Chapter 7

DIGITAL SECURITY

KEY FINDINGS

- Digital security incidents harm businesses, governments and individuals by undermining the availability, integrity and/or confidentiality of their data, information systems and networks. With the advent of the consumer and industrial Internet of Things bridging the online and offline worlds, damages can extend to the physical environment and affect safety.
- Threats such as phishing, denial of service and ransomware attacks are becoming increasingly targeted and sophisticated. Cryptocurrencies continue to attract cybercriminals. Dozens of successful attacks have stolen more than USD 1 billion worth of cryptocurrencies from coin exchanges.
- High-profile attacks have highlighted significant digital security gaps, especially to end-of-life of products that contain software code. OECD countries are increasingly developing digital security labels and regulatory requirements.
- Artificial intelligence and other emerging technologies are a double-edged sword. They hold great promise for better protection, but can also be used to bypass traditional digital security measures. Emerging best practices illustrate the need for more co-operation among stakeholders.
- In 2020, most OECD countries had whole-of-government digital security strategies. However, too often, these strategies lack an autonomous budget, evaluation tools and metrics, and integration into overall national digital plans. The emergence of digital security innovation hubs suggests that governments may increasingly harness digital security for economic development rather than see it only as a cost or a threat.
- The COVID-19 outbreak created a fertile environment for cybercriminals. Massive numbers of people and organisations switched to telework, using new tools for the first time. Malicious actors took advantage of lax security to increase scams and phishing campaigns related to the pandemic.
- Ransomware and distributed denial of service attacks targeted hospitals, but no more than before the COVID-19 crisis. Digital security agencies have raised awareness and aided operators of critical activities, particularly in the health sector.

Introduction

Digital security incidents harm businesses, governments and individuals by undermining the availability, integrity and/or confidentiality of their data, information systems and networks. Victims can face tangible and intangible damages, including monetary losses, reduced competitiveness, reputational damages, interruption of operations and privacy breaches. With the advent of the consumer and industrial Internet of Things (IoT) bridging the online and offline worlds, damages can extend to the physical environment and affect safety.

This chapter reviews trends in digital security risk and digital security policies. It focuses on policies to encourage digital security innovation, improve digital security of products and enhance vulnerability management. Lastly, it introduces challenges and opportunities arising from artificial intelligence (AI) for digital security.

Trends in digital security risk

Digital security risk arises 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 threats, such as a human error or a power cut.

Distributed denial of service attacks are still common, but large-scale ones are rarer

Distributed denial of service (DDoS) attacks are a common type of incident that disrupts the operation 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. In 2016, attackers behind the Mirai botnet took down dozens of the largest North American websites for a few hours. They leveraged over 100 000 endpoints to aggregate over 1.2 Terabits per second (Tbps) of bandwidth.

Data on DDoS attacks generally come from companies offering DDoS mitigation services. They do not have a comprehensive picture of the landscape, but can provide useful insights on key trends. For example, according to Netscout, the magnitude of the largest DDoS attacks has increased over time. In 2005, the largest attacks reached 11 Gigabits per second (Gbps), 50 Gbps in 2009, 100 Gbps in 2010, 500 Gbps in 2015 and 800 Gbps in 2016. In 2018, one reached 1.7 Tbps (Netscout, 2019[1]).

In 2019, such spectacularly large DDoS attacks were not detected. This reveals perhaps attackers' reluctance to attract attention from law enforcement for attacks that are disproportionate in light of their (malicious) benefits. However, the number of common DDoS attacks detected by Netscout is still high, with 6.91 million attacks in 2018, 4% less than in 2017 (Netscout, 2019[1]).

In 2018, the frequency of large-scale DDoS attacks decreased year on year, while attackers multiplied smaller attacks in the 100 Gbps to 200 Gbps range (Netscout, 2020[2]). This is still high for most online services. DDoS attacks do not need to use such massive amount of bandwidth to block online services. In 96% of cases, DDoS attacks in 2018 consumed less than 10 Gbps (NexusGuard, 2019[3]). Meanwhile, 91% of enterprises that experienced a DDoS attack indicated that at least one attack completely saturated their Internet bandwidth (Netscout, 2019[1]). While the longest attack in Q3 2019 lasted more than 20 hours, 85% of attacks lasted fewer than 90 minutes; only 0.78% lasted over 20 hours (NexusGuard, 2019[3]).

