 93% of malware were polymorphic, i.e. impossible to be detected by simple signature-based security tools.

Source: Abridged from OECD (2020[1]), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en.

Cyber-attacks often involve human error

Measuring the prevalence and costs of digital incidents remains a challenge due to a lack of international standards and comparable data (Box 2.2). The data available need to be carefully interpreted because enterprises either do not understand their real risk exposure; or do not detect incidents; or do not measure their impact in a standard way; and might not report them at all. Nevertheless, when carefully interpreted, some trends do emerge from the evidence.

Verizon, a large US telecommunications enterprise, recently released its Data Breach Incident Report for 2020 (Verizon, 2020[11]). Data come from a broad spectrum of government and non-government representatives across 81 countries. Keeping in mind the methodological issues related to measuring

digital incidents (Box 2.2), the authors found that 70% of breaches were perpetrated by external actors. Of those, 55% were organised criminal groups. However, errors are also commonplace, responsible for 22% of breaches, which make them more common than malware, i.e. malicious code (Verizon, 2020[11]). For instance, vulnerabilities arise when a system administrator neglect to put in security controls to limit access to the company's data posted on a cloud platform (misconfiguration), or the threat increases when sensitive data goes to the wrong recipient(s) as the autocomplete "To:" or "Cc:" field directs an email to the wrong party (misdelivery). In other instances, it could be a mass-mailing misstep where the addresses are no longer paired with the correct contents. These errors, including incorrect administration, accidentally exposing hosts, or misconfiguration of protocols and controls, may be linked to a rapid shift to the cloud and a general lack of understanding of securing cloud environments and services.

Box 2.2. Measuring digital security incidents and data breaches: A lack of comparable evidence

Some data in this report come from a variety of surveys undertaken in OECD countries (Table 2.1). The best of efforts has been made to cite sources with representative samples; clear and well-defined questions; and results are broken down by enterprise size. However, there is still a lack of internationally comparable data on digital incidents and data breaches (OECD, 2019[12]).

Between 2016-18, the OECD Working Party on Security and Privacy in the Digital Economy (SPDE) and the OECD Working Party on Measurement and Analysis of the Digital Economy (MADE) developed a measurement framework and survey questionnaire to help collect more comparable and better quality data in this area. To date, few OECD countries have implemented this approach. This limits the scope of countries included in this paper.

Data on digital security incidents come with several methodological issues (OECD, 2019[12]), such as non-randomised and non-representative sampling, under-reporting due to reputation or legal concerns, or uneven detection and measurement capabilities across enterprises. In addition, coverage by firm size is heterogeneous across sources (Table 2.1). Surveys used herein have been selected because they do not suffer from the non-representative and, for the most part, non-randomised sampling issues that are common amongst the literature and studies on digital security and data protection. Nonetheless, trends described in this document tend to be consistent between enterprises of the same size or the same industry across OECD countries.

With all these caveats in mind, data herein should be interpreted as a "floor" (i.e. lower-bound) estimates of the number of incidents experienced, the losses incurred and the security measures implemented.

Table 2.1. Data sources on digital security incidents and breaches

Organisation	Survey name	Geographical coverage	Year(s)	Firm size definition
Verizon	Data Breach Investigations Report	International	2019-20	Employment-based - Small < 1 000 employees; large 1 000 or more.
NetDiligence	Cyber Claims Study	International	2019	Revenue-based - SMEs less than USD 2 billion annually.
Eurostat and national statistical agencies	Community Survey of ICT Use in Businesses	EU28	2015 and 2019	Employment-based - Micro [1 to 9 employees]; small [10 to 49], medium [50 to 249] and large [250 or more].
Ipsos Mori for the UK Department for Digital, Culture, Media and Sport	Cyber Breaches Study	United Kingdom	2017-19	Employment-based - Micro [1 to 9 employees]; small [10-49]; medium [50-249]; large [250 employees or more].
Statistics Canada	Survey on Cyber Security and Cybercrime	Canada	2018	Employment-based – Small [1-99 employees]; medium [100-499]; large [500 and more].

Monitor Deloitte for the Danish Business Agency	IT Security and Data Management in Danish SMEs	Denmark	2018	Employment-based – Micro [5-9 employees]; small [10-49]; medium 50-249].
Bank of Italy (Biancotti)	The price of cyber (in)security: Evidence from the Italian private sector	Italy	2018	Employment-based – bands are 20-49 employees; 50-199; 200-499; 500 and over.
Australian Institute of Criminology	Australian Business Assessment of Computer User Security (ABACUS) survey	Australia	2009	Employment-based - Small [0-19 employees]; medium [20-199 employees]; and large [200 or more].
Bureau of Justice Statistics	National Computer Security Survey	United States	2005	Employment-based (excluding sole traders) – Small [25-99 employees], medium [100-999], large [1 000 and more].
Cyentia Institute	Information Risk Insight Study	United States	2020 (based on data from 2009-19)	Revenue-based with explicit numerical bands.

Threats are increasingly sophisticated and difficult to detect and defeat

Some kinds of cyber-attacks become increasingly targeted and sophisticated over time, making it more difficult for businesses, organisations and governments to detect and defeat them. Malicious attacks, techniques and approaches evolve continuously in order to escape law enforcement, circumvent progress in digital security prevention and protection and better adapt to their targets' vulnerabilities.

However, attackers first try the old and cheap methods of attack, and only increase in sophistication when gains worth it. Many enterprises, especially the smaller ones, fall to simple basic attacks because they lack the baseline protection and a minimum digital "hygiene". More sophisticated approaches tend to target those firms that have already reached this baseline level. Phishing, denial of service and ransomware attacks continue to be prevalent in the digital landscape (OECD, 2020[1]).

Most products that contain software code have vulnerabilities

High-profile attacks, such as the ransomwares WannaCry and NotPetya, highlighted significant digital security gaps in thousands of businesses and public sector organisations, in particular regarding the end-of-life of products that contain software code. According to estimates, there are between 20 and 100 flaws in every 2 000 lines of code (Dean, 2018[13]), down to one flaw in every 2 000 lines if "security by design" guidelines are followed (DHS and DoC, 2018[14]). To put things in perspective, an average iPhone app has around 50 000 lines of code, while Android has around 12 million and Windows 10 counts more than 50 million. On average, 46 new vulnerabilities are discovered and publicly disclosed every day, including for widely used products such as Android, iOS or Windows (NIST, 2020[15]).

Products are increasingly digital-intensive and entire sectors are digitally dependent (OECD, 2021, forthcoming[16]). On the consumer side, traditional goods are becoming "smart", i.e. contain code and can interconnect (e.g. connected cars and home appliances). The number of connected devices is expected to reach 20 billion globally in 2020 (Schneier, 2018[17]). On the business side, companies increasingly use software to perform core functions such as production and distribution (see Chapter 1 on SME digital uptake and Chapter 5 on AI), and they increasingly rely on the development of cloud computing and subscription-based models for software for their daily operations.

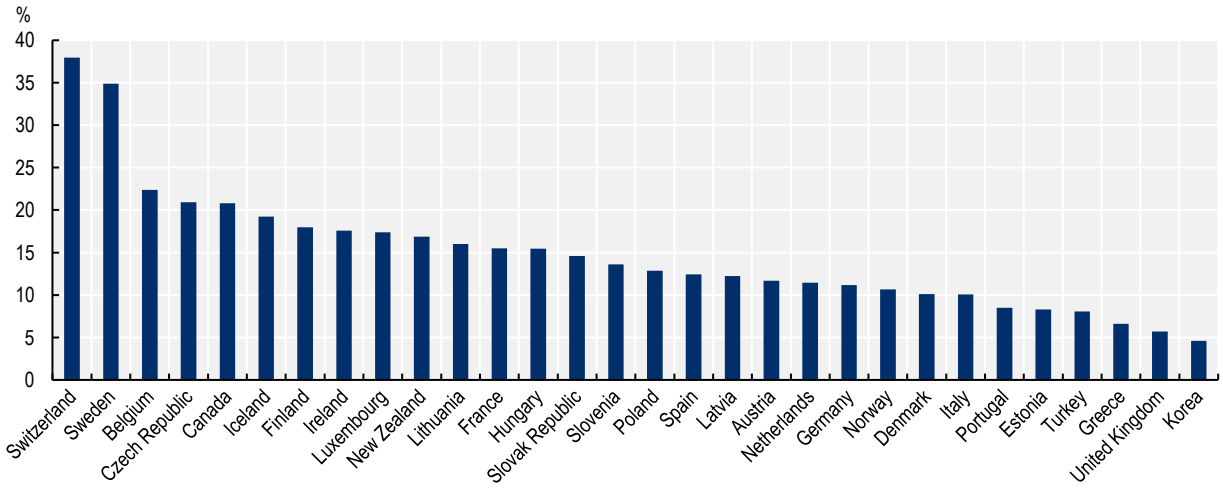
Prevalence and costs of digital security incidents

Nowadays, organisations regardless of size, are troubled with attacks on web applications, user devices, servers and people (social engineering attacks). Estimates vary drastically across sources but figures remain substantial. In Europe, the share of firms having experienced ICT security incidents in 2019, such as unavailability of ICT services, destruction or corruption of data, or disclosure of confidential data, is on

average of 13%, but ranges from 6% (United Kingdom) to 35% (Sweden) (Eurostat, 2020[18]). OECD data complement the picture for non-EU countries and give between 10% and 20% of all firms (employing 10 or more employees) having experienced security breaches in 2019, with a few extremes such as Japan (56%), on the one hand, and Korea (5%), on the other hand (Figure 2.1). A 30% – corresponding to 36% of total employees – of Italian businesses reported at least some damage from a cyber-attack between September 2015 and September 2016 (Biancotti, 2017[19]). Once data were corrected to account for unwillingness to report or inability to detect attacks, figures climbed to 45% and 56% respectively. In 2005, among 7 818 US businesses surveyed, 67% detected at least one cybercrime (US Bureau of Justice Statistics, 2005[20]).

Figure 2.1. Prevalence of security breaches in enterprises, 2019

Percentage of enterprises experiencing security breaches



Note: Enterprises with 10 and more employees.
Source: OECD (2020[21]), OECD ICT Access and Usage by Businesses Database, https://stats.oecd.org/Index.aspx?DataSetCode=ICT_BUS (accessed on 19 September 2020).

StatLink https://doi.org/10.1787/888934227260

The ideal target: Vulnerable organisations with valuable data

Data that an enterprise possesses, and its financial and cash capacity (i.e. the amount of money it possesses or processes), are the key motives behind the majority of digital security attacks. While there is a small subset of attacks that are perpetrated for the purpose of espionage or hacktivism, the majority of threat actors aims to find a way to break in and steal something of value, which can then be sold (data, trade secrecy, intellectual property, etc.) or laundered (money).

The typical criminal is primarily interested in obtaining credentials and personal data (Verizon, 2020[11]). After those two categories, medical, internal or payment data are roughly the same in terms of interest. Phishing via mass emails is still the easiest, cheapest and most effective means for that, including for stealing credentials that could then be traded on the dark web, without their owner being even aware of the intrusion. The risks –and gains- related to stolen credentials can be high when individuals reuse their credentials for multiple accounts (both professional and personal), and organisations did not implement multifactor authentication methods.

Table 2.2. Prevalence and type of digital security incidents by industry, 2019

Number of incidents and as a share of total incidents (%)

	Digital intensity	Prevalence of digital security risks		Actors (%)	Main data compromised (%)					
		Incidents	Breaches	External attacks	Personal data	Credentials	Internal data	Payment data	Bank data	Medical data
Professional, Scientific and Technical Services	High	7 463	326	75%	75%	45%				
Public Administration	Medium-high	6 843	346	59%	51%	33%				
Information services	High	5 741	360	67%	69%	41%	16%			
Financial and Insurance	High	1 509	448	64%	77%	35%			32%	
Manufacturing	Medium-low to high	922	381	75%	49%	55%		20%		
Educational Services	Medium-low	819	228	67%	75%	30%	13%			
Healthcare	Medium-low	798	521	51%	77%	18%				67%
Retail	Medium-high	287	146	75%	49%	27%		47%		
Arts, Entertainment and Recreation	Medium-high	194	98	67%	84%			25%		31%
Mining, extraction and utilities	Low	194	43	75%	41%	41%	19%			
Accommodation and food	Low	125	92	79%	44%	14%		68%		
Transportation and storage	Low	112	67	68%	64%	34%				
Other Services	Low to high	107	66	68%	81%	36%				
Construction	Low	37	25	95%	N/A	N/A				
Real Estate	Low	37	33	73%	83%	40%	43%			

Note: Digital intensity corresponds to a taxonomy of digital intensive sectors that accounts for some of the key facets of the digital transformation. The indicators used to classify 36 sectors defined along the international standard industrial classification of economic activities (ISIC revision 4) over the period 2013-15 are: share of ICT tangible and intangible (i.e. software) investment; share of purchases of intermediate ICT goods and services; stock of robots per hundreds of employees; share of ICT specialists in total employment; and the share of turnover from online sales. The Verizon report uses the North American Industry Classification System (NAICS) standard at the two-digit level to categorise the victim organisations. Verizon data refer to 2019.

Source: based on (Verizon, 2020[11]) and (Calvino et al., 2018[22]).

Table 2.3. Largest proportions of personal data breaches by sector, Australia, February 2018 – June 2019

Share of total personal data breaches notified to the Australian Office of the Information Commissioner

Sector	Total	% of total
Health service providers	268	35
Finance (including superannuation)	188	25
Legal, accounting and management services	134	18
Education	104	14

Note: Incident data collected due to mandatory data breach notification requirements for enterprises.
Source: Australian Office of the Information Commissioner quarterly breach notification reports, 2018-20.

All industries are affected by digital security risks, but to different degrees and in different ways (Table 2.2 and Table 2.3). While numbers vary across sources, several key trends seem to emerge:

- The most digital-intensive sectors tend to be the most impacted, in particular, professional, scientific and technical services (i.e. legal, accounting, management, R&D, etc.), which involve high value-added activities and process large volume of data.
- Public administration that possesses detailed information about citizens and businesses it serves is a target and ransomware is a now major problem for this sector. According to (Kaspersky, 2019[8]), at least 174 municipal organisations worldwide were targeted by ransomware in 2019, a 60% increase from 2018. However, human errors, due to misdelivery and misconfiguration, remain responsible for a large share of data breaches in the sector (Verizon, 2020[11]). The same seems to stand in the healthcare services.
- Beyond credentials and personal data, the type of data compromised varies across industry, depending on opportunities. In accommodation and food services (68% of cases) and retail services (47%), payment data are the main data compromised, while in healthcare services and financial services, medical records (67%) and bank data (32%) are respectively at stake.
- Attacks can be targeted to the firm's business models. In accommodation and food services, where a wide range of enterprises offer their services directly to customers and internet presence is important for operations, distributed denial of service (DDoS) attacks are major disruptors. The same is true in the entertainment industry where consumers expect videos to load fast and website content to get updated at high speed. In retail services, e-commerce applications are the leading cause of breaches in this industry.
- Motives are financial in most cases of attacks. However, theft of intellectual property plays a significant role in the breaches incurred in the manufacturing sector.

Globalisation can also be a channel of both additional digital security risk exposure but also ability to learn from experience and thus better manage this risk. This is because, "firms with an international dimension are more likely to have experience in conducting business online, resulting in higher threat awareness, and they are more exposed to cross- border attacks (Biancotti, 2017[19])."

SMEs have less "attack surface" but can incur relatively high costs due to security incidents

On average, an SME tends to have a lower intensity of digitalisation (see Chapter 1 on digital access and uptake by SMEs) and a smaller portfolio of digital assets to manage and protect (OECD, 2019[23]). This does not mean that they are not exposed to digital security risk though. SMEs, as users and sometimes producers of digital technologies, are exposed to the risk that vulnerabilities in these technologies may be exploited by malicious parties. Historically SMEs have been less likely to detect and report digital security breaches than large enterprises. This is due to many reasons including: less employees to commit errors;

a potentially lower reward for thieves/criminals given their smaller size and lesser degree of digitalisation (OECD, 2019[23]); lower internal capacity, skills and awareness to detect and address incidents; and less access to finance to invest in protection and/or detection capabilities.

Table 2.4. Prevalence of digital security incidents by firm size, national statistics, United Kingdom, 2019

Prevalence of breaches or attacks in the last 12 months

	Micro	Small	Medium	Large
Average number of breaches or attacks among the organisations that identified any case in the last 12 months	Incl. in small	7 690	330	7 710
Median number of breaches or attacks among the organisations that identified any case in the last 12 months		6	6	12

Note: Survey data. For businesses, analysis by size splits the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more).
Source: UK Cyber Breaches Survey 2019.