The People's Republic of China (hereafter "China") (19.87%), Turkey (15.25%), the United States (15.24%) and Korea (12.33%) accounted for over 60% of the devices involved in DDoS attacks detected by NexusGuard in Q3 2019. This figure indicates the location of the compromised zombie hosts participating in the attack rather than that of the criminals controlling them (NexusGuard, 2019[3]). However, these figures only account for DDoS attacks that can be traced back to the compromised hosts.

Phishing remains high and is becoming more difficult for humans to detect

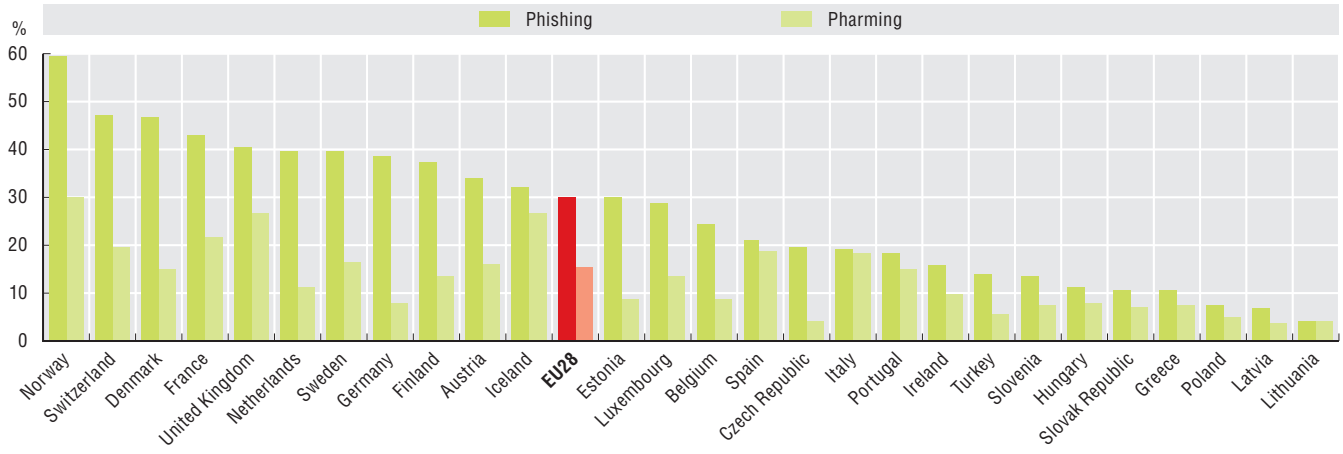
In phishing, one of the main vectors, attackers disguise themselves as a trustworthy entity in an online communication. In this way, they obtain sensitive information, such as usernames and passwords, or deliver malicious code ("malware"). There are different types of phishing attacks. Phishing messages often include links to malicious sites that are increasingly difficult for end-users to detect without using some automated protection. Broad untargeted campaigns aim to collect credentials by directing users to fake e-commerce or financial websites. More sophisticated emails target specific individuals to plant malware in their organisation's information system (spear-phishing).

In European Union (EU) countries, phishing and pharming (being redirected to fake websites that ask for personal information) vary greatly between countries (Figure 7.1). Based on surveys of individuals and households, 60% of Internet users in Norway have experienced phishing, but the figure drops to less than 10% in Greece, Poland, Latvia or Lithuania. More than 25% of Internet users in Iceland and the United Kingdom and 30% in Norway have experienced pharming, but less than 10% in 13 other EU countries. Various factors might contribute to explain those differences. These include lack of awareness/understanding of phishing attempts and/or the inability to identify them, national languages, security measures offered by email and Internet service providers (ISPs), etc.

According to Symantec, spear-phishing remained the most popular avenue for targeted attacks in 2018. It was used by 65% of all known cybercrime and state-sponsored groups (Symantec, 2019[5]). According to Verizon, 32% of data breaches in 2018 involved phishing activity. Phishing was present in 78% of digital security espionage incidents, including the installation and use of backdoors (Verizon, 2019[6]).

Figure 7.1. Individuals who experienced phishing and pharming attacks, 2019

As a percentage of all Internet users



Notes: Phishing relates to receiving fraudulent messages. Pharming relates to being redirected to fake websites asking for personal information.