Table 2.5. Prevalence of digital security incidents by firm size, national statistics, United States, 2005

Prevalence of computer security incidents, by business size, % of respondents

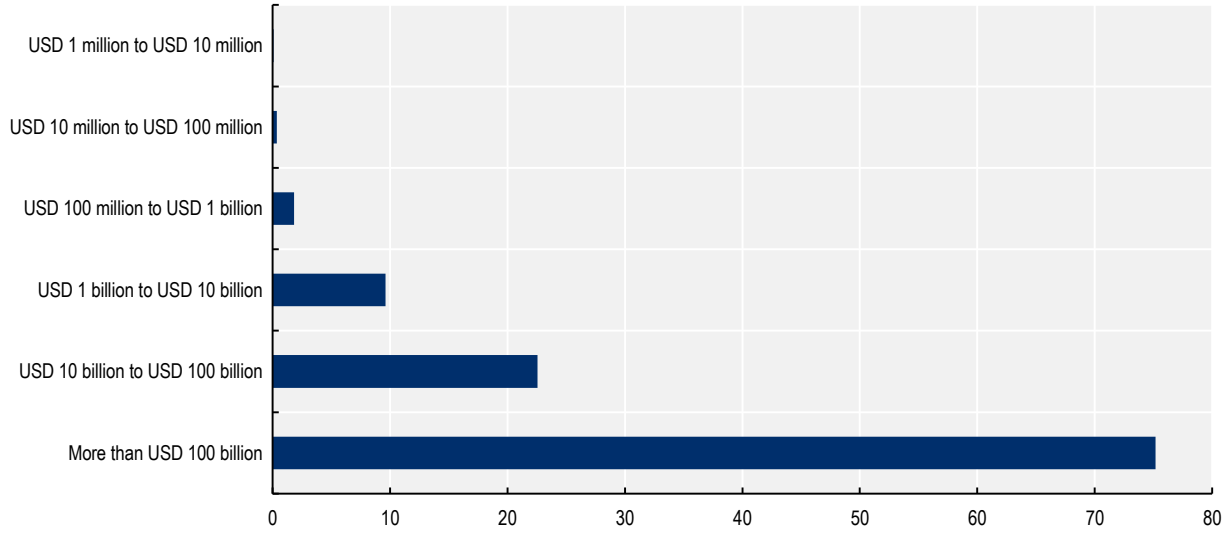
(headcount)	All incidents	Cyber attack	Cyber theft	Other
All businesses	67	58	11	24
2-24 employees	50	44	8	15
25-99 employees	59	51	7	17
100-999 employees	70	60	9	24
1000+ employees	82	72	20	36

Note: Survey data. “Cyber attack” encompasses computer viruses, denial of service attacks, electronic vandalism or sabotage. “Cyber theft” includes embezzlement, fraud, theft of intellectual property and theft of personal or financial data.
Source: 2005 National Cyber Security Survey.

National surveys conducted at different times are consistent over time as well (Table 2.4):

- The 2019 UK Cyber Breaches Survey found that the proportion of enterprises that detected an incident over the prior 12 months increased with size. The median number of incidents detected also increased, albeit marginally, with enterprise size. The mean number was higher for micro and small enterprises, compared with medium enterprises, due to a very small number of respondents experiencing larger numbers of incidents compared to their peers.
- In a 2016 survey conducted by the Bank of Italy, 40.8% of enterprises with 20-49 employees, 45.4% of enterprises with 50-199 employees, 49.2% of enterprises with 200-499 employees and 51.3% of enterprises with 500+ employees suffered at least one incident.
- Based on older data, across all subsets of incidents covered in the 2005 US National Cyber Security Survey, SMEs were less likely to detect an incident than larger enterprises.

Figure 2.2. Annual breach likelihood, by firm revenue, United States, 2009-19



Note: Advisen tracks several different types of cyber events such as ransomware, privacy, denial of service, etc. They compile information from publicly-available sources such as breach disclosures, company filings, litigation details, Freedom of Information Act requests, etc., in a dataset that is periodically updated. The ten-year observation period from 2009-2019 includes 56 000 cyber events, of which 1 900 record financial losses associated with the event and nearly 12 000 have counts for the number of records involved. Cyentia retrieved the data for the most recent completed year (2019), filtered down to those companies with headquarters in the United States, and applied categories to the revenue and employee counts. This gives them 37 352 breached firms in the observation window, with about three quarters (28 041) headquartered in the United States.
Source: Cyentia Institute (2019[24]), *Information Risk Insights Study 2020*, based on Advisen's Cyber Loss Data.

StatLink https://doi.org/10.1787/888934227279

Data analysed by Cyentia Institute, using a large historical incident response repository, show that smaller enterprises, as per their revenues, are less likely to experience at least one breach in the year and this likelihood increases as revenue increases (Figure 2.2). Once over USD 1 billion in annual revenues, the likelihood of dealing with at least one breach in the year increases dramatically, and again beyond USD 10 billion and USD 100 billion revenues.

However, there are subsets of SMEs that are relatively more digitally-intensive and are more likely to suffer an incident. Factors that increase the probability of failure include the nature of their business processes and models, the sector of activity (e.g. Information and communication technologies –ICT- industry and services) or a mismanagement of digital security. For instance, following up on the previous example in Figure 2.2, firms at the small end of the revenue spectrum but operating in certain digital-intensive or sensitive industries (e.g. healthcare, ICT) may have a higher probability of suffering a breach than firms in other non-digitally- or data-intensive industries (e.g. agriculture, mining).

Damages mount to many USD billions, with hidden costs

When a digital incident occurs, accidentally or intentionally, the enterprise cannot operate as usual and may incur additional costs and losses, depending on the nature of the incident (e.g. forensic costs, business interruption costs, legal costs, regulatory fines, etc.). It is important to differentiate between costs, losses and opportunity costs, as they are often mixed up in the literature in the economics of digital security (Dean, 2017[25]) (Box 2.3).

Box 2.3. Types of costs and losses related to digital security incidents

Direct costs of cybersecurity include investment in preventative security measures and measures to combat cybercrime. These costs are redistributive, i.e. the total capital stock of an economy is not reduced but reallocated ("the economic pie does not shrink"). For example, if a firm incurs a cybersecurity incident, and pays consultants to help repair the damage, then resources are redistributed from one party (the enterprise) to the other (the consultants).

Economic losses occur when there is a loss of income because economic activities were interrupted, or when the perceived value of a good or service is reduced. This is destroyed value (the "economic pie" shrinks). Another example of lost value can be found in the value that is not captured due to the theft of intellectual property rights.

Costs and losses may occur at the same time. For instance, if wiper malware (i.e. malware that corrupts and thus renders data unusable) is used to destroy a network, in addition to the redistributive costs (like consultants) there may also be economic losses (as the business was unable to operate and generate revenue).

Finally, opportunity costs are associated with direct costs. They arise when capital is allocated to cybersecurity purposes rather than value creation or social benefit. For private sector companies, rather than spending on security consultants and preventative measures, funds could be invested in profit-making activities that contribute to the top-line revenue activities, or to increase the productivity and scale-up capacity of the firm. For the public sector, taxpayer money spent on combatting cybercrime or improving cybersecurity environment could be invested in other areas generating greater societal benefits, such as health, education or well-being.

Part of the benefits of digital security, therefore, can be considered as the cost avoidance of digital security incidents. Another part can be seen in the subsequent ability to maximise productivity and value creation opportunities that are made possible from the digital transformation.

Source: Dean (2017[25]), *Trans-Atlantic Cyber Insecurity and Cyber Crime: Economic impact and future prospects*, European Parliament, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603948/EPRS_STU(2017)603948_EN.pdf.

Estimates for digital security incident losses are rare and often underestimated. One way in which to account for losses is by looking at insurance claims. Insurance policies aim to cover the losses from certain kinds of digital security incidents. When enterprises claim on these policies, and the claims data are made public, it is possible to see actual amounts lost. However, these amounts may understate the total economic damage. The costs and losses incurred due to digital security incidents also increase with enterprise size.

The 2019 NetDiligence Cyber Claims Study shows significant differences in losses between US SMEs and large firms over 2014-18 (Table 2.6). First, in terms of amounts. In financial services, where large enterprises incurred maximum average losses, the gap between small and large firms is of 1 for 100 USD. In professional services, where large enterprises incurred minimum average losses, the gap is 1 for 23 USD. Second, in terms of sectors affected. Average losses over the period were larger in retail for US SMEs, and larger in financial services for large enterprises. Third, in terms of dispersion. There are outlier cases among large enterprises. Some large enterprises received very high amounts of compensation for their losses, which increases the distance between the average and the median. This is particularly the case in professional services. To a lesser extent, similar extreme cases occur among SMEs in healthcare services.

Business surveys are another source of information about losses from digital security incidents. Findings from an Italian survey that was conducted in 2017 are converging with previous results (Biancotti, 2017[26]) (Table 2.7). Incidents are less costly in an absolute sense for SMEs as compared to large enterprises. The proportion of enterprises that have experienced no costs or losses following an ICT incident tend to decrease with enterprise size, and, as the amount of losses increases, more large enterprises are affected. This is somewhat to be expected – the larger the enterprise, the larger the revenue, and the larger costs and losses potentially incurred, particularly in case of business interruption. It is important to acknowledge though that surveys are not typically designed to sample "tail events" i.e. low probability but high impact incidents. Therefore, in this particular case, there could be a minor but non-zero proportion of enterprises that experienced losses in excess of EUR 200 000 but, given they were not included in the sample, they do not appear in the results of the survey.

Table 2.6. Costs of digital security incidents, national statistics, United States, 2014-18

Insurance claims paid for digital security incidents, US dollars, by firm size and industry

	SMEs		Large enterprises	
	Average	Median	Average	Median
Professional services	89 000	39 000	3 400 000	259 000
Healthcare	182 000	37 000	4 200 000	2 500 000
Retail	240 000	60 000	N/A	N/A
Financial services	106 000	40 000	10 700 000	3 900 000
Education	N/A	N/A	216 000	94 000

Note: Insurance claims data from multiple insurance companies, which are compiled and analysed by NetDiligence.
Source: NetDiligence Cyber Claims Study 2019.

Table 2.7. Costs of digital security incidents, national statistics, Italy, 2016

Proportion of enterprises experiencing digital security incidents by range of losses and firm size

Number of employees	No cost	Less than EUR 10 000	EUR 10 000-49 999	EUR 50 000-199 999	More than EUR 200 000	Don't know/ no answer
20-49	30.0	58.9	2.6	0.5	0	8.0
50-199	26.0	53.2	12.4	0.9	0	7.5
200-499	19.4	60.5	8.3	2.0	0	9.9
500+	29.5	41.5	17.2	2.2	2.2	7.4

Note: Survey data.
Source: Biancotti (2017[19]), "Cyber Attacks: Preliminary Evidence from the Bank of Italy's Business Surveys", Bank of Italy, Occasional Paper No. 373, http://dx.doi.org/10.2139/ssrn.2954991; Biancotti (2017[26]), "The price of cyber (in)security: Evidence from the Italian private sector", Bank of Italy, Occasional Papers No 407, https://www.bancaditalia.it/pubblicazioni/qef/2017-0407/QEF_407.pdf?language_id=1.

Table 2.8. Costs of digital security incidents, national statistics, United Kingdom, 2017

Relative number of incidents, cost of all incidents, per employee or as a % of revenues, in GBP Pounds

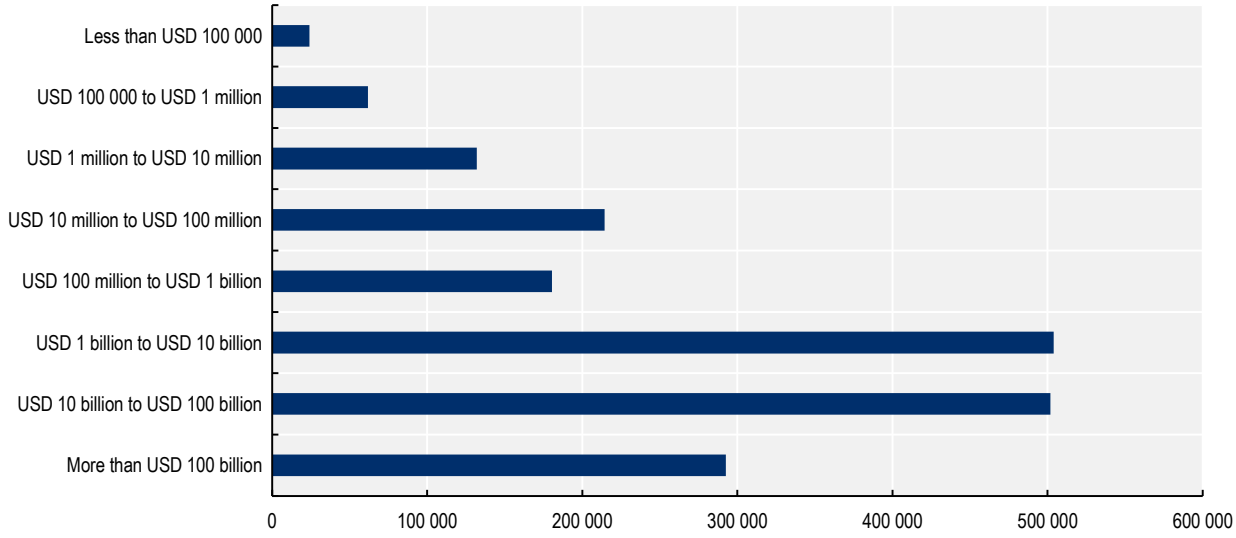
	All incidents					
	Number per employee		Cost per employee		Cost as a % of revenues	
Firm size	Mean	Median	Mean	Median	Mean	Median
Large	154	1	446	71	N/A	0.01
Medium	45	0	216	21	1.79	0.01
Small	26	0	78	16	0.90	0.01
Micro	2	0	81	4	1.57	0.01

Note: Survey data. For businesses, analysis by size splits the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more). For "all incidents" and "worst incident" figures respondents are asked what the total cost was for all and their worst incident over the past year. This estimate is then divided by the number of employees of that enterprise. The mean and median correspond to the population mean and median.
Source: OECD calculations based on microdata from UK 2017 Cyber Breaches Survey.

Finally, large historical databases on digital security incidents and losses can provide further insights into the probability of incurring an incident and the volumes of losses that could be incurred. One such database is compiled by Advisen and is based on publicly-available sources such as breach disclosures, company filings, litigation details, Freedom of Information Act requests, etc. A study conducted using this database in 2019 found an upward trend in typical losses as enterprise revenue increase (Figure 2.3) (Cyentia Institute, 2019[24]).

Figure 2.3. Average breach losses by firm revenues, United States, 2009-19

In USD Dollar



Note: Advisen tracks several different types of cyber events such as ransomware, privacy, denial of service, etc. They compile information from publicly-available sources such as breach disclosures, company filings, litigation details, Freedom of Information Act requests, etc., in a dataset that is periodically updated. The ten-year observation period from 2009-19 includes 56 000 cyber events, of which 1 900 record financial losses associated with the event and nearly 12 000 have counts for the number of records involved. Cyentia retrieved the data for the most recent completed year (2019), filtered down to those companies with headquarters in the United States, and applied categories to the revenue and employee counts. This gives them 37 352 breached firms in the observation window, with about three quarters (28 041) headquartered in the United States.
Source: (Cyentia Institute, 2019[24]) based on Advisen's Cyber Loss Data.

StatLink https://doi.org/10.1787/888934227298

However, there are differences between the absolute and relative losses that firms effectively incur. In fact, there are a number of ways in which to measure economic losses from digital security incidents, and a number of sub-cost components, which depend on the type of incident experienced.

For instance, the 2019 study on breach losses by class of firm revenues mentioned in Figure 2.3 shows that an enterprise generating USD 100 billion a year could expect a typical breach cost that is equivalent to 0.0005% of its annual revenues (Cyentia Institute, 2019[24]). A mom-and-pop shop, on the other hand, will likely lose 25% of its annual earnings. In extremes cases, the USD 100 billion enterprise will lose a fourth of its annual revenues, while the mom-and-pop shop will lose more than it can earn in the year. Without significant cash reserves - and the COVID-19 crisis has highlighted SME lack of liquidities, many of them not having enough cash to maintain activities over 2 or 3 months, the small business is likely to close. It should be noted that, due to the skewed distribution of digital security losses, a small proportion of firms can incur larger losses than the “likely” or “typical” ones. There is therefore only a small probability that small enterprises incur losses, in an extreme event, that exceed their annual revenue. The same does not apply to enterprises at the upper end of the revenue scale, simply because their revenues are so large that an incident could not possibly result in such heavy losses (in relative terms).

Results from the UK Cyber Breaches Survey 2017 show similar patterns (Table 2.8). When the numbers of incidents and total costs incurred are adjusted to the size of the enterprise, being as measured as per the number of employees or a proportion of revenues, it appears that most enterprises do not incur any incident, the median values being extremely low, if not null. This confirms the skewed distribution of incidents and costs. It also becomes apparent that micro firms with 1 to 9 employees incur disproportionately high cost per employee (GBP 81) for a small number of incidents (2), whereas large firms, if they experience more incidents (154), face less relative losses (GBP 154). To a lesser extent, medium-sized firms are also disproportionately impacted.

These results are to be put into perspective with the very large size of the SME population that account for over 99% of businesses in OECD countries (OECD, 2019[23]). While large losses tend to be borne by large enterprises, the sum of all smaller losses incurred by SMEs ends up into substantial amounts, not to mention the temporary or definite losses of capacity and scale-up opportunities, or the risk of eviction of viable enterprises from the market, that are difficult to include into loss assessment.

In addition, over time, weak digital security practices may become a barrier for SMEs to establish and maintain partnerships and business relationships with larger enterprises (OECD, 2019[23]). This is because larger enterprises need to manage their own digital security risk exposure throughout their supply chain. SMEs can be weak nodes in such supply chains and become a target for digital security attacks that would attempt to penetrate the medium-to-large sized –and more profitable-counterparties (OECD, 2019[27]). In response, larger enterprises may sever or avoid relationships with vulnerable SMEs. Conversely, SMEs that can demonstrate that they implement best practice to manage digital security risk can raise their business profile by increasing security within their supply chains, and are thus more likely to be able to take advantage of the opportunities made possible in this new industrial era (OECD, 2019[23]).

The digital transition and rising security risk

The digital transformation increases business exposure to digital security risk

Emerging digital technologies have the potential to spur innovation, enhance productivity and improve well-being. Many SMEs stand to benefit from new digital-enhanced practices and products, which create room for them to overcome the size-related barriers they typically face in innovating, going global and growing (OECD, 2019[23]).

Box 2.4. Artificial intelligence and digital security: The double-edged sword

An AI system enables making predictions, recommendations, or decisions that can influence real or virtual worlds (OECD, 2019[28]). How AI will transform digital security is likely to be by both supporting and challenging it.

AI techniques applied to digital security cover detection, repair and specification analysis. AI can help improve digital security by enhancing the capability of digital security teams. Digital security systems can be trained to identify the behaviour of malware and detect them before they enter IT systems or create damages. Given the shortage of skilled digital security professionals and the increasing volume of vulnerabilities, the automation of basic digital security tasks can help monitor higher volumes of security data. The deployment of AI powered security applications can therefore contribute to reduce time and costs of dealing with digital security threats. In addition, automation can reduce the likelihood of human errors and negligence, and AI can help develop code with fewer vulnerabilities.

AI can however create new digital security challenges because AI security techniques are also vulnerable to attacks. AI systems can be affected by new techniques that leverage their heavy dependence on data to be trained. Data poisoning, adversarial input and model attack, for instance by introducing bad data points, can disrupt the learning process of AI and make it inoperant.

AI is not yet widely used in cyber-attacks because cheaper techniques continue to be effective. As the cost of AI decreases, malicious actors are likely to turn towards more sophisticated approaches and leverage the AI potential for cybercrime, which will accelerate the digital security race between the attackers and the defenders.

Source: OECD (2020[1]), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en.

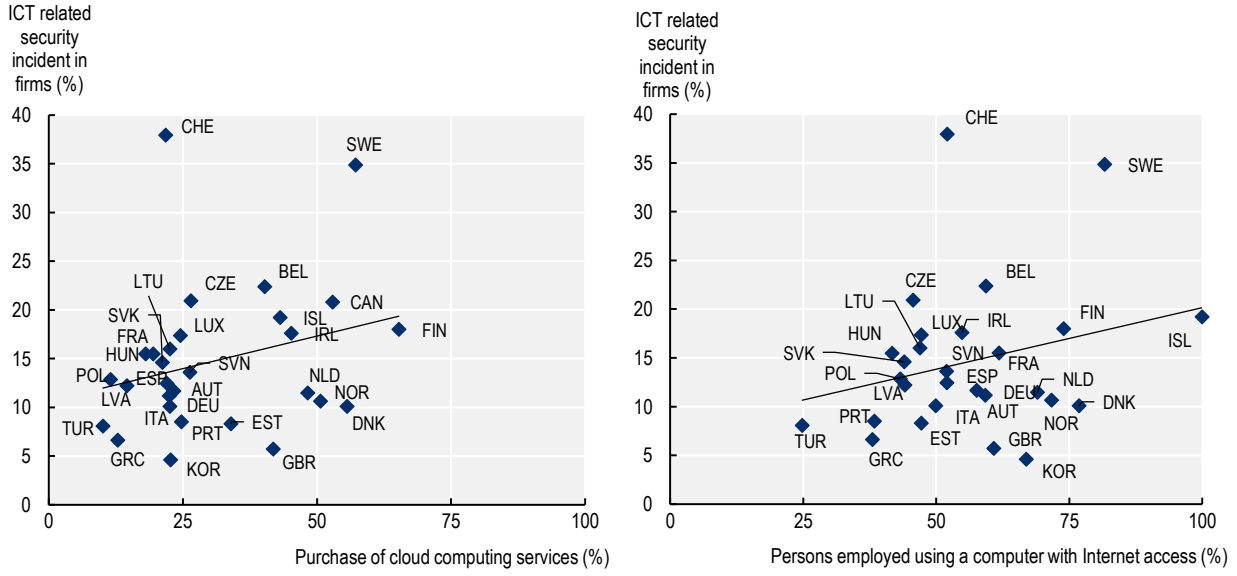
However, the digital transformation also increases business digital dependency and exposure to digital security risk. The advancement of computing technology and storage capacities have encouraged the widespread use of personal computing devices and the production of data. The Internet, smart apps and big data increase the volume of data available. The 5G broadband increases the speed and volume of data transfer. Artificial intelligence increases business capacity to make use and sense of it (OECD, 2017[29]). In addition, there is a non-negligible risk that AI creates new digital security challenges (Box 2.4). In fact, digital security incidents can affect all information systems, including those that rely on AI.

The Internet of Things (IoT), i.e. hyper-connectivity of sensors, devices, and systems that support machine-to-machine communication, will dramatically increase the volume of data available (and exploitable through AI and machine learning). Yet, with the IoT, the likelihood of security incidents is likely to grow, the IoT components becoming both targets of attacks and channels for disrupting physical systems (OECD, 2019[23]). As IoT can bridge the online and offline worlds, digital damages are likely to extend to the physical environment. Cyberattacks could increasingly alter the functioning of control and monitoring systems (e.g. self-driving cars, medical devices, etc.) or defense and security systems and disrupt the supply of essential services (e.g. electricity, heating, water, finance, transport), with lethal consequences.

Cloud computing allows access to extra processing power or storage capacity online, as well as databases and software, and supports the diffusion of other digital technologies, as well as innovative business practices (OECD, 2019[23]). Due to its flexibility and scalability, cloud computing reduces the costs of technology upgrading by exempting firms of upfront investments in hardware and regular expenses on maintenance, IT team and certification, turning ICT management model into a model based on software acquisition (codes) and digital (hyper)connectivity.

Figure 2.4. Hyper-connectivity and codification increase the vulnerability of firms, 2019

Prevalence of ICT security incidents, purchase of cloud computing services and use of computers with Internet access at work, as a % of total firms with 10 or more employees



Note: Data refer to enterprises experienced at least once problems due to an ICT related security incident (unavailability of ICT services, destruction or corruption of data, disclosure of confidential data).
Source: Data are drawn from OECD (2020[21]), OECD ICT Access and Usage by Businesses Database, , https://stats.oecd.org/Index.aspx?DataSetCode=ICT_BUS (accessed on 19 September 2020).

StatLink https://doi.org/10.1787/888934227317

Data on business use of ICT across OECD and EU countries highlights the close relationship between digital vulnerability, and hyper-connectivity and codification (Figure 2.4). As firms tend to increasingly purchase cloud computing services or their employees to use computer with Internet access, they are more likely to experience ICT related security incidents. In fact, the increasing connectivity of data-intensive activities adds layers of complexity, volatility and dependence on existing infrastructures and processes (OECD, 2017[30]).

Digitalisation increases the economic value of data, and incentives to steal them, while SMEs are ill-prepared to protect them

Data have never been so prevalent and digitalisation has turned them into a strategic asset (OECD, 2019[23]).

Data are increasingly generated along business operations, e.g. production and delivery (process data), and compiled at various stages of business transactions (user, consumer and supplier data) (OECD, 2019[23]). Process data can improve stock management, logistics and maintenance, and business reactivity to just-in-time production requirements. They also increase the scope of efficiency gains including in terms of energy and resource consumption. User, consumer and supplier data are crucial for developing market knowledge, improving customisation and shaping new products and business models. The volume of data produced globally is forecast to grow from 33 zettabytes in 2018 to 175 zettabytes in 2025, resulting in a compounded annual growth rate of 61 percent (European Commission, 2020[31]).

In this context, how SMEs protect their data is becoming more pertinent. SMEs tend to privilege trade secrecy as their default mode of data protection (OECD, 2019[23]). Trade secrecy is confidential business information that can cover new manufacturing processes, improved recipes, business plans or commercial information on whom to buy from and whom to sell to (e.g. customer list). Unlike patents, trade secrets are protected by law on confidential information, e.g. confidentiality agreement, or non-disclosure or covenant-not-compete clauses. Trade secret popularity holds on its relative ease of use (due to low technicity and the absence of formal registration requirements), lower costs incurred for administration and the absence of definite term of protection (Brant and Lohse, 2014[32]).

Digitalisation has made the protection of trade secrets increasingly difficult. The revolution in data codification, storage and exchange (i.e. cloud computing, emails, USB drives) are prime drivers of a rise in trade secret infringements. Increasing value given to intellectual property (and *de facto* its misappropriation), staff mobility and changing work culture and relationships (e.g. temporary contracts, outplacement, teleworking) or the fragmentation of global value chains (with more foreign parties involved within more diverse legal frameworks and uneven enforcement conditions) also contribute to increase exposure and risk of disclosure (Almeling, 2012[33]).

The COVID-19 crisis has been an opportunity for malicious actors to intensify attacks

The COVID-19 pandemic of 2020 has imposed a radical rethinking of business models. Small businesses in retail trade, manufacturing and a broad range of services, where physical presence and social contact once were common practice, have been confronted with the need to deliver and do business in a "contactless" way, or otherwise shut down non-mission critical, on-premise operations either periodically or permanently (OECD, 2020[34]) (OECD, 2021 forthcoming[35]). Business opportunities also emerge in this difficult context.

Some digital technologies and tools were sufficiently advanced and affordable to offer viable work-arounds and solutions in this context. Existing businesses have re-engineered their organisational structure and processes, adapting practices, proposing new products and/ or services (e.g. e-shops, home deliveries, Click and Collect, etc.), and accelerating digital adoption, while customers and employees stay home. SMEs have been at the forefront of these adjustments as the most affected by the crisis. The digital transition took place, sometimes with no former digital experience or very low digital maturity or preparedness (OECD, 2020[36]) (see Chapter 1 on digital access and uptake of SMEs).

Table 2.9. Early evidence of the impact of the COVID-19 on business digital adoption and risk

Based on national business surveys and private sources

Sources	Trends
Canadian Federation of Independent Business (4 May 2020)	Of the 26% of business owners who had online operations prior to the COVID-19 crisis, 30% have seen an increase in sales.
US Chamber of Commerce (5 May 2020)	Over April-May 2020, the share of small businesses transitioning some or all of their employees to teleworking increased from 12% to 20%, and the share of small businesses that had begun moving the retail aspect of their business online increased from 10% to 17%.
Pew Research Center survey (late March 2020)	40% of adults aged 18 to 64 in the United States reported they had worked from home as a result of the COVID-19 outbreak, as compared to estimates of 7% of private-industry workers and 4% of state and local workers who had the option to telework prior to the pandemic.
McKinsey (Germany)	Whereas at the outset of the crisis, 88% of German SMEs operated with mandatory in-person work, 81% expect that the pandemic will make their companies more flexible and one-third of SMEs esteems digitalisation has grown in importance due to the pandemic.
IBM/Ponemon (August 2020)	76% of survey respondents said remote work would increase the time to identify and contain a data breach. 70% of respondents said remote work would increase the cost of a data breach.

Source: (OECD, 2020[37]), "Coronavirus (COVID-19): SME policy responses", *OECD Policy Responses to Coronavirus (COVID-19)*, http://www.oecd.org/coronavirus/policy-responses/coronavirus-covid-19-sme-policy-responses-04440101/ (accessed on 18 July 2020); (IBM/Ponemon, 2020[38]), *Cost of a Data Breach Report*, www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (accessed 29 August 2020); Pew Research Center (2020[39]), "Telework may save US jobs in COVID-19 downturn – especially among college graduates", www.pewresearch.org/fact-tank/2020/05/06/telework-may-save-u-s-jobs-in-covid-19-downturn-especially-among-college-graduates/ (accessed 15 June 2020).

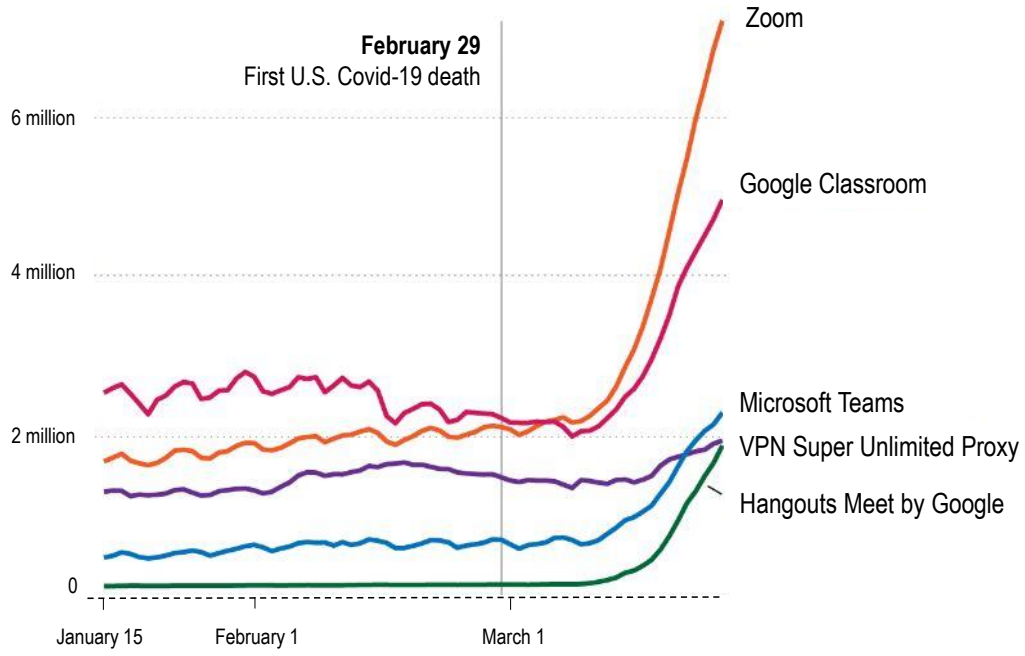
Some business surveys and analysis that were conducted during this period in order to track the impact of the pandemic on business activities provide data on the uptake of teleworking and digital practices during and following lockdowns (Table 2.9) (OECD, 2020[37]).

Teleworking has clearly widespread because of the pandemic, albeit differently between and within countries, depending on former practices and structural capacity (OECD, 2020[40]). For instance, prior to the pandemic, a 2016 Swedish study found that "telework has become routine for over 20% of all employed" (Vilhelmson and Thulin, 2016[41]). A 2017 study of 30 European countries (Ojala and Pyöriä, 2017[42]) found that 23% of Danes, 21% of Dutch and 18% of Swedes worked from home "at least several times a month". The lowest work-from-home rates in that sample were 6% in both Bulgaria and Cyprus (DeSilver, 2020[43]). The lowest-ranked OECD countries in the sample were Slovak Republic (8%) and Lithuania (8%). In the US, estimates were about 7% of private-industry workers and 4% of state and local workers who had the option to telework. A recent OECD study explores the diversity of tasks performed in different types of occupations, and the geographical distribution of those occupations. Results show that cities have a larger share of people that can work remotely - from 50% of the employed population in Luxembourg to 21% in Turkey – and capitals have, in most cases, the highest share of employment in occupations that can potentially be performed remotely (OECD, 2020[40]).

Zoom, an online remote conferencing platform, saw its daily active users jump from 10 million to about 200 million in three months following increased remote working (Chailytko, 2020[44]) (Figure 2.5). This was the highest jump in commonly used video conferencing platforms in absolute numbers. However, other similar services also saw fast and drastic increases in their user bases. Each service has differing security features, including end-to-end encryption, which means that the security of users differed depending on which service they used and how they used it.

Figure 2.5. COVID-19 containment measures gave a push to the adoption of smart working tools, United States, first months of 2020

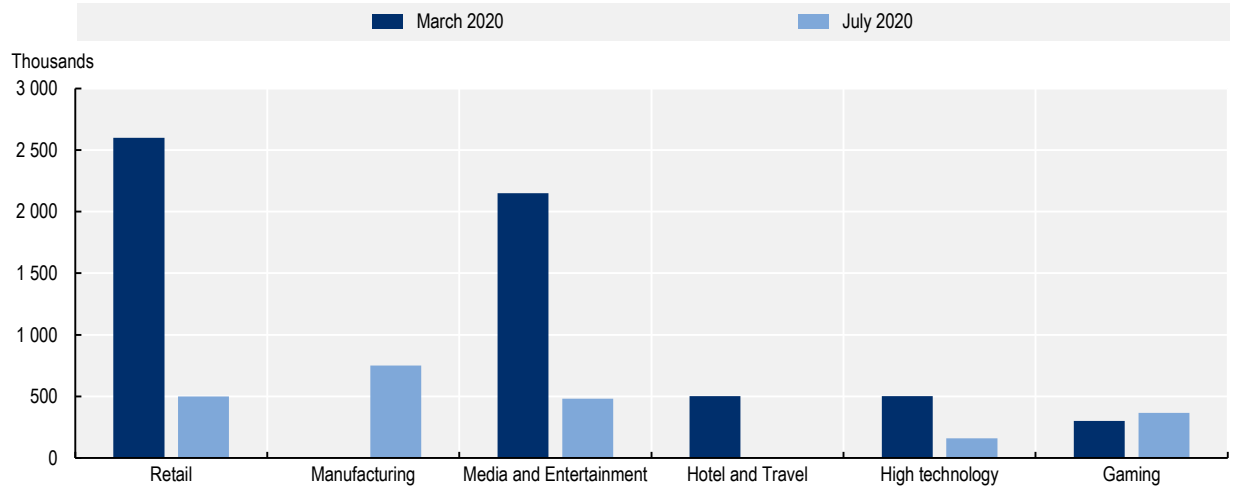
Daily app sessions for popular remote work apps



Source: (Koeze and Popper, 2020[45]), The Virus Changed the Way We Internet, The New York Times, based on Apptopia data.