Source: OECD based on Eurostat (2019[4]), *Digital Economy and Society Statistics*, Comprehensive Database (accessed in March 2020).

StatLink https://doi.org/10.1787/888934192338

The frequency of phishing attacks is unclear, largely due to the absence of common definitions and divergences in measurement tools and techniques. For example, phishing levels declined in 2018, dropping from 1 in 2 995 emails to 1 in 3 207 emails from the year before (Symantec, 2019[5]). At the same time, another study found phishing attacks in 1% of 55.5 million emails received by a sample of companies with 20 to 100 000 employees in 2018 (Avanan, 2019[7]). A third study found a 40.9% increase in phishing attacks in 2018 (PhishLabs, 2019[8]). According to PhishLabs, these emails aimed at implanting malware on the recipient's device (50.7%), harvesting credentials (40.9%), extorting money (8%) and spear-phishing (0.4%).

Several sources report a significant increase in the number of websites deemed dangerous or malicious. For example, Symantec security software identified 1 in 10 URLs in 2018 as malicious, up from 1 in 16 in 2017. Every day in 2018, Symantec software blocked, on average, almost 1 million users from clicking on a link containing malicious content (Symantec, 2019[5]). The number of phishing sites detected by Google Safe Browsing service has also drastically increased since 2017, while malware sites significantly decreased during the same period (Google, 2020[9]). It is unclear, however, whether this discrepancy accounts for variations in the number of phishing and malicious sites or for variations in how Google and Symantec tools detect them.

Table 7.1. Certificates for valid vs. lookalike domains for top 20 retailers in five countries

Country	Certificates for valid retail domains	Lookalike domains	Percentage
United States	12 272	28 532	232
United Kingdom	3 848	6 449	168
France	1 071	318	30
Germany	975	3 617	371
Australia	593	1 735	293
Total	**18 759**	**40 651**	**217**

Note: Not all lookalike domains are suspicious.

Source: Venafi (2018[10]), *Venafi Research Brief: The Risk Lookalike Domains Pose to Online Retailers*, *https://www.venafi.com/sites/default/files/2018-09/Venafi-Research-Retail-Lookalike-Domains-1809.pdf* (accessed on 30 March 2020).

More generally, the presence of a Secure Sockets Layer (SSL) padlock pictogram is no longer sufficient to trust a hyperlink. The hosts of an increasing number of phishing sites use technically valid digital certificates. According to Phishlabs, 50% of malicious phishing sites were using valid SSL digital certificates in Q4 2018. This was up from 30% in Q4 2017 and from less than 5% in 2016 (PhishLabs, 2019[8]).

Furthermore, a security firm analysis of over 32 billion URLs found that 40% of malicious URLs were on legitimate websites compromised to host malicious content. The study underlined that users clicking on short links using URL shorteners such as bit.ly had a 1 in 130 chance of landing on a malicious page in 2018 (Webroot, 2019[11]).

Ransomware attacks become more targeted

Ransomware is a type of malicious software that uses cryptography to limit or disable the accessibility of data and demands a ransom for recovery. Ransomware attacks are a form of digital extortion (ANSSI and BSI, 2018[12]). Although ransomware has been around for many years, it hit mainstream headlines in 2017.

The WannaCry and NotPetya attacks used malware designed to spread rapidly inside and outside victims' networks, to encrypt files and to ask for a ransom in exchange for a decryption key. WannaCry infected over 100 000 systems globally, while NotPetya initially infected devices in Ukraine prior to rapidly spreading globally.

Together, these two ransomware caused billions of dollars of damage to businesses such as Boeing, Beiersdorf (Nivea), Deutsche Bahn, DHL, DLA-Piper, FedEx (USD 400 million), Honda, Renault, Merck (USD 870 million), Mondelez, Petrobras, PetroChina, Reckitt Benckiser, Rosneft, Saint-Gobain (USD 384 million) and AP Moller Maersk (USD 300 million) (Greenberg, 2018[13]). They also affected public sector organisations such as the National Health Service in the United Kingdom and the Russian Interior Ministry (RT World News, 2017[14]). The total cost of these attacks is unclear because a large number of small and medium-sized enterprises (SMEs) were also likely affected.