Figure 2.6. Digital attacks have continued during lockdowns, targeting sensitive sectors

Top five industries by attacks volume, real time



Note: Number of phishing, malware, and command & control threats that Akamai is blocking (for customers). Akamai is a content delivery network, one of the world's largest distributed computing platforms, responsible for serving between 15% and 30% of all web traffic. Akamai's data visualisation tools display how data is moving across the Internet in real-time. Viewers are able to see global web conditions, malicious attack traffic, and Internet connectivity.
Source: Akamai (2020[46]), https://www.akamai.com/uk/en/resources/visualizing-akamai/ (accessed 24 March 2020 and 18 July 2020).

Digital security attacks have continued during lockdowns, targeting the most sensitive sectors (Figure 2.6). Akamai data shows real time activity on the Internet, through the lens of its distributed network of computing platforms and servers located worldwide. Akamai is estimated to serve between 15% and 30% of all web traffic, and data are reported by Akamai consumers. The five industries that have been the most subject to attacks end March 2020 were retail services, media and entertainment, hotel and travel, high technology and gaming. These also are the sectors that have been the most impacted by the shutdown of operations and those that have experienced sudden increases in digital activities. As a comparison, malicious activities have sharply decreased in volume in July 2020, as containment measures were gradually released. Targets also changed, for instance moving away from tourism services towards manufacturing industry.

Similarly, converging evidence point to a resurgence of digital security attacks in the past months and in a number of ways:

- Coronavirus-related scams and phishing campaigns have been on the rise (OECD, 2020[4]). There are also cases of ransomware and distributed denial of service attacks targeting hospitals, including in France, Spain and the Czech Republic.
- An increase in phishing emails, or at least a change in the content of these emails, has been observed in the early months of the crisis (Shi, 2020[47]). Purporting to come from official sources like the World Health Organisation these emails were intended to harvest credentials from victims, and subsequently break into networks, or simply to defraud the victim.
- In Italy, one COVID-19 themed phishing campaign hit over 10% of all organisations in the country with an email luring recipients into opening a malicious attachment (OECD, 2020[4]).
- The US Federal Bureau of Investigation saw a spike in cybercrimes as reported to its Internet Crime Complaint Center since the beginning of the COVID-19 pandemic. It was claimed that between 3 000 and 4 000 cybersecurity complaints were consistently received each day as compared to about 1 000 daily complaints prior to the COVID-19 pandemic (Miller, 2020[48]). Reports of increased business email compromise, scams and other fraudulent activity were also reported (FBI, 2020[49]).

Check Point, a cyber-security firm, reported in May 2020 that threat actors had registered thousands of fake and malicious Zoom domains in less than a month. In the context of the COVID-19, there has been a strong correlation between the increased digitalisation of business practices and the intensification of digital security attacks (Box 2.5. D4SME Webinar on Digital Security in SMEsBox 2.5). Finally, he noted that the digital environment has become more complex (e.g. business operations shifting online, individuals using their mobile phones and tablets more). All these trends have created new vulnerabilities that hackers can exploit.

In fact, the COVID-19 crisis drew attention to the weak digital security of SMEs and small organisations such as local governments (OECD, 2020[50]). Like large businesses, they were forced to switch to teleworking, sometimes overnight. This shift has increased the potential for attacks and introduced new vulnerabilities. For instance, many SMEs did not have Virtual Private Networks (VPNs) in place, did not use multi-factor authentication for remote access, or had to allow employees to use their own devices, which were not as secure as the ones provided by the organisation.

Box 2.5. D4SME Webinar on Digital Security in SMEs

On 29 October 2020, the OECD hosted a virtual webinar on digital security in SMEs. This webinar was convened as part of the Digital for SMEs (D4SME) Global Initiative, which "*intends to promote knowledge sharing and learnings on how different types of SMEs can seize the benefits of digitalisation, and on the role of government, regulators, business sectors and other institutions in supporting SME digitalisation"*. (OECD, 2020[36])

The webinar brought together experts, SMEs, large enterprises, government representatives, industry associations, etc., to discuss SME needs to effectively manage digital security risks, particularly given that the COVID-19 pandemic increased their digital reliance.

Some key messages from the webinar included:

- Attackers use tools of the same level of sophistication independently from the fact that the target is a small or a large firm.
- In the context of the COVID-19 pandemic, there has been an increased digitalisation of business practices and an intensification of digital security attacks.
- The digital environment has become more complex (e.g. business operations shifting online, individuals using their mobile phones and tablets more frequently), which creates new vulnerabilities that hackers can exploit.
- In parallel, the lack of experts in digital security services is striking, putting businesses at loss of where to find individuals with appropriate skills.
- A major risk for SME digital security is associated with human error, such as how individuals interact with their personal or work emails. These behavioural risks are harder to control at an organisational level. And if many small firms purchase digital security software, often they do not have the knowledge on how to best use and configure them.
- The digital insecurity in COVID-19 has deepened the divide between small and large firms, larger firms having often dedicated digital security departments in defending against these threats whilst SMEs turn into the easiest access points for hackers to target larger firms.
- The heterogeneous nature of SMEs also presents a challenge as digital security solutions need to be tailored to different levels of digitalisation, and different capability gaps (organisational, individual or ecosystem) should be addressed.. That is why awareness campaigns need to be targeted not only at the organisational level (executive level, HR, finance department) but also to the business ecosystem at large.
- There is an important role to be played by digital front runners or "enablers" to assist the SME "missing middle" to implement more secure practices, for instance through business partnerships. And there is a place for intermediaries such as chambers of commerce, sector associations and service providers like accountants and insurance, as well as local authorities, to work with legislators and strengthen the ecosystem.

The Australian Cyber Security Centre (ACSC) national survey 2019 shows that SMEs spend much less than is optimal on their digital security strategy, with over 50% indicating they would not spend more than EUR 250 annually. The survey also indicated that many SMEs overestimate their ability to respond to attacks and often outsource ICT security management.

SMEs and digital risk management

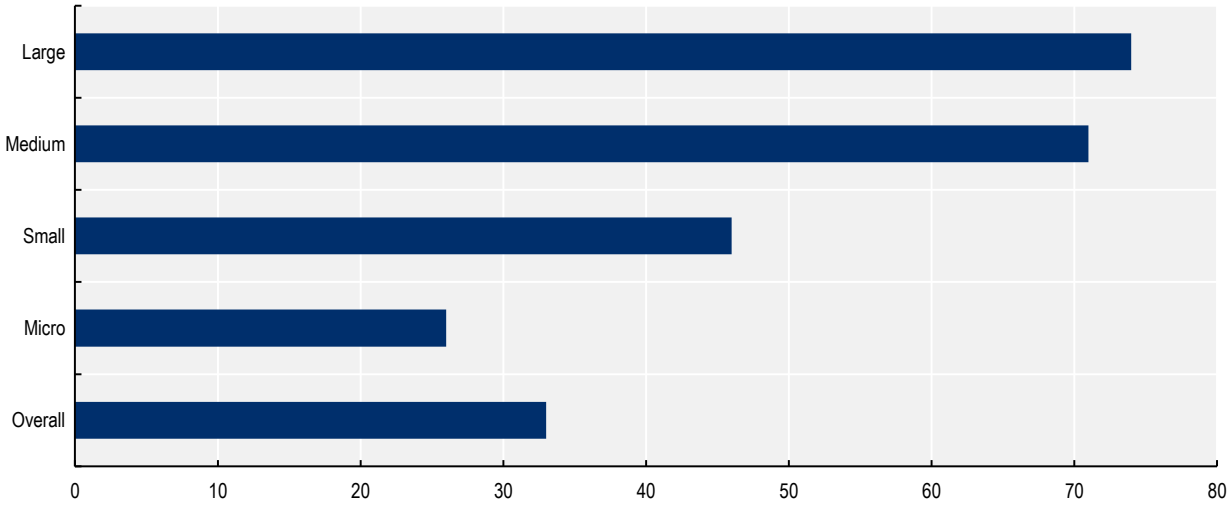
The digital security toolkit of smaller firms is less comprehensive and sophisticated

Smaller firms implement less often digital security measures

There is a strong relationship between adoption of digital security measures and enterprise size. As enterprises become larger, a higher proportion implement a greater number of and more advanced digital security measures.

Figure 2.7. Firms implement more digital security measures as they get larger, national statistics, United Kingdom, 2019

Percentage of enterprises with a formal policy covering cyber security risks

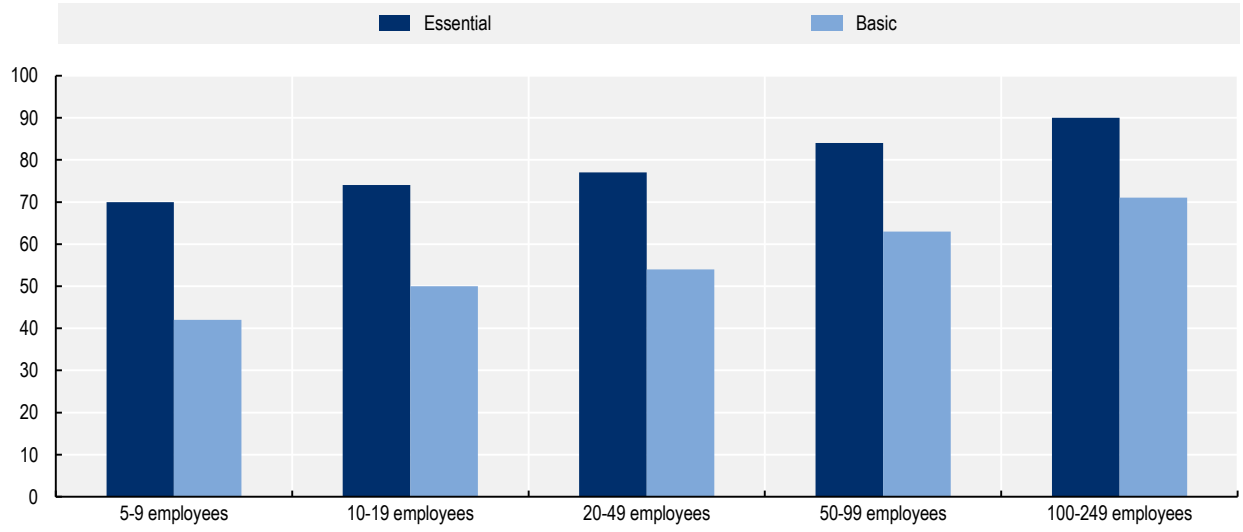


Note: Survey data. Micro businesses (1 to 9 employees), small (10 to 49), medium (50 to 249) and large (250 or more).
Source: UK Cyber Breaches Survey 2019.

StatLink https://doi.org/10.1787/888934227336

Figure 2.8. Firms implement more digital security measures as they get larger, national statistics, Denmark, 2018

Share of SMEs that have implemented essential and basic IT security measures

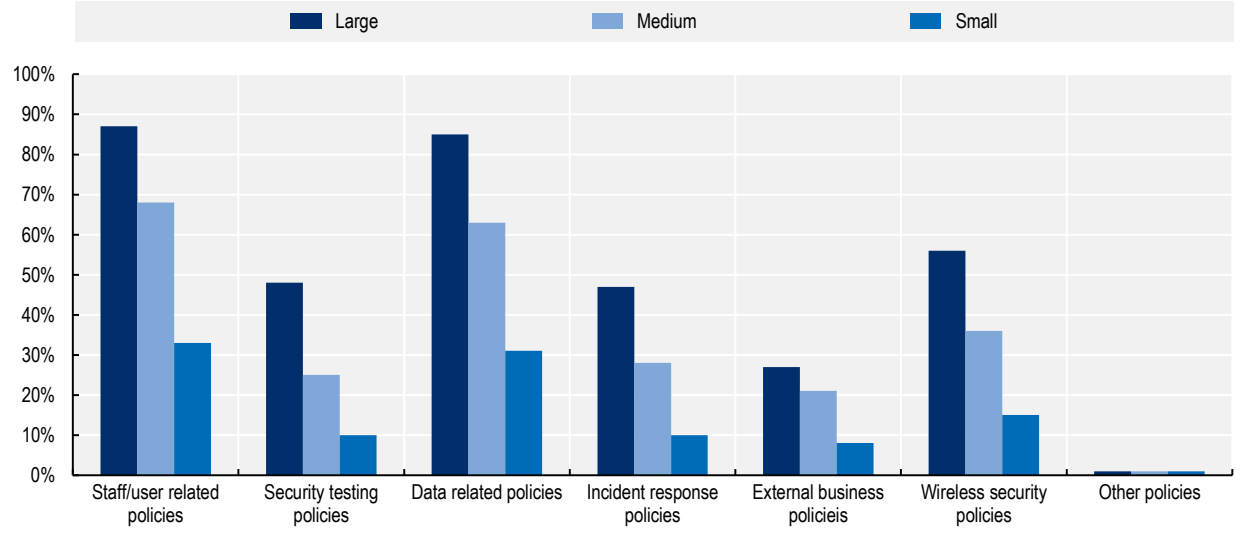


Note: Survey data. "Essential measures" defined as conducting systematic and ongoing updates as well as documented and thoroughly tested backup procedures. "Basic measures" include a fixed procedure for handling personal sensitive data; ongoing assessments and follow-up of employee accesses; ongoing IT risk assessments; ongoing external IT security analysis and/or IT audit; documented overview of critical information and systems; and ongoing internal IT security analysis and/or IT audit.
Source: 2018 IT Security and Data Management in Danish SMEs, Monitor Deloitte for the Danish Business Agency.

StatLink https://doi.org/10.1787/888934227355

Figure 2.9. Firms implement more digital security measures as they get larger, national statistics, Australia, 2009

Share of enterprises that use some forms of computer security policy

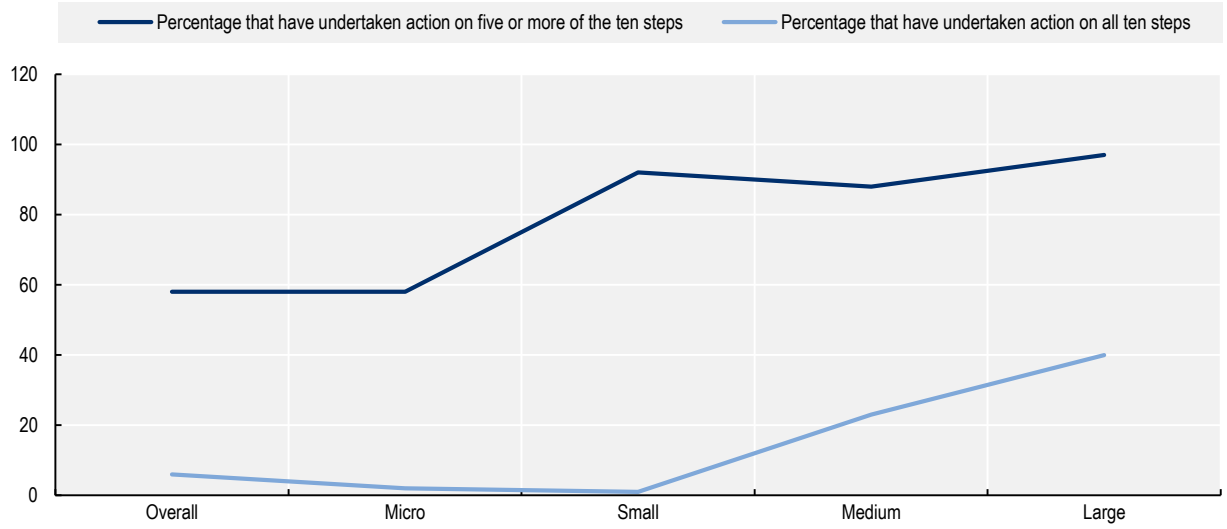


Note: Survey data.
Source: 2009 ABACUS survey.

StatLink https://doi.org/10.1787/888934227374

Figure 2.10. Firms implement more digital security measures as they get larger, national statistics, UK Government's "10 Steps Guidance", 2019

Percentage of firms that have implemented five or all ten of the recommended digital security measures



Note: Survey data. Micro businesses (1 to 9 employees), small (10 to 49), medium (50 to 249) and large (250 or more).
Source: UK Cyber Breaches Survey 2019.

StatLink https://doi.org/10.1787/888934227393

National statistics provide similar results and a sense of the persistence of this relationship from year to year:

- A separate survey undertaken in the United Kingdom indicates that the proportion of enterprises with a formal policy covering cyber security risks increased as enterprise size increased (Figure 2.7). This trend is echoed in the prior two years' (2018 and 2017) results for this survey, which used comparable and representative samples.
- A 2018 study on IT Security and Data Management in Danish SMEs, conducted for the Danish Business Agency, found a clear relationship between enterprise size (by headcount) and the digital security measures in place (Figure 2.8). As headcount increases, the proportion of enterprises that have implemented either basic or essential security measures increases (Monitor Deloitte for Erhvervsstyrelsen, 2018[51]).
- Outside Europe, the 2009 ABACUS survey in Australia show that the proportion of businesses with some form of computer security policy increased as enterprise size increased (Figure 2.9).
- When put against the UK Cyber Breaches Survey 2019, one can see that this tendency has persisted over time (Figure 2.10). SMEs are less likely to have implemented five or all ten of the recommended digital security measures as part of the Government's "10 Steps Guidance", which was first issued in 2015.[1]

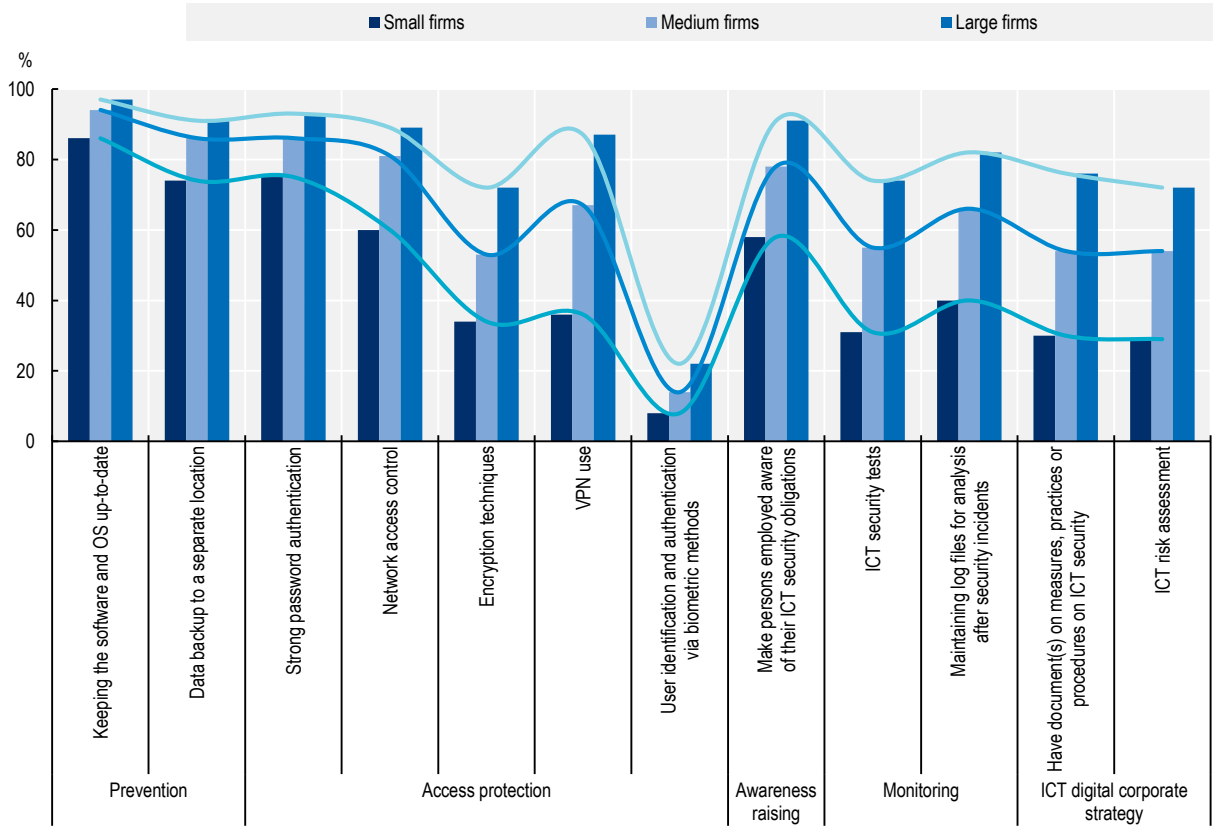
While it may be tempting to infer that the more limited deployment of digital security measures among smaller firms is in-of-itself problematic, as the prior section identified, there might be alternative explanations. This might be due to smaller enterprises simply not using digital technologies or being subject to different scale/sophistication of threats, and thus not requiring as many or the same kinds of measures/practices as larger enterprises.

Digital security practices are more sophisticated among larger firms

ICT digital security practices differ across firm size classes (Figure 2.11). European business surveys on ICT use show that all firms seem to engage actively in prevention, through data backup to separate location and regular updates of software and operating systems. The gap in implementation between micro and large firms is limited as compared to other digital security practices. In terms of access protection, micro firms tend to use relatively often strong password authentication, like larger firms.

Figure 2.11. SME digital practices increasingly differ from those of large firms as they become more sophisticated or comprehensive, EU28, 2019

Percentage of enterprises implementing ICT digital security measures, by type of measure and firm size



Note: VPN are Virtual Private Network that extends a private network across a public network to enable secure exchange of data over public network. The lines help figure out the implementation patterns of different ICT security practices by firm size. The lightest blue line refers to micro firms, the darkest to large firms. Micro-firms include firms with [0-9] employees; small [10-49]; medium-sized firms [50-249] and large firms [250 and more].
Source: Based on Eurostat (2020[18]), ICT Usage by Businesses data.

StatLink https://doi.org/10.1787/888934227412

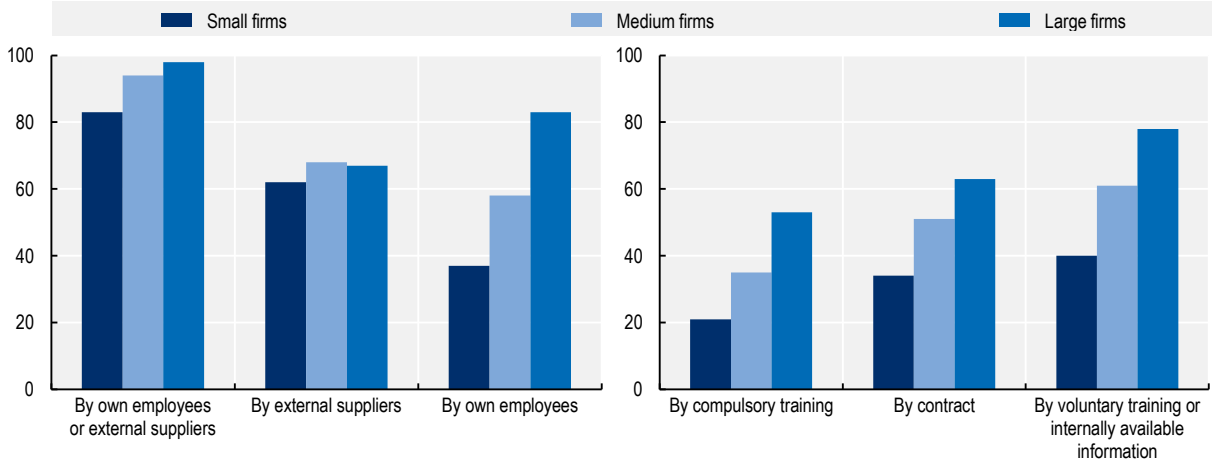
However, smaller firms tend to drop out when it turns to more sophisticated (e.g. VPN or biometrics) or more integrated (e.g. ICT digital corporate policy) approach of cybersecurity, or continuous monitoring.

Smaller firms rely less on their own employees for digital security purposes

Smaller firms have less of a tendency to have dedicated employees for carrying out ICT security-related activities (Figure 2.12). For instance, across the EU28 area, security activities in over 80% large firms are carried out by their own employees compared to less than 40% of small firms. At the same time, smaller firms tend to outsource their digital security responsibilities explicitly, by contracting external consultants/specialists, just about as much as their larger peers (Box 2.6). Again, across the EU28 area in 2019, 65% of SMEs compared to 68% of large enterprises, ICT security-related activities were carried out by external suppliers.

Figure 2.12. Smaller firms rely less on their own employees for cybersecurity purposes, EU28, 2019

Share of enterprises that carried out ICT security-related activities by approach, and that make persons employed aware of their obligations in ICT security-related issues, by channel and firm size



Note: Small firms include firms with [10-49] employees; medium-sized firms [50-249] and large firms [250 and more].
Source: Based on Eurostat (2020[18]), ICT Usage by Businesses data.

StatLink https://doi.org/10.1787/888934227431

Box 2.6. SME use case: Smart & Final (United States)

Smart & Final is a food retail company headquartered in Los Angeles, USA. Smart & Final operate 330 grocery and foodservice stores in California, Oregon, Washington, Arizona, Nevada, Idaho and Utah. The business focuses heavily on price and customer service. Consumer trust and accordingly security is crucial. The enterprise holds the details of millions of customers' credit cards, with a security breach or a hacking of those details having potentially a catastrophic impact on its corporate reputation. However, its internal IT resources and skilled personnel are limited.

Smart & Final decided to outsource its digital security and data protection in order to reduce the strain on the small in-house IT team. The company implemented different solutions and its in-house team of two IT engineers managed to roll out firewalls to all 330 stores.

Source: OECD Global Digital for SMEs Initiative (D4SME), Databank.

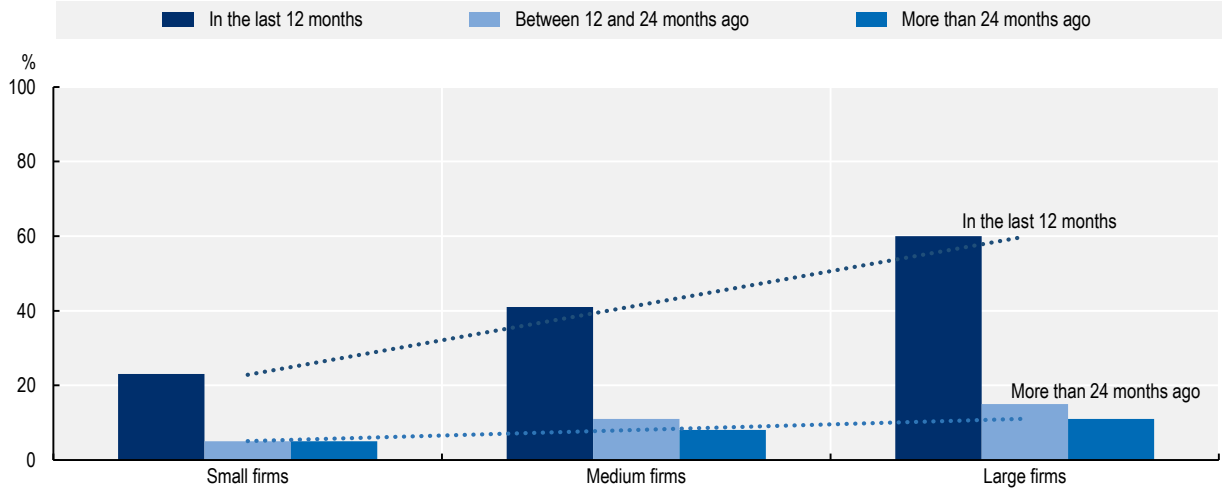
Another way that enterprises implicitly or explicitly delegate responsibility for digital security to external third parties is through the products or services that they choose to use. Examples might include using commercial software like Microsoft Office, Gmail, Salesforce or Adobe, amongst countless others. Software and hardware are designed in very specific ways, which include the basic functionality of the product or service and/or security features. When enterprises choose to use these products or services they are implicitly delegating part of the responsibility to the designer, manufacturer and/or end-retailer. This delegation can be effective in instances where the external party has the ability to make more sophisticated design choices and use greater resources in the design and maintenance of security features. An example of such a service would be Cloud services, which leverage network effects amongst service users to deliver a better-resourced set of security features than the individual users would be able to maintain on their own. By contrast, this delegation may be sub-optimal in instances where the end user is unable to ascertain the quality or robustness of the security features in the absence of the specialised knowledge/information to make such a decision.

Smaller businesses tend to update their ICT security policy less often

The same data provide some insights on the frequency at which firms review their ICT policy, or have designed the current one (Figure 2.13). Although all size firms, when they have recently revised their ICT policy, have done so in the last 12 months, the proportion of small firms remains twice lower than medium-sized firms, and three times lower than large firms.

Figure 2.13. Smaller firms tend to update their ICT policy less often, EU28, 2019

Percentage of enterprises that designed or last reviewed their ICT policy, by frequency and firm size



Note: Micro-firms include firms with [0-9] employees; small [10-49]; medium-sized firms [50-249] and large firms [250 and more].
Source: Based on Eurostat (2020[18]), ICT Usage by Businesses data.

StatLink https://doi.org/10.1787/888934227450

SMEs tend to invest less in digital security, though the sector matters

In absolute terms, SMEs tend to invest less in digital security than large counterparts do (Table 2.10). This is due in part to their lesser tendency to use digital technologies. Spending does tend to be skewed though, with a small number of digitally intensive enterprises in certain sectors (e.g. finance, information, healthcare) spending orders of magnitude more per year on digital security – due to necessity – than

enterprises in less intensive industries (e.g. hospitality, real estate, construction). One element to note is that, according to the 2019 UK Cyber Breaches Survey, a higher proportion of smaller enterprises claim to spend nothing on digital security as compared to larger enterprises.

Table 2.10. Small firms tend to spend less on digital security, national statistics, United Kingdom, 2019

Median investment in cyber security in the last financial year, by firm size

	Micro and small firms	Medium-sized firms	Large firms	Total
Median investment (GBP)	200	5 000	42 600	200
Share of total annual spending (%)	33%	18%	16%	33%

Note: Survey data. Investment is the amount of spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. This does not include any spending to repair or recover from breaches or attacks. Micro businesses (1 to 9 employees), small (10 to 49), medium (50 to 249) and large (250 or more).
Source: UK Cyber Breaches Survey 2019.

Table 2.11. Small firms tend to spend less on digital security, national statistics, Italy, 2016

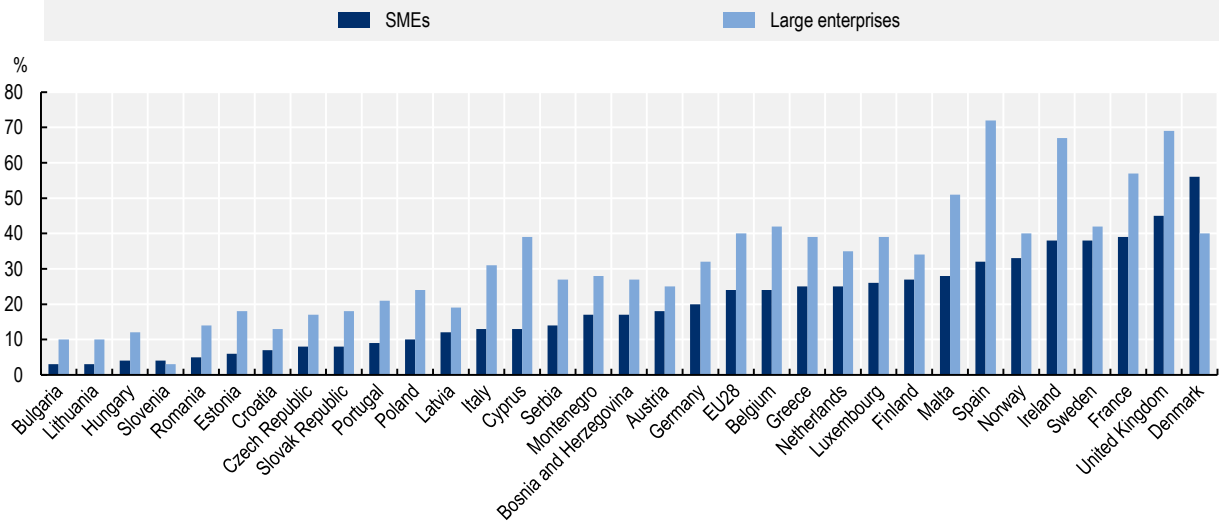
Percentage of firms by level of expenditure on cyber defence and firm size

Number of employees	No cost	< EUR 10 000	EUR 10 000-49 999	EUR 50 000-199 999	> EUR 200 000	Don't know/no answer
20-49	19.8	57.0	12.0	0.8	0.1	10.3
50-199	12.8	45.7	26.3	3.5	0.8	10.8
200-499	9.9	29.5	34.4	11.1	2.6	12.6
500+	7.8	13.1	28.5	18.3	15.1	17.3

Note: Survey data.
Source: Biancotti (2017[26]), "The price of cyber (in)security: Evidence from the Italian private sector", Bank of Italy, Occasional Papers No 407, www.bancaditalia.it/pubblicazioni/qef/2017-0407/QEF_407.pdf?language_id=1.

Figure 2.14. SMEs tend to be less well covered in case of incidents, 2019

Percentage of enterprises having insurance against ICT incidents



Note: Survey data. SMEs firms include firms with [10-249] employees and large firms [250 and more]. The financial sector is not covered.
Source: Based on Eurostat (2020[18]), ICT Usage in Enterprises Database.

StatLink https://doi.org/10.1787/888934227469

There is a growing industry for insurance policies that aim to cover the costs and losses associated with digital security incidents. According to Moody's, based on US regulatory financial data, direct cyber premiums written grew to USD 2 billion in 2018, or a cumulative annual growth rate of 26% since 2015 (Moody's, 2019[52]). It was hoped that the European Union's (EU) General Data Protection Regulation (GDPR) would help spur faster growth in Europe following its implementation in 2018 (OECD, 2018[53]).