These high-profile attacks helped raise awareness about digital security and encouraged many businesses and organisations to enhance their basic security measures, including backup and recovery plans. As a result, ransomware attacks evolved in 2018 to become more targeted. For example, security firms observed a 20% decrease in ransomware activity (Symantec, 2019[5]). To increase the likelihood of receiving a ransom, cybercriminals have been increasingly choosing their victims among organisations that heavily rely on information and communication technologies (ICTs) and are known to pay less attention to digital security. Examples included in 2018 and 2019:

- Ports in Barcelona (Tsonchev, 2018[15]) (Spain), San Diego (Senzee, 2019[16]) and Long Beach (United States).
- Airports in Bristol (Cimpanu, 2018[17]) (United Kingdom), as well as Atlanta (Saraogi, 2019[18]), Cleveland (Goud, n.d.[19]) and New York (Insurance Journal, 2020[20]) (United States).
- Hospitals and health care organisations in the United States, including 17 hospitals tied to New Jersey's Hackensack Meridian Health (Eddy, 2020[21]); and hospitals in in Alabama, Washington, California, Ohio, Hawaii, as well as others in Australia, Romania and France (CISO MAG, 2019[22]; Garrity, 2019[23]; Eddy, 2020[21]). In February 2020, NRC Health in the United States had to shut down its systems due to a ransomware attack. The company sells patient administration tools to 9 000 health care institutions, including 75% of the 200 largest hospital chains (DARK Reading, 2020[24]).
- Local governments. At least 174 municipal organisations were targeted by ransomware in 2019, a 60% increase from 2018 (Kaspersky, 2019[25]). Examples include cities and regions in Canada – Nunavut (Osborne, 2019[26]); France – Grand Est region (Vitard, 2020[27]) and Sarrebourg (Héritier, 2019[28]); United States – Baltimore (Chokshi, 2019[29]), New Orleans City (Korosec, 2019[30]), State of Louisiana (Gallagher, 2019[31]) and 23 local governments in Texas; and South Africa – Johannesburg (Goodin, 2019[32]).

In all these cases, the scenario is often the same: the entity under attack is paralysed, the leadership contacts emergency response services and evaluates whether to pay the ransom. The demand for ransom ranged from USD 5 000 to USD 5 million. On average, it was equal to around USD 1 million, with great variations depending on the size of the city (Kaspersky, 2019[25]).

According to limited data gathered by a US security firm, only 17.1% of state and local government entities hit by ransomware paid the ransom. Meanwhile, 70.4% of agencies confirmed they did not pay the ransom (Liska, 2019[33]). For example, the city of Baltimore refused to pay the USD 114 000 ransom and spent USD 18 million to restore its infrastructure.

Ransomware can paralyse physical operations in plants and manufacturing environments. If attackers obtain access to the information technology (IT) system, they may successfully pivot their attack towards the operational technology (OT) infrastructure that manages physical installations.

In February 2020, for example, a natural gas facility was forced to shut down operations for two days after becoming infected with commodity ransomware (CISA, 2020[34]). Attackers first targeted the plant with a spear-phishing email, through which they accessed the OT network.

The ransomware used to attack the gas plant was not specially designed to paralyse industrial control systems (ICS). However, in December 2019, a security firm identified a new ransomware called Ekans or Snake that could paralyse such systems. It targets ICS such as manufacturing, product handling, production and distribution in plants, factories, along pipelines and rail tracks, on oil platforms, solar panels, etc. (Palmer, 2020[35]).

Cryptocurrencies continue to attract cybercriminals

Malicious actors have employed different means over the last five years to exploit a growing interest in cryptocurrencies.

Most commonly, cryptocurrencies are stolen from cryptocurrency exchanges. Between 2012 and 2019, at least 42 successful attacks hit exchanges. In 2019, for example, 12 attacks resulted in the theft of USD 292 million worth of cryptocurrencies. In 2018, eight attacks resulted in the theft of USD 844 million (Table 7.2).

Some of these attacks led affected companies to bankruptcy (e.g. Mt. Gox, Cryptopia, Youbit). In some cases, partial amounts were recovered or reimbursed to clients. Some exchanges have been successfully attacked several times, such as Bithumb (Cimpanu, 2019[36]). The exact circumstances of attacks are often described as unclear.

Some attackers choose to exploit vulnerabilities in cryptocurrency software. In February 2020, for example, the entire network of the non-profit organisation behind the IOTA cryptocurrency was shut down. This was in response to criminals exploiting a vulnerability in the official IOTA wallet app to steal users' funds. The losses are estimated to be around USD 1.6 million worth of IOTA coins (Cimpanu, 2020[38]).

Other attackers take control of the blockchain supporting a cryptocurrency. In 2018, Bitcoin Gold (BTG) was delisted from cryptocurrency exchange Bittrex following an initial 51% attack. Attackers had assumed a majority of the network's processing power to reorganise the blockchain allowing for a USD 18 million worth of double spending (Canellis, 2018[39]). In January 2020, another 51% attack allowed for double spending USD 72 000 worth of BTG. In 2018, Ethereum Classic suffered a similar 51% attack totalling USD 1.1 million worth of double spending of ETC coins (Beedham, 2019[40]).

Over the last three years, malicious actors have also developed more inconspicuous techniques called cryptomining and cryptojacking. Cryptomining occurs when criminals install malware that usurps a user's processing power to mine cryptocurrency. Cryptojacking is cryptomining through scripts inserted in web content running in the user's browser.

According to several sources, both cryptomining and cryptojacking have grown rapidly to become major threats. For example, in 2018, Symantec blocked 69 million cryptojacking events, four times as many events as in 2017 (Symantec, 2019[5]). In late 2017, cryptojacking started with Coinhive that was promoted as a means for website owners to make money without advertising. Criminals quickly diverted Coinhive and attacked legitimate sites. They then inserted the script in pages to retrieve the resulting coins it would mine from users visiting the site. Later, many other cryptojacking scripts were found on line. In Brazil, the vulnerable MikroTik routers were massively attacked to insert a cryptojacking script onto every webpage browsed via the router (Trustwave, 2019[41]). However, the cryptomining rush of 2018 may have dried out in 2019 (Malwarebytes Labs, 2020[42]).

Table 7.2. Cryptography exchanges affected by digital security attacks

Exchange	Location	USD stolen
	2019	
Upbit	Korea	51 million
VinDAX	Viet Nam	500 000
Bitpoint	Japan	30 million
Bitrue	Unknown	5 million
GateHub	United Kingdom, Slovenia	10 million
Binance	China	40 million
DragonEx	Unknown	7 million
Bithumb	Korea	20 million
CoinBene	Unknown	> 100 million
Coinbin	Korea	30 million
Coinmama	Slovak Republic	Unknown
Cryptopia	New Zealand	3 million
	2018	
MapleChange	Canada	5.7 million
Zaif	Japan	60 million
Coinrail	Korea	40 million
Bithumb	Korea	31 million
Taylor	Estonia	1.5 million
CoinSecure	India	3.5 million
Bitgrail	Italy	170 million
Coincheck	Japan	533 million
	2017	
NiceHash	Slovenia	62 million
Youbit	Korea	Unknown
Bithumb	Korea	7 million
Yapizon	Korea	5 million
	2016	
Bitfinex	Hong Kong, China	72 million
GateCoin	Hong Kong, China	2 million
ShapeShift	Switzerland	230 000
	2015	
BTER	China	1.5 million
KipCoin	China	Unknown
Bitstamp	United Kingdom, Slovenia, Luxembourg	5.1 million
LocalBitcoins	Finland	Unknown

Notes: Many of these cases are still under investigation. Estimates of amounts stolen are based on available information. They reflect the value of the stolen coins when the attack was first made public. Location can be unknown or vary across time.

Source: OECD based on SelfKey (13 February 2020[37]), "A comprehensive list of cryptocurrency exchange hacks", *https://selfkey.org/list-of-cryptocurrency-exchange-hacks/* and additional research.

Malware is increasingly sophisticated

Malicious actors demonstrate considerable agility and innovation, adapting malware to evade detection and target new technologies. Between 2018-19, for example, security company TrendMicro noted an 18% increase in the prevalence of fileless techniques (Trend Micro, 2019[43]). Fileless malware is less visible since the code is only executed in a system's memory or leverages normally allowed tools installed in a system. Cryptojacking malware fall into this category as they are executed in the user's browser without leaving any trace on the hard drive.

Malware has evolved from encrypted to oligomorphic to polymorphic and metamorphic. Over time, malicious actors have considerably improved their techniques to develop malware that can better evade detection.

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 decrypts it and remains the same across infections.