However, SMEs tend to purchase stand-alone digital security insurance policies less than larger enterprises. This is a common feature in all countries covered by the European business survey on ICT use, with the notable exception of Denmark (Figure 2.14). In the EU28, on average, about 40% of large enterprises purchase ICT insurance as compared to about 20% of SMEs.

Setting aside that many non-stand-alone insurance policies could be triggered in the event of some digital security incidents (e.g. property and casualty lines triggered due to ransomware), there are thought to be a few reasons why SMEs tend to buy such insurance compared to larger enterprises. "*The needs and expectations of many businesses can diverge from the scope of coverage commonly provided by insurance companies*" (OECD, 2018[54]). "*Buying the right policies can be challenging, particularly for companies whose understanding of their own vulnerabilities may be sketchy"* (OECD, 2018[55]). When surveyed in 2019 on the reasons why they do not have "cyber insurance", respondents in the United Kingdom replied:

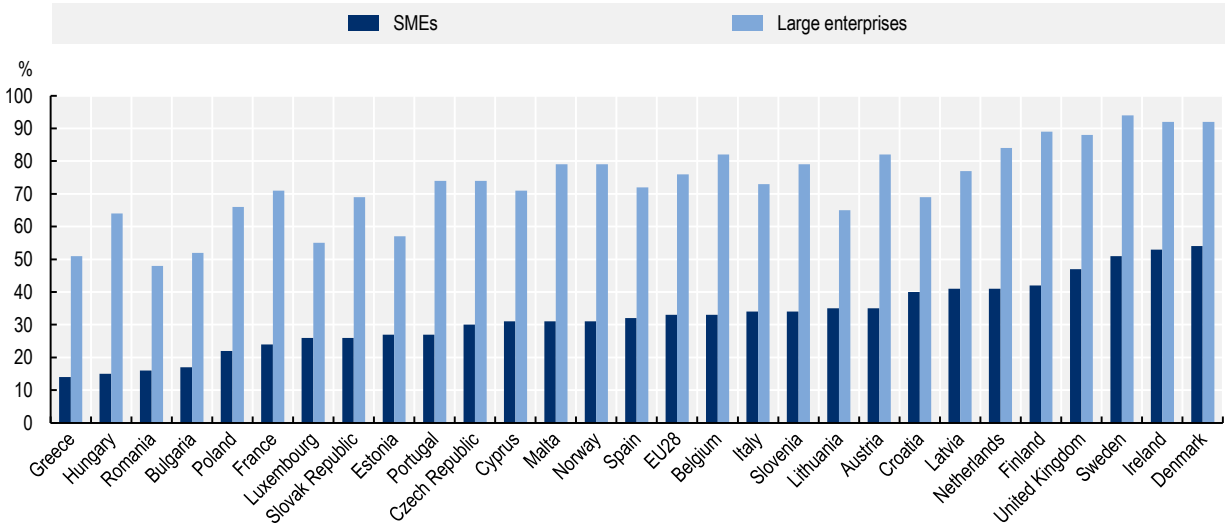
- They are already being covered by an external cyber security provider (23% of businesses and 26% of charities).
- They lack awareness of cyber insurance (23% of businesses and 15% of charities).
- They consider themselves to have too low a risk (29% of charities and 22% of businesses).[2]

There are large variations across countries on how SMEs secure their systems and data.

There is substantial variation in the implementation of digital security practices and measures by country. In almost all countries surveyed as part of the 2015 Community survey on ICT usage in enterprises, when asked if the enterprise had a formally defined ICT policy[3] in place the difference between SMEs and large enterprises was approximately 30%. These results were reinforced in the most recent 2019 survey, though the terminology used was slightly different[4] (Figure 2.15).

Figure 2.15. There are large variations across countries on business adoption of ICT security measures, EU28, 2019

Businesses with a document(s) on measures, practices or procedures on ICT security (%) by firm size



Note: SMEs firms include firms with [10-249] employees and large firms [250 and more].
Source: Based on (Eurostat, 2020[18]), ICT Usage by Businesses data.

StatLink https://doi.org/10.1787/888934227488

Public policies for strengthening digital risk management among SMEs

In light of the reasons why SMEs manage their digital security risk the way that they do, and the economic consequences of poor digital security risk management amongst these enterprises, governments in many OECD countries have developed and implemented various policies. Owing to the fact that SMEs make up close to 99% of enterprises in almost all OECD countries (OECD, 2019[23]), any government initiative to improve digital security in enterprises ends up applying to and/or affecting SMEs. A limited number of OECD countries have implemented SME-specific policies aimed at improving digital security in various ways. This section goes in depth to explain the rationales behind these policies and then provides past and current policy examples, based on national documentation and country responses to the OECD Survey on Digital Security Policies 2019.

Understanding the rationale for policy intervention

Governments have first a key role to play in maintaining the legal and judicial frameworks within which public administration and markets operate, refraining misappropriation of data, infringement of property and privacy rights, fraud and extortion. This is of importance as SMEs are disproportionately affected by inefficiencies in institutions and regulatory frameworks (OECD, 2019[23]).

In addition, digital security risk is partly the consequence of a range of failures in digital technologies markets (Dean, 2018[56]). In that sense, governments can provide the conditions for the market to reach a socially optimal level of digital security, taking into account that cybersecurity presents the features of a public good. Market failures include:

- **Information asymmetry among consumers**: It can be difficult for consumers to evaluate the security features of highly technical products. It can also be difficult for them to evaluate the relative quality of software code, because of a lack of technical competences, and because many producers use protection to prevent software inspection. When considering which products to purchase, if given a choice, consumers are not always able to assess which is truly the more secure option.
- **Distortion of market signals for producers**: Compounding matters, the inability of consumers to assess the relative security of a product means that producers who have invested in more secure products cannot easily differentiate themselves in the market. This prevents them from passing the additional cost of security development onto end users, e.g. in the form of price premium, also resulting in a "market for lemons", i.e. where "good" products are crowded out by the "bad" ones (Akerlof, 1970[57]). As a result, private investment in digital security may be below the socially desirable level if firms cannot fully appropriate the returns from their investments.
- **Negative externalities**: The cost of digital security incidents are not always borne by the producer of the technology in question. Moreover, some producers do not implement sufficient security measures to reduce the probability of some classes of incidents, given that the costs of the incidents are borne by others. Again, negative externalities may lead to an under-investment in digital security.
- **Moral hazard**: Moral hazard raises uncertainty as it involves that one party bears the costs and losses due to the risky actions of others.

Recent government initiatives to improve SME digital security practices

To date, government efforts have aimed to incentivise the production of more secure digital products ("security by design" or "privacy by design"), and to introduce penalties for actors whose products lead to digital security incidents, or whose failure to properly manage digital security risk results in costs or losses for others parties. Many of these initiatives have been implemented as part, or following, the adoption of national cybersecurity strategies across OECD countries and they have increased in number and span over time (OECD, 2017[30]). The following section provides a panorama of the major types of initiatives typically undertaken to assist SMEs with digital security across OECD countries.

National digital security strategies serve as major container for related policies, and, according to the OECD Recommendation (OECD, 2015[58]), should consider SMEs specifically in design and implementation, especially because of possible governance failures between digital security agencies and SME policy instances (Table 2.12).

Table 2.12. Mainstreaming of SME policy considerations in national digital security strategies

Country	National strategies	Involving SMEs in design	Involving SME business associations in implementation
Brazil	National Cyber Security Strategy (2019-23)		
Canada	National Cyber Security Strategy - Canada's Vision for Security and Prosperity in the Digital Age (2010-24)	Yes	Yes
Colombia	National Digital Security Policy (2016-20)		
Denmark	Cyber and Information Security Strategy (2018-21)	Yes	Yes
Finland	Finland´s Cyber security Strategy (2013-20)		
Japan	Cybersecurity Strategy (2018-21)		
Mexico	National Cybersecurity Strategy (Estrategia Nacional de Ciberseguridad) (2017-18)		
Netherlands	National Cyber Security Agenda (2018)	Yes	Yes
Spain	National Cybersecurity Strategy (2019-24)		Yes
Sweden	Digital Strategy (May 2017) National Cybersecurity Strategy (June 2017).	Yes	
Turkey	National Cyber Security Strategy (2016-19)		
United States	National Cyber Security Strategy (2018)	Yes	Yes

Source: based on country responses to the OECD Survey on Digital Security Policies 2019.

Government initiatives to improve the overall level of digital security in markets can fall into the following categories. On the one side are policies that aim to encourage businesses to supply existing/novel digital security solutions (supply side) or, on the other side, those that aim to encourage businesses to improve the adoption of better digital security risk management practices (demand side) (Table 2.12).

Table 2.13. Selected examples of policy initiatives aiming to raise digital security in the SME sector

Strategic objectives	Policy instruments	Country examples
Supply-side: Encouraging the supply of business digital security solutions		
Enhancing “security by design” or ”privacy by design” features in IT products	Regulation and legislation	• Mandatory security requirements of California’s Bill SB-327 for connected devices
Reducing transaction costs in trading, including abroad	Security standards	• EU Cybersecurity Act • US NIST Cybersecurity Framework
Developing novel digital security technologies through SMEs	Grants, tax credits, clusters and other finance mechanisms	• Canada’s Innovation and Skills Plan • Mexico’s PROSOFT programme
Demand-side: Encouraging the adoption of better digital security practices in firms		
Setting rules and guidelines for data management	Regulation and legislation	• EU General Data Protection Regulation and Directive (GDPR) and national implementation frameworks • California Consumer Privacy Act
Setting rules and requirements for data localisation	Regulation and legislation	• China Law 2017 on Chinese citizen data
Increasing market differentiation and price premium for good practices	Certification schemes	• CyberSecure Canada Certification Program and CyberSecure Canada Logo
Reducing information asymmetry for adopters	Security standards and procedure	• UK Cyber Essential Plus • EU Cybersecurity Act
Enhancing business capacity towards digital risk management	Business development services and informational resources	• US Small Business Cybersecurity Act • US “Stop. Think. Connect” programme

Strategic objectives	Policy instruments	Country examples
Building a broader culture and skills for cybersecurity		
Education and training	Provision of educational material, conferences, training	• Canada's Get Cyber Safe toolkit • Japan's Cybersecurity Human Resource Development Plan • Korea's Internet Security Agency's programmes • US National Initiative for Cybersecurity Education
Building knowledge base on digital security risks, and educational materials	Computer Emergency Response Teams (CERT)	• Australia, Austria, Denmark, Korea
Raising awareness on digital security risks and good practices	Awareness campaigns	• Cybersecurity Month (Canada, Chile, European Union) • National campaigns (Mexico, United Kingdom, United States)

Digital security legislations

In recent years, numerous national governments have undertaken efforts to develop and implement legislation intended to improve digital security. These legislative efforts sometimes overlap with the aforementioned data protection and privacy efforts but can be thought of as separate given their differing goals and compositions. National digital security legislations often aim to improve digital security in public-sector organisations, and create new public-sector organisations responsible for digital security, though in some cases their provisions also apply to, or affect, private sector enterprises.

The most recent, noteworthy federal legislation effort relative to digital security in the United States is the NIST Small Business Cybersecurity Act.[5] Signed into law in August 2018, it requires the National Institute of Standards and Technology (NIST) to, *"disseminate clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks"*. These informational resources must be generally applicable to a wide range of small businesses; vary with the nature and size of small businesses; promote cybersecurity awareness and workplace cybersecurity culture; and include practical application strategies.

However, one notable example with implications for SMEs is California's Bill SB-327 "Information privacy: connected devices"[6] that "*requires a manufacturer that sells or offers to sell a connected device in California to equip the connected device with a reasonable security feature or features appropriate to the nature and function of the device that is designed to protect the device from unauthorized remote access or use"*. This bill is notable because it mandates specific security measures that should be implemented in an Internet of Things device, which is a stark departure from the tendency of legislators in most jurisdictions to avoid prescriptive legislation that mandates certain security features.

Perhaps in recent years, a consequential national legislation in the area of digital security has been implemented in China. The law came into force in June 2017 and imposes new digital security and data governance requirements on companies doing business in and with entities domiciled in China, which means a substantial number of SMEs (International Association of Privacy Professionals, 2017[59]). The most consequential part of this law for SMEs relates to data localisation requirements. If a company operates in China, and it collects personal information on Chinese citizens, that company is required to store that data on servers located physically in China. If companies deem it "necessary" to transfer such information overseas "due to business requirements", the transfer may only be carried out following a security review (Livingston, 2017[60]). The effect is to make it more difficult and costly for non-Chinese companies to operate in China, which places greater constraints on enterprises' ability to generate and provide value in what is a digital world with potentially global reach but increasingly regional limits.

This is part of a larger trend around data localisation, which is introducing similar additional costs to doing business in a number of other countries. Other examples include Australia (Chander and Lê, 2015[61]), Germany (Determann and Weigl, 2016[62]), Turkey (Yavuzdogan Okumus, 2020[63]), the Russian Federation (Bowman, 2015[64]) and South Korea (Chander and Le, 2014[65]) among other countries. Data localisation requirements' potential impact on SMEs should be understood in light of the proliferation of new services such as big data, cloud computing, and IoT. Many providers of these services have significant international footprints; as such, data localisation requirements may raise barriers to entry and discourage new market entrants. Local SMEs could thus face substantial increases in their computing costs, potentially as high as 30-60% (Leviathan Security Group, 2015[66]).

Certification schemes and security standards

A number of countries have started to develop national certification schemes for digital security. These initiatives involve the development of a series of "best practices" that enterprises can implement in their own operations or in the design of their products and services. Upon completing the requisite steps, enterprises receive a certification that can signal to consumers or business partners the level of digital security of the enterprise or its products/services. These schemes aim to raise the firm's profile and reduce information asymmetry on the market. These schemes may also incentivise producers to design their products/services in a way that is "secure by design" (OWASP, 2020[67]). In this way, labelling schemes can help suppliers turn security into a competitive advantage and support market differentiation (OECD, 2019[27]).

The EU Cybersecurity Act creates, "*an EU-wide cybersecurity certification framework for ICT products, services and processes"* (European Commission, n.d.[68]). Still in development, the framework is intended to provide a comprehensive set of rules, technical requirements, standards and procedures for the evaluation of the security properties of a specific ICT-based product or service. This is potentially of benefit to SMEs in that it would provide a generally agreed upon standard and greater clarity for digital security in products/services.

A consistent or common certification scheme across countries also comes with additional benefits: consumers could refer to a trusted and recognisable standard, while producers could benefit from reduced transaction and opportunity costs associated with operating across borders, which would also increase the profitability of their products.

The United Kingdom, as part of its National Cyber Security Programme, has developed and implemented the Cyber Essentials and Cyber Essentials Plus programmes (National Cyber Security Centre, n.d.[69]). These programmes include an assurance framework and a simple set of security controls that enterprises can implement to protect their data and systems from threats coming from the internet. Cyber Essentials is a self-assessment tool, which is independently verified. Cyber Essentials Plus, by contrast, involves independent testing. Divided up into five technical controls, an enterprise is encouraged to implement boundary firewalls and internet gateways, secure configuration, access controls, malware protection and patch management. The UK government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium to develop Cyber Essentials and it is backed by the Federation of Small Businesses (United Kingdom Government, 2019[70]). Any enterprise can apply for and receive these certifications, but they may be particularly helpful to SMEs in that they provide succinct and clear guidance on useful digital security measures. Moreover, they are required for government contracts where the supplier is providing ICT services or handling personal information (Cyber Management Alliance, 2016[71]). Having a clear set of minimum criteria may be helpful for SMEs in their efforts to win public contracts.

A similar initiative is Canada's CyberSecure Canada Certification Program, which was announced in August 2019. "SMEs that demonstrate compliance with specified baseline cybersecurity controls[7], based on an audit by an accredited certification body, will be granted a two-year certification and be entitled to use the CyberSecure Canada logo" (Freedman, 2019[72]).

Innovation in digital security technologies

SMEs can be the source of new and improved digital security products, services or methods. A subset of fast-growing SMEs are a particularly important source of such innovations in OECD countries (OECD, 2010[73]). There are a number of ways that governments can foster digital security innovation by enterprises, including SMEs, such as tax incentives, acting as an early customer for innovative products, using regulation to stimulate demand for such products, or through the creation of a digital security innovation ecosystem (OECD, 2020[74]).

Canada's Innovation and Skills plan seeks to encourage the growth of many innovative industries including the "digital" industry, which includes digital security. While SMEs are not specifically mentioned as a target for these initiatives, the plan will have implications for SMEs through the creation of superclusters, attraction of new high-quality business investments (via the Strategic Innovation Fund), and the support given to innovative businesses with venture capital (Government of Canada, 2017[75]).

Mexico, through its long-standing PROSOFT Program, promotes the creation of industrial Innovation Centers (IIC) that are focused on providing trained and specialised human capital, as well as the adoption of new technologies linked to "Industry 4.0", such as digital security (Government of Mexico, 2016[76]).

Spain's National Cyber Security Strategy aims to generate knowledge and develop research and development activities in digital security. Line of Action 5 is specifically focused on, "*strengthen[ing] the Spanish cybersecurity industry and its capacity to nurture and retain talent, to bolster digital autonomy"* (Government of Spain, 2018[77]). Amongst the different measures proposed are: boosting R&D support programmes in digital security in SMEs, businesses, universities and research centres; facilitating access to national and international incentive programmes; and innovative public purchasing programmes.