Oligomorphic malware can change its decryptor at each generation of the malware code, i.e. each time the code is spreading to a different place. But this technique can only produce a few hundred different generations, which is not sufficient to evade security tools.

Polymorphic malware can create a countless number of decryptors using a mutation engine. It is impossible to be detected by simple signature-based security tools. According to Webroot (2019[11]), 93% of malware was polymorphic in 2017 and 2018.

Metamorphic malware can completely rewrite its code. In this way, each new version of itself propagated elsewhere no longer matches its previous iteration without using encryption (You and Yim, 2010[44]). The morphing engine code can take up to 80% of the overall malware code, versus 20% only for the actual malicious payload (Crane, 21 May 2019[45]).

Box 7.1. Emotet, the tenacious multi-purpose malware

Malware can live long and evolve over time. For example, the Emotet Trojan, discovered in 2014, continued to spread and create harm in 2020. A Trojan is a type of malware that conceals its true content to fool a user into thinking it is a harmless file. Emotet is among the most costly and destructive malware affecting the public and private sector (CISA, 2018[46]). For example, the city of Allenton, Pennsylvania, spent USD 1 million to eliminate it from its systems (The Morning Call, 2018[47]).

Emotet is a polymorphic banking Trojan that can evade typical signature-based detection. It uses several methods such as remote command and control servers to maintain persistence, continuously evolve and update its capabilities. Furthermore, it is Virtual Machine-aware and can generate false indicators if run in a virtual environment (a common way for security experts to contain and analyse malware without exposing sensitive information). It is disseminated through spam with malicious attachments or links that use branding familiar to the recipient.

Emotet uses a victim's contact list to send itself to other people, sometimes sending a message that includes the contents of a previous email exchange between the victim and the recipient. Once downloaded, Emotet establishes persistence and attempts to propagate the local networks.

Between 2014 and 2020, Emotet evolved to integrate new features. From initially stealing bank account details, it began transferring money, sending spam and installing other malware to infected machines, such as other Trojans and ransomware. For example, Lake City, Florida, was infected by Emotet, which installed a ransomware forcing the city to pay USD 460 000. In January 2020, a concerted phishing campaign used emails purporting to be from the Permanent Mission of Norway to the United Nations. The emails, sent to 600 staffers and officials across the United Nations, tried to trick recipients into installing Emotet.

Sources: Seals (2020[48]), "U.N. weathers storm of Emotet-TrickBot malware", *https://threatpost.com/un-weathers-emotet-trickbot-malware/151894/*; McKay (2019[49]), "Florida City fires IT employee after paying $460,000 bitcoin ransom to hackers", *https://gizmodo.com/florida-city-fires-it-employee-after-paying-460-000-in-1836031022* (accessed on 6 April 2020).

Malicious actors leveraged the COVID-19 crisis to make their attacks more successful

Malicious actors leveraged the coronavirus epidemic to make their attacks more successful, especially phishing campaigns using COVID-19 content. Emails with a coronavirus theme in the subject field or as an attachment filename, for example, have circulated. Attackers have also sent emails or SMS impersonating governments in Australia and the United Kingdom, as well as leaders or institutions such as the World Health Organization. In addition, they have sent emails, links or web applications

mimicking legitimate initiatives. In March 2020, for example, a security firm found that Italian companies saw a rise in phishing attacks. One phishing campaign in Italy with a COVID-19 theme hit over 10% of all organisations in the country, luring email recipients into opening a malicious attachment. Cybercriminals also mimicked the Johns Hopkins University's interactive dashboard[1] that tracks coronavirus infections to spread password-stealing malware. The malware kit was for sale on underground dark web forums for USD 200. An email campaign targeting health care and manufacturing industries in the United States in early March 2020 abused a legitimate distributed computing project for disease research. The email asked recipients to install an attachment to help find a coronavirus cure. The attachment contained malware stealing credentials and cryptocurrency cold wallets (cryptocurrency wallets that are stored off line).

During the crisis, there have also been cases of ransomware and DDoS attacks targeting essential activities. Hospitals in France and Spain, for example, were hit by DDoS attacks, while the Brno Hospital in the Czech Republic was severely hit by a ransomware. However, such attacks were neither more numerous nor more sophisticated than before the crisis.