The United Kingdom uses public procurement to encourage SMEs and supply chain actors to enhance their digital security. Companies that wish to become government suppliers need to implement the Cyber Essentials or Cyber Essentials Plus certification schemes. This approach promotes digital security without creating rigid compliance regulation that is likely to become outdated quickly or create burdensome requirements for business (OECD, 2020[74]).

The European Cyber Security Organisation (ECSO), is a public-private partnership that co-ordinates the innovation roadmaps and investments in the EU. It brings together many stakeholders including SMEs and industry more broadly, academia, regional representatives and Member States. ECSO helps prioritise investments across many technical areas of which digital security. (OECD, 2020[74])

Education and awareness campaigns

Numerous countries have undertaken a variety of efforts to increase awareness of digital security amongst the wider public, sometimes especially targeted to the business sector and SMEs. Those efforts aim to provide quality advice/guidance, and relatively inexpensive solutions, that, if adopted, would reduce SME digital security exposure and potential losses substantially. Indeed, the risk of exposure follows a Pareto distribution, whereby a large proportion of possible losses can be avoided with small investments in and implementation of certain protection measures.

As a part of its 2020 Cyber Security Strategy, Australia has implemented a number of SME-specific initiatives including some related to education and awareness campaigns. The Australian Cyber Security Centre (ACSC) chose to offer both guidance on *what* SMEs should be doing, but *how* they should implement a digital security strategy. Policy examples include tailored toolkits (e.g. to assess maturity levels).

The Belgian Federal Public Service for the Economy, SMEs, Middle Classes and Energy has an online set of resources to inform and assist SMEs in digital security matters. The information kit includes documents on undertaking risk assessments, key principles for ensuring digital security, what to do in the event of an

incident and a glossary of key technical terms (Belgian Federal Public Service for the Economy, SMEs, Middle Classes and Energy, 2018[78]).

Brazil, amongst many activities proposed as part of its Cyber Security Strategy, aims to 'create cyber security awareness actions for SMEs'. This intends to raise the level of maturity in digital security across society, and increase Brazil's resilience to digital security threats (Government of Brazil, 2020[79]).

Canada's Centre for Cyber Security provides people with a "Get Cyber Safe" toolkit during the Cybersecurity Month in October. The structured curriculum covers topics like "How cyber threats work", "How cyber threats affect you", and "How to protect your small business" (Government of Canada, 2020[80]).

Chile's National Cybersecurity Policy includes the design of a large-scale cybersecurity campaign to promote the implementation of awareness and dissemination programmes in partnership with the private sector (Government of Chile, 2020[81]). The policy document also makes reference to October as the Cybersecurity Month and a Safe Internet Day in February each year. More broadly, the Ministry of Education administers the "Internet Segura" (Safe Internet) initiative, to help people use the internet in a way that is "*responsible, informed, safe, ethical, free and participatory*" (Internet Segura y Ciudadanía Digital, 2020[82]).

Denmark's Cyber and Information Security Strategy focuses on strengthening the IT security knowhow of SME primary advisors, so they can operate as "bridge-builders". The aim is to make these advisors (e.g accountants, lawyers, etc.) raise IT security issues in their dialogue with SME leadership (Government of Denmark, 2018[83]).

France has a label SecNumedu for professional training courses targeting SMEs,[8] a guide for developing cyber hygiene within SMEs[9] and a platform that reports on malicious activities and provides assistance to professionals.[10] Japan established the Cybersecurity Strategic Headquarters in 2014, with a number of responsibilities of which implementing a "Cybersecurity Human Resource Development Plan" (National center of Incident readiness and Strategy for Cybersecurity, 2020[84]). Its outreach functions include a collaboration with Association of South East Asian Nations (ASEAN) members on "awareness raising, capacity building and so on.[11]"

Korea's Internet Security Agency (KISA) provides various educational and professional training programmes in order to raise awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in both public and private sectors[12].

Mexico has a National Cybersecurity Strategy and conducts awareness campaigns. The Federal Police runs a National Prevention Campaign called Cybersecurity Mexico, which seeks to "*raise awareness in Mexican society about the responsible use of new technologies and the Internet to reduce the damage caused by cybercrime"* (Council of Europe, 2020[85]). Additionally, since 2015, National Cybersecurity Weeks are organised in collaboration with the Organization of American States.

In 2018, Sweden assigned an authority to develop and implement a programme that aims to increase digitalisation skills among the management and boards of small companies. It is a three-year venture, whereby small businesses raise capacity to assess and manage digitalisation risks from an economic perspective (Swedish Agency for Economic Growth and Regional Development, 2020[86]).

The UK Centre for the Protection of National Infrastructure has developed a series of security awareness campaigns, designed to provide organisations with a complete range of materials they need. Some of the topics covered in these materials include "Don't take the bait", which addresses the risk of spear-phishing, "Identifying the right security behaviours" and "Think before you link" (Center for the Protection of National Infrastructure, 2020[87]).

The US Department of Homeland Security (DHS) administers a National Initiative for Cybersecurity Education. This comprises four key activities: 1) National Cybersecurity Awareness Campaign, 2) formal cybersecurity education, 3) federal Cybersecurity Workforce Structure[13] and 4) Cybersecurity Workforce Training and Professional Development (McConnell, 2017[88]). The "Stop. Think. Connect" programme is a national public awareness campaign aimed at increasing the understanding of cyber threats and encouraging the public to be safer and more secure online (Cybersecurity and Infrastructure Agency, 2020[89]). A toolkit has been assembled for various groups, including the industry (Cybersecurity and Infrastructure Agency, 2020[90]) and small businesses (Cybersecurity and Infrastructure Agency, 2020[91]). October is National Cybersecurity Awareness Month (NCSAM) and DHS releases at this occasion a new toolkit each year to make it easy for people and organisations, regardless of size or industry, to engage and promote NCSAM (Cybersecurity and Infrastructure Agency, 2020[92]).

The European Cybersecurity Month (ECSM) is an awareness campaign in October of each year that:

"promotes cybersecurity among EU citizens and advocates seeking to change the perception of cyber-threats by promoting education, sharing of good practices and competitions in data and information security" (ENISA, 2020[93])

In practice, this involves numerous activities including training, conferences, online quizzes and by providing general presentations to end users (ENISA, 2019[94]).

The European Commission and EASME, the Executive Agency for SMEs, recently ran an initiative to support specialised skills development related to Big Data, IoT and Cybersecurity for SMEs in Europe. The initiative involved convening many stakeholders to discuss the issues, and resulted in a final report containing an analysis of the potential benefits and barriers for technology adoption by SMEs. The work presents a vision, roadmap and toolbox to increase the capacity of industry, social partners, education and training organisations and policy makers at all levels to promote and support the acquisition of these skills by SMEs in Europe (European Commission, 2020[95]).

Box 2.7. Computer emergency response teams

Computer Emergency Response Teams (CERTs) have been set-up in most OECD countries. In many cases, governments provided the initial funding for their development and growth. They are often SMEs themselves and provide a variety of digital security services to members. Services typically include incident response, security bulletins, security incident notification, educational materials and conferences.

The CERTs sizes, by headcount, vary but typically do not number more than fifty people in total. The CERTs are sometimes funded by the government in their infancy until a critical mass of membership and funding is reached. Sometimes public-private partnerships are established from the start. Other times, the CERTs are housed within a government agency or body. Some countries may have multiple CERTs if, for instance, a sector-specific CERT is required. The examples in the table are illustrative and do not represent a definitive list of all CERTs currently in operation.

Country	Name	Description
Australia	AusCERT	Established in the mid-1990s and has continued providing a growing range of services to Australian enterprises since then (GovCERT Austria, 2020[96]). Alongside AusCERT, CERT Australia was set up in 2010 by the Federal Government. It was integrated into the Australian Cyber Security Centre, as part of the National Cybersecurity Strategy at the time, then eventually integrated into the Australian Signals Directorate (Australian Signals Directorate, 2020[97]).
Austria	NIC.at	Operates as part of the domain registry NIC at for the top-level domain address at CERT.at (2020[98]).
	govCERT	*govCERT Austria* was set up between *CERT.at* and the Austrian Chancellery to provide services to all enterprise and across domain names in Austria (GovCERT Austria, 2020[96]).
	Austrian Energy CERT	The *Austrian Energy CERT* is a co-operation between *CERT.at* and the Austrian energy and gas sector. It provides specialised services to enterprises operating in those sectors (CERT.at, 2020[99]).
	ACOnet-CERT	*ACOnet-CERT* provides services to the national research and education network in Austria (Aconet, 2020[100]).
Denmark	Danish Computer Security Incident Response Team (DKCERT)	DKCERT traces its history back to 1991. Services to members include incident response (for the national research and education network), vulnerability scanning and educational/information materials. DKCERT is notable for its Data Protection Officer service, which aims to help research and education institutions comply with the EU GDPR (DKCERT, 2020[101]).
Italy	CERT-PA	CERT-PA operates within the Agency for Digital Italy and has the task of supporting administrations in preventing and responding to IT security incidents.
	CERT Nazionale	CERT Nazionale was established at the Institute of Communications and Information Technology with the task of supporting private operators that are managing critical information infrastructure.
	CSIRT Italia	CSIRT Italia, by contrast, was established at the Presidency of the Council of Ministers in 2018 to implement the Directive on security of network and information systems (NIS Directive) in Italy. It pursues this goal in co-ordination with its counterparts, CERT-PA and CERT Nazionale (CSIRT, 2020[102]).
Korea	KrCERT/CC	Korea's KrCERT/CC is responsible for early detection systems and the co-ordination of incident response for non-government networks in the country (KRCERT, 2020[103]).
	KN-CERT	Responsible for similar tasks as KrCERT/CC but solely with government-run networks.
United States	US-CERT	US-CERT, which is currently part of the National Cyber Security Division of the US Department of Homeland Security (US DHS, 2020[104]), provides most of the services that one would come to expect from a CERT.
	CERT/CC	The Defense Advanced Research Projects Agency (DARPA) created CERT/CC in 1988. It is currently run by the Software Engineering Institute at Carnegie Mellon University. Aside from its unique housing within a federally funded university institute, CERT/CC has a very specific and unique goal: to research software bugs that impact software and internet security, publishes research and information on its findings, and works with business and government to improve security of software and the internet as a whole (Carnegie Mellon University, 2020[105]).

Conclusion

Although SMEs have a smaller "attack surface", they are increasingly exposed to digital security threats and digital security breaches. The digital transformation raises their level of exposure as it implies greater connectivity and reliance on software, and make them more vulnerable if proper digital security risk management practices are not in place. In addition, the COVID-19 crisis has made more businesses reliant on digital technology than before, giving an opportunity for malicious actors to intensify attacks, e.g. phishing then fraud, taking advantage of sudden and massive surge in teleworking arrangements and online transactions. A combination of low digital security risk management experience/maturity coupled with increased reliance also makes the potential impact of disruptions more serious (i.e. business interruption).

Phishing, denial of service and ransomware attacks continue to be the most prevalent methods, and can be often countered by implementing baseline security measures. But attacks have also become more sophisticated over time, techniques evolving continuously and requiring more advanced risk management capacities that smaller firms are less likely to have first.

Digital security incidents can result in sizeable costs and losses, and tend to increase with firm size. A small proportion of enterprises incur the lion's share of incidents and losses. However, when affected by rare but very costly incidents, SMEs can incur costs that can add up to several months of revenues. In addition, weak digital security practices may become a barrier for them to build business networks.

SMEs tend to have less comprehensive and sophisticated digital security risk management practices. They often do not have a person dedicated to digital security internally. They tend to seek less information from external sources on digital security and do not tend to have formal procedures in place to detect intrusions. They also tend to update their procedures less often and invest less in digital security, although this varies across sectors and countries.

Governments increasingly aim to encourage the adoption of better digital security practices in SMEs through certification schemes, security standards, or by raising awareness and building business competences on digital security. Policy initiatives are often not specific to SMEs, or not specifically designed towards this segment of the business population, although recent policy trends show a shift towards more targeted approaches (e.g. UK cyber essentials, France's training label and reporting platform, etc.).

Looking forward, SMEs need to be more aware of and effectively manage digital risk so as to make the most of the opportunities afforded by the digital transformation. This message has been consistently reinforced by the OECD, and the 2015 OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity states that "*digital risk should be approached as an economic risk; it should therefore be an integral part of an organisation's overall risk management and decision making processes*." (OECD, 2019[27]; OECD, 2015[58]).

Unfortunately, there is no one-size-fits-all digital security governance, as methods and techniques vary, depending on the risks incurred, the types of attacks suffered, the types of assets to protect, and in turn, the business models prevailing in the sector. This makes managing digital security risk effectively challenging. Various policies have attempted to assist SMEs to improve their digital security risk management practices. The rapid intensification of digital uses in the context of COVID-19 has made the need to manage this risk more urgent. If old trends hold, there is possibly a widening gap emerging between the need and ability of SMEs to manage this risk.

The evidence base for digital security policies, and risk management, improve with each passing year. A much more substantive research base is now available (and has been cited throughout this paper). There is still much more work to be done though, so as to ensure that the best evidence and research is available to guide decision making both within enterprises and government.

Further research would be useful to:

- Better understand the correlation between firm-level vulnerability and investment in digital security, and the various types and amounts of costs incurred due to different types of digital security incidents. These incidents and their costs may differ across OECD countries depending on many factors such as the composition of the enterprise population and their industrial structure.
- The impact that age has on an enterprise's likelihood to have mature digital security risk management practices. Some evidence has pointed to younger enterprises being more likely to use and be reliant upon digital technologies. This would imply that their digital security risk management practices would need to be, and perhaps are more, sophisticated than older larger enterprises. However, there is little in the way of evidence-based consensus in this area.
- The link between the incidence of digital security attacks or failure and the policies implemented in a country has not been clearly established. Anecdotally, ransomware incidents are not as severe or frequent in Germany as in other OECD countries. This is because the government mandates enterprises to have backups, which makes recovery from a ransomware attack much faster. An evaluation of the impact of some policies, backed by methods involving natural experiments, might shine more light on policies that work with the best return on investment by type of enterprises and sector.
- In addition, as digital services are increasingly connected and extending beyond the reach of a single jurisdiction and control institution, the risks of systemic failures are likely to grow and new governance challenges for businesses and governments to emerge. These single points of failure aggregate systemic risk, which if disrupted could lead to cascading losses throughout economies. Better understanding of where these single points of failure lie, and which enterprises are connected to and reliant upon them, would help future efforts to manage this risk.

All this calls for enhanced co-operation and knowledge exchange: within industries where actors share similar business models; between SMEs and large firms that share similar threats with different and potentially complementary response capacity; across jurisdictions that face no-border attacks; or between policy domains, for instance research and innovation policy and SME policy.

References

Aconet (2020), *The ACOnet CERT*, https://www.aco.net/cert.html?L=1. [100]

Akamai (2020), *Visualizing Global Internet Performance*, https://www.akamai.com/uk/en/resources/visualizing-akamai/ (accessed on 18 July 2020). [46]

Akerlof, G. (1970), "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84/3, p. 488, http://dx.doi.org/10.2307/1879431. [57]

Almeling, D. (2012), "Seven Reasons Why Trade Secrets Are Increasingly Important", *Berkeley Technology Law Journal*, Vol. 27, p. 1091, http://dx.doi.org/10.15779/Z38SM4F. [33]

ANSSI and BSI (2018), "ANSSI/BSI Common situational picture", https://www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf (accessed on 30 March 2020). [5]

Australian Signals Directorate (2020), *About the ACSC*, https://www.cyber.gov.au/about. [97]

Belgian Federal Public Service for the Economy, SMEs, Middle Classes and Energy (2018), *Cybersecurity – is your enterprise ready?*, https://economie.fgov.be/fr/publications/cybersecurite-votre-entreprise (accessed on 11 December 2020). [78]

Biancotti, C. (2017), "Cyber Attacks: Preliminary Evidence from the Bank of Italy's Business Surveys", Bank of Italy, Occasional Paper No. 373, http://dx.doi.org/10.2139/ssrn.2954991. [19]

Biancotti, C. (2017), "The price of cyber (in)security: Evidence from the Italian private sector", Bank of Italy, Occasional Papers No 407, https://www.bancaditalia.it/pubblicazioni/qef/2017-0407/QEF_407.pdf?language_id=1. [26]

Bowman, C. (2015), "A Primer on Russia's New Data Localization Law", *Privacy Law Blog*, https://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/ (accessed on 4 March 2020). [64]

Brant, J. and S. Lohse (2014), "Trade Secrets: Tools for Innovation and Collaboration in Innovation", *Intellectual Property Series*, International Chamber of Commerce, https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-Research-Trade-Secrets-english.pdf (accessed on 18 July 2018). [32]

Calvino, F. et al. (2018), "A taxonomy of digital intensive sectors", *OECD Science, Technology and Industry Working Papers*, No. 2018/14, OECD Publishing, Paris, https://dx.doi.org/10.1787/f404736a-en. [22]

Carnegie Mellon University (2020), "The CERT Division", Software Engineering Institute, http://sei.cmu.edu/about/divisions/cert/index.cfm. [105]

Center for the Protection of National Infrastructure (2020), *Security awareness campaigns*, https://www.cpni.gov.uk/security-awareness-campaigns (accessed on 11 December 2020). [87]

CERT.at (2020), *Australian energy CERT*, https://cert.at/de/ueber-uns/austrian-energy-cert/ (accessed on 11 December 2020). [99]