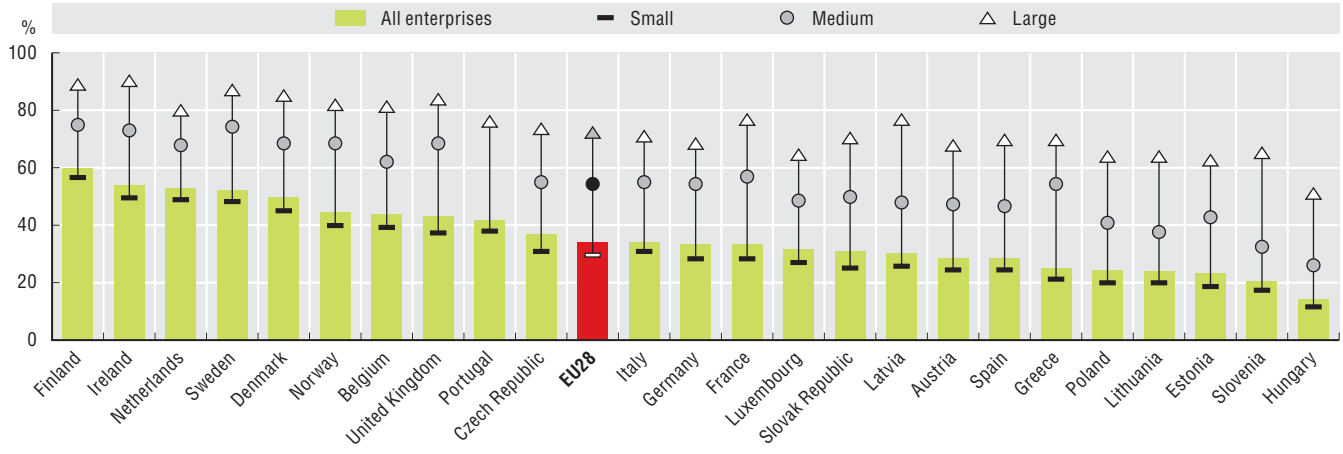
Digital security risk management measures in businesses

Given the complexity of digital security risk management, it is difficult to quantify the extent to which businesses implement good practices in this area. Nevertheless, several recent statistical indicators provide useful insights. They measure specific aspects that can be used as proxies to form a relatively valid representation of this situation in the European Union. They relate to firms assessing digital security risk, making their employees aware of digital security obligations, implementing security tests or regular backups, and insuring against digital security incidents.

Digital security risk assessment – the periodical assessment of probability and consequences of digital security incidents – is at the core of digital security risk management (OECD, 2015[50]). Overall, the share of enterprises carrying out risk assessment ranges from 14% in Hungary to 60% in Finland. As for other digital security indicators, this share is increasing on average with the size of firms. It is less than one-third among small firms but nearing three-quarters among large firms (Figure 7.2).

Figure 7.2. Enterprises making ICT risk assessment, by size, 2019

As a percentage of enterprises in each employment size class



Note: Risk assessment: periodical assessment of probability and consequences of ICT security incidents.

Source: OECD based on Eurostat (2019[4]), *Digital Economy and Society Statistics*, Comprehensive Database (accessed in March 2020).

StatLink https://doi.org/10.1787/888934192357

Digital security risk assessment is essential to help decide what to do with the risk. The risk can be reduced or transferred. It can also be taken or eliminated, although eliminating removes both risk and benefits. To reduce risk to an acceptable level, firms have to select security measures commensurate to the risk and the context. Too much security would inhibit the economic and social activities the security measures aim to protect. Too little security would not sufficiently lower the risk. Security measures may include security tests, backup procedures, cryptography techniques, two factor authentication, network access control and usage of Virtual Private Networks.

In the European Union, risk assessment practices strongly correlate with security tests or backup procedures (Figure 7.3). As observed for other ICT security indicators in this section, large firms undertake those activities on average much more frequently than small firms. In addition, the variability across countries is relatively similar between large and small firms for security tests, but much broader among small firms compared to large firms for backup. Across EU countries, a high share of large firms carry out backups regardless of the share of large firms practising risk assessment. By contrast, in countries where a large share of SMEs practise risk assessment, a large share of SMEs also practise backups. This suggests that backup in large firms is part of core digital security practices, while in SMEs it is more sensitive to the practice of risk assessment.