CERT.at (2020), *Zuständigkeit*, https://www.cert.at/about/scope/scope.html (accessed on 11 December 2020). [98]

Chailytko, A. (2020), *Zoom-zoom: we are watching you*, https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/. [44]

Chander, A. and U. Le (2014), "Breaking the Web: Data Localization vs. the Global Internet", *Emory Law Journal, UC Davis Legal Studies Research Paper* No. 378, https://ssrn.com/abstract=2407858 (accessed on 15 January 2021). [65]

Chander, A. and U. Lê (2015), "Data nationalism", *Emory Law Journal*, Vol. 64/3, https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2 (accessed on 4 March 2020). [61]

Council of Europe (2020), *Mexico: National cybersecurity strategy and awareness campaign*, https://www.coe.int/en/web/cybercrime/-/mexico-national-cybersecurity-strategy-and-awareness-campaign (accessed on 11 December 2020). [85]

CSIRT (2020), *CSIRT Italia*, http://www.csirt-ita.it (accessed on 11 December 2020). [102]

Cyber Management Alliance (2016), "Cyber Essentials: The security standard for small to medium companies", https://www.cm-alliance.com/consultancy/compliance-gap-analysis/cyber-essentials/ (accessed on 7 March 2020). [71]

Cybersecurity and Infrastructure Agency (2020), *Cybersecurity Awareness Month*, https://www.cisa.gov/national-cyber-security-awareness-month. [92]

Cybersecurity and Infrastructure Agency (2020), *Stop. Think. Connect.*, https://www.cisa.gov/stopthinkconnect (accessed on 11 December 2020). [89]

Cybersecurity and Infrastructure Agency (2020), *Stop. Think. Connect. Industry resources*, https://www.cisa.gov/publication/stopthinkconnect-industry-resources. [90]

Cybersecurity and Infrastructure Agency (2020), *Stop. Think. Connect. Small business resources*, https://www.cisa.gov/publication/stopthinkconnect-small-business-resources. [91]

Cyentia Institute (2019), *Information Risk Insights Study 2020*, https://www.cyentia.com/iris/. [24]

Dean, B. (2018), "An exploration of strict products liability and the internet of things", Center for Democracy and Technology, https://dx.doi.org/10.2139/ssrn.3193049. [56]

Dean, B. (2018), *Strict Products Liability and the Internet of Things*, Center for Democracy and Technology, https://cdt.org/wp-content/uploads/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf. [13]

Dean, B. (2017), *Trans-Atlantic Cyber Insecurity and Cyber Crime: Economic impact and future prospects*, European Parliament, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603948/EPRS_STU(2017)603948_EN.pdf. [25]

DeSilver, D. (2020), "Before the coronavirus, telework was an optional benefit – mostly for the affluent few", Pew Research Center, https://www.pewresearch.org/fact-tank/2020/03/20/before-the-coronavirus-telework-was-an-optional-benefit-mostly-for-the-affluent-few/ (accessed on 16 September 2020). [43]

Determann, L. and M. Weigl (2016), "Data residency requirements creeping into German law", *Bloomberg Law*, https://web.archive.org/web/20171207221329/https://www.bna.com/data-residency-requirements-n57982069680/ (accessed on 4 March 2020). [62]

DHS and DoC (2018), *Report on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets"*, https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets. [14]

DKCERT (2020), *DKCERT homepage*, https://www.cert.dk (accessed on 11 December 2020). [101]

ENISA (2020), *European Cybersecurity Month*, https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month (accessed on 11 December 2020). [93]

ENISA (2019), *ECSM Deployment Report 2019*, https://www.enisa.europa.eu/publications/ecsm-deployment-report-2019. [94]

European Commission (2020), *A European Strategy for Data*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - COM(2020) 66 final, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. [31]

European Commission (2020), *Supporting Specialised Skill Development: Big Data, Internet of Things and Cyber Security for SMEs – Final report*, https://op.europa.eu/en/publication-detail/-/publication/bb5c6c09-6285-11ea-b735-01aa75ed71a1/language-en. [95]

European Commission (n.d.), "The EU cybersecurity certification framework", *Shaping Europe's digital future*, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (accessed on 4 March 2020). [68]

Eurostat (2020), *ICT Usage in Enterprises Database*, https://ec.europa.eu/eurostat/data/database (accessed on 18 July 2020). [18]

FBI (2020), "FBI urge vigilance during Covid-19 pandemic", https://www.fbi.gov/coronavirus (accessed on 17 December 2020). [49]

Freedman, B. (2019), *Ready, set, certify – Canada's new CyberSecurity Canada certification program*, https://cybersecuritylaw.ca/home/2019/8/16/ready-set-certify-canadas-new-cybersecure-canada-certification-program (accessed on 4 March 2020). [72]

GovCERT Austria (2020), *GovCERT in Österreich*, http://govcert.gv.at/ (accessed on 11 December 2020). [96]

Government of Brazil (2020), *National Strategy of Cyber Security*, https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419 (accessed on 11 December 2020). [79]

Government of Canada (2020), *Cyber Security Awareness Month Toolkit*, https://www.getcybersafe.gc.ca/cnt/rsrcs/csam-tlkt-en.aspx (accessed on 11 December 2020). [80]

Government of Canada (2017), "Chapter 1: Skills, Innovation and Middle Class Jobs", *Budget 2017*, https://www.budget.gc.ca/2017/docs/plan/chap-01-en.html#archived (accessed on 11 December 2020). [75]

Government of Chile (2020), *National Cybersecurity Policy*, https://www.ciberseguridad.gob.cl/media/2017/05/NCSP-ENG.pdf. [81]

Government of Denmark (2018), *Danish Cyber and Information Security Strategy 2018-2021*, https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf. [83]

Government of Mexico (2016), "Programme for the development of the software industry (PROSOFT) and innovation 2019", https://www.gob.mx/se/acciones-y-programas/programa-para-el-desarrollo-de-la-industria-de-software-prosoft-y-la-innovacion-2016. [76]

Government of Spain (2018), "National security strategy", https://www.dsn.gob.es/documento/informe-anual-seguridad-nacional-2018 (accessed on 11 December 2020). [77]

Greenberg, A. (2018), *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed on 30 March 2020). [6]

IBM/Ponemon (2020), *Cost of a Data Breach Report*, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (accessed on 29 August 2020). [38]

International Association of Privacy Professionals (2017), "China's new cybersecurity law", https://iapp.org/resources/article/chinas-new-cybersecurity-law-2/ (accessed on 4 March 2020). [59]

Internet Segura y Ciudadanía Digital (2020), *Quiénes somos*, http://www.internetsegura.cl/quienes-somos/ (accessed on 11 December 2020). [82]

Kaspersky (2019), *Story of the year 2019: Cities under ransomware siege*, Securelist, https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/ (accessed on 31 March 2020). [8]

Koeze, E. and N. Popper (2020), "The Virus Changed the Way We Internet", *The New York Times*, https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html (accessed on 17 July 2020). [45]

KRCERT (2020), *KRCERT homepage*, http://eng.krcert.or.kr. [103]

Leviathan Security Group (2015), *Quantifying the Cost of Forced Localization*, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf. [66]

Livingston, S. (2017), "China set to expand data localization and security review requirements", International Association of Privacy Professionals, https://iapp.org/news/a/china-set-to-expand-data-localization-and-security-review-requirements/ (accessed on 4 March 2020). [60]

McConnell, B. (2017), *National Cybersecurity Awareness Campaign*, https://www.nist.gov/system/files/documents/2017/01/25/bmcconnell_national-cybersec-awareness.pdf. [88]

Miller, M. (2020), "FBI sees spike in cyber crime reports during coronavirus pandemic", The Hill, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic (accessed on 17 December 2020). [48]

Monitor Deloitte for Erhvervsstyrelsen (2018), *IT security and data management in Danish SMEs*, https://erhvervsstyrelsen.dk/sites/default/files/2019-11/Analyse%20af%20digital%20sikkerhed%20blandt%20SMV%27er%202019.pdf (accessed on 9 September 2020). [51]

Moody's (2019), "Battling hidden cyber exposures, insurers position for growing opportunity", https://www.grupoaseguranza.com/adjuntos/fichero_32099_20190729.pdf (accessed on 9 September 2020). [52]

National center of Incident readiness and Strategy for Cybersecurity (2020), *About NISC*, https://www.nisc.go.jp/eng/. [84]

National Cyber Security Centre (2018), "Executive Summary: the 10 Steps to Cyber Security", https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary. [106]

National Cyber Security Centre (n.d.), *"Information for Individuals and Families"*, https://www.cyberaware.gov.uk/cyberessentials/ (accessed on 4 March 2020). [69]

NIST (2020), *National Vulnerability Database*, https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=last3years. [15]

OECD (2020), "Capacity for remote working can affect lockdown costs differently across places", *OECD Policy Responses to Coronavirus (COVID-19)*, http://www.oecd.org/coronavirus/policy-responses/capacity-for-remote-working-can-affect-lockdown-costs-differently-across-places-0e85740e/ (accessed on 18 July 2020). [40]

OECD (2020), "Coronavirus (COVID-19): SME policy responses", *OECD Policy Responses to Coronavirus (COVID-19)*, http://www.oecd.org/coronavirus/policy-responses/coronavirus-covid-19-sme-policy-responses-04440101/ (accessed on 18 July 2020). [37]

OECD (2020), "Dealing with digital security risk during the Coronavirus (COVID-19) crisis", *OECD Policy Responses to Coronavirus (COVID-19)*, http://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/ (accessed on 18 July 2020). [4]

OECD (2020), *Enabling SMEs to benefit from digitalisation: In progress report*, Internal document, CFE/SME(2020)3. [34]

OECD (2020), "Encouraging digital security innovation", *OECD Working Party on Security in the Digital Economy*, DSTI/CDEP/SDE(2020)7/REV1. [74]

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [1]

OECD (2020), *OECD Digital for SMEs Global Initiative*, https://www.oecd.org/going-digital/sme/ (accessed on 18 July 2020). [36]

OECD (2020), *OECD ICT Access and Usage by Businesses Database*, https://stats.oecd.org/Index.aspx?DataSetCode=ICT_BUS (accessed on 19 September 2020). [21]

OECD (2020), "Seven lessons learned about digital security during the COVID-19 crisis", *OECD Policy Responses to Coronavirus (COVID-19)*, https://www.oecd.org/coronavirus/policy-responses/seven-lessons-learned-about-digital-security-during-the-covid-19-crisis-e55a6b9a/ (accessed on 10 December 2020). [50]

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en. [28]

OECD (2019), "Measuring digital security risk management practices in businesses", *OECD Digital Economy Papers*, No. 283, OECD Publishing, Paris, https://dx.doi.org/10.1787/7b93c1f1-en. [12]

OECD (2019), *OECD SME and Entrepreneurship Outlook 2019*, OECD Publishing, Paris, https://dx.doi.org/10.1787/34907e9c-en. [23]

OECD (2019), "Roles and responsibilities of actors for digital security", *OECD Digital Economy Papers*, No. 286, OECD Publishing, Paris, https://dx.doi.org/10.1787/3206c421-en. [27]

OECD (2018), "Supporting an Effective Cyber Insurance Market: OECD report for the G7 Presidency", http://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf (accessed on 9 September 2020). [53]

OECD (2018), *The Cyber Insurance Market: Responding to risk with few boundaries*, http://www.oecd.org/finance/insurance/The-cyber-insurance-market-responding-to-a-risk-with-few-boundaries.pdf. [55]

OECD (2018), *Unleashing the Potential of the Cyber Insurance Market: Conference outcomes*, http://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf. [54]

OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264276284-en. [30]

OECD (2017), *The Next Production Revolution: Implications for Governments and Business*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264271036-en. [29]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en. [58]

OECD (2010), *SMEs, Entrepreneurship and Innovation*, OECD Studies on SMEs and Entrepreneurship, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264080355-en. [73]

OECD (2021 forthcoming), *OECD SME and Entrepreneurship Outlook 2021*, OECD Publishing, Paris. [35]

OECD (2021, forthcoming), *Understanding the Digital Security of Products: An in-depth analysis*, OECD Publishing, Paris. [16]

Ojala, S. and P. Pyöriä (2017), "Mobile knowledge workers and traditional mobile workers", *Acta Sociologica*, Vol. 61/4, pp. 402-418, http://dx.doi.org/10.1177/0001699317722593. [42]

OWASP (2020), "Security by design principles", Open Web Application Security Project, https://www.owasp.org/index.php/Security_by_Design_Principles (accessed on 11 December 2020). [67]

Pew Research Center (2020), "Telework may save US jobs in COVID-19 downturn – especially among college graduates", http://www.pewresearch.org/fact-tank/2020/05/06/telework-may-save-u-s-jobs-in-covid-19-downturn-especially-among-college-graduates/ (accessed on 15 June 2020). [39]

RT World News (2017), *Ransomware virus plagues 100k computers across 99 countries*, RT, https://www.rt.com/news/388153-thousands-ransomeware-attacks-worldwide/ (accessed on 30 March 2020). [7]

Schneier, B. (2018), *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, Norton & Company. [17]

Shi, F. (2020), "Threat spotlight: Coronavirus related phishing", Barracuda Networks, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ (accessed on 20 June 2020). [47]

Swedish Agency for Economic Growth and Regional Development (2020), *The Digilift is renewing industry*, https://tillvaxtverket.se/english/digitalization.html (accessed on 11 December 2020). [86]

Symantec (2019), *"ISTR Internet Security Threat Report"*, https://docs.broadcom.com/doc/istr-24-2019-en (accessed on 30 March 2020). [2]

United Kingdom Government (2019), *"Cyber Essentials Scheme: overview"*, https://www.gov.uk/government/publications/cyber-essentials-scheme-overview (accessed on 7 March 2020). [70]

US Bureau of Justice Statistics (2005), *National Computer Security Survey*, https://www.bjs.gov/index.cfm?ty=tp&tid=41. [20]

US DHS (2020), "About CISA", US Department of homeland Security CISA Cyber + Infrastructure, https://www.us-cert.gov/about-us. [104]

Verizon (2020), "2020 Data Breach Investigation Report", https://agio.com/newsroom/key-takeaways-from-verizons-2020-data-breach-investigation-report/ (accessed on 30 March 2020). [11]

Verizon (2019), "2019 Data Breaches Investigations Report", http://veriscommunity.net/veris_webapp_min.html (accessed on 30 March 2020). [3]

Vilhelmson, B. and E. Thulin (2016), "Who and where are the flexible workers? Exploring the current diffusion of telework in Sweden", *New Technology, Work and Employment*, Vol. 31/1, pp. 77-96, http://dx.doi.org/10.1111/ntwe.12060. [41]

Webroot (2019), *2019 Webroot Threat Report*, Webroot, https://www-cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf (accessed on 30 March 2020). [10]

Yavuzdogan Okumus, B. (2020), "Latest development on data localization requirements in Turkey", *International Association of Privacy Professionals*, https://iapp.org/news/a/latest-development-on-data-localization-requirements-in-turkey/ (accessed on 11 December 2020). [63]

You, I. and K. Yim (2010), "Malware Obfuscation Techniques: A Brief Survey", *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, http://dx.doi.org/10.1109/BWCCA.2010.85. [9]

Notes

[1] Network security, user education and awareness, malware prevention, removable media controls, secure configuration, managing user privileges, incident management, monitoring, home and mobile working.

See: National Cyber Security Centre (2018[106]), "Executive Summary: the 10 Steps to Cyber Security", available from: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary

[2] Department for Digital, Culture, Media and Sport (2019), Cyber Security Breaches Survey 2019: Statistical Release

[3] This is a set of security procedures, protocols and policies that are in a written form.

[4] Instead of being asked if they had a "formally defined ICT security policy", respondents were asked if they had "document(s) on measures, practices or procedures on ICT security".

[5] Public Law 115-236, NIST Small Business Cybersecurity Act (August 18, 2018), available from: https://www.govinfo.gov/content/pkg/PLAW-115publ236/pdf/PLAW-115publ236.pdf.

[6] California Senate Bill 327, available from: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 (accessed 4 March 2020).

[7] (1) develop an incident response plan; (2) automatically patch operating systems and applications; (3) enable security software; (4) securely configure devices; (5) use strong user authentication; (6) provide employee awareness training; (7) backup and encrypt data; (8) secure mobility; (9) establish basic perimeter defences; (10) secure cloud and outsourced IT services; (11) secure websites; (12) implement access control and authorisation; and (13) secure portable media.

Canadian Center for Cyber Security, "Baseline cyber security controls for small and medium organizations", available from: https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations (accessed 4 March 2020).

[8] www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/; www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/formations-continues-labellisees-secnumedu/cybersecurite-des-tpe-et-des-pme-chef-dentreprise-face-aux-risques-cyber-etes-vous-pret/.

[9] www.ssi.gouv.fr/actualite/petites-et-moyennes-entreprises-decouvrez-le-guide-des-bonnes-pratiques-de-linformatique-adapte-a-vos-besoins/.

[10] www.cybermalveillance.gouv.fr/.

[11] For an example of such activities, see: https://www.nisc.go.jp/eng/pdf/Intl_Campaign_poster.pdf.

[12] https://www.kisa.or.kr/eng/main.jsp.

[13] Identify and code positions with information technology, cybersecurity, and other cyber-related functions using the National Initiative for Cybersecurity Education (NICE) Framework.