Figure 7.3. Risk assessment, ICT security tests and backup in small and large firms, 2019

As a percentage of enterprises in each employment size class

Notes: SMEs = small and medium-sized enterprises. "ICT security tests" relate to activities such as performing penetration tests, testing security alert systems, review of security measures or testing of backup systems. "Backup" refers to data backup to a separate location (including backup to the cloud).

Source: OECD based on Eurostat (2019[4]), *Digital Economy and Society Statistics*, Comprehensive Database (accessed in March 2020).

StatLink https://doi.org/10.1787/888934192376

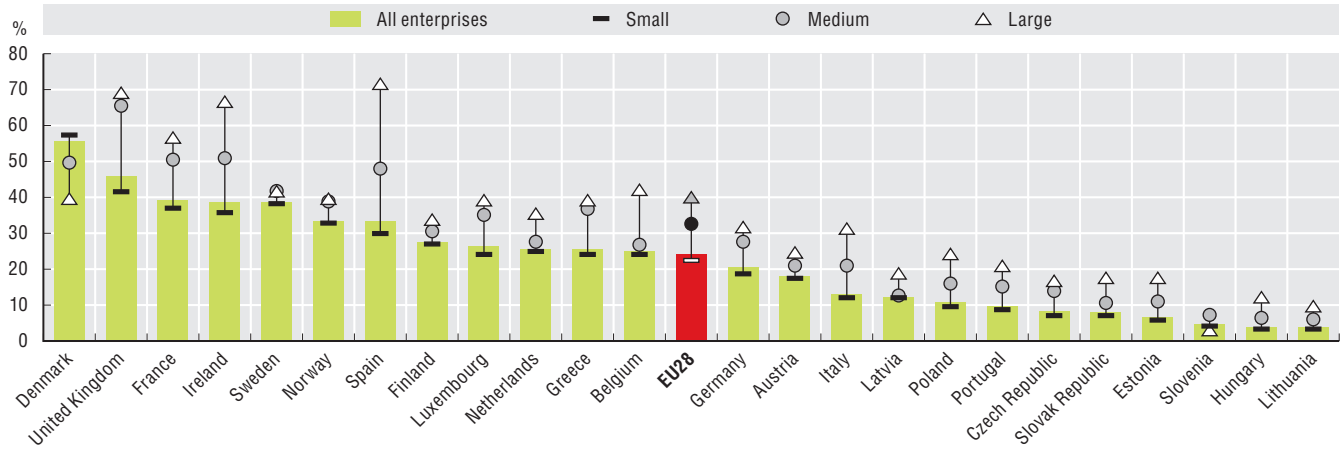
Firms can decide to transfer the risk by buying insurance, if it is available. EU firms' propensity to acquire insurance policy is highly variable, ranging from 4% in Lithuania to more than 56% in Denmark. In all but two EU countries, the propensity increases with the size of enterprises. In Denmark, it is significantly higher among small enterprises (57%) compared to medium (5%) and large enterprises (40%). This is also the case in Slovenia, although to a much lesser extent (Figure 7.4). In general, the propensity to acquire insurance can be viewed as a sign of how seriously firms consider digital security. However, it also depends upon the extent to which insurance policies covering digital security risk are available in the country. The digital security insurance market is complex. Traditional insurance policies or stand-alone "cyber insurance" policies may cover risks. As a result, some companies may think traditional policies cover them when they do not (OECD, 2020[51]).

Another indication of commitment to digital security is the share of enterprises making persons employed aware of their obligations in issues related to ICT security. It ranges from one-third in Greece to more than three-quarters in Ireland, where there is also a high concentration of businesses in the ICT sector, often multinational bridgeheads for Europe. This share is also increasing with the size of enterprises: less than 60% among small enterprises, but more than 90% among large enterprises (Figure 7.5).

More generally, all the above indicators based on Eurostat data clearly show the propensity of the firms to implement digital security measures increases with their size. Furthermore, this propensity is also systematically higher for firms in specific industries, such as the ICT sector, or professional, scientific and technical activities. In addition, risk assessment is also higher, on average, in real estate activities. Lastly, risk assessment is relatively higher in the energy industry compared to other sectors in Finland, Ireland, Norway and Sweden.

Figure 7.4. Enterprises with insurance against ICT security incidents by size, 2019

As a percentage of enterprises in each employment size class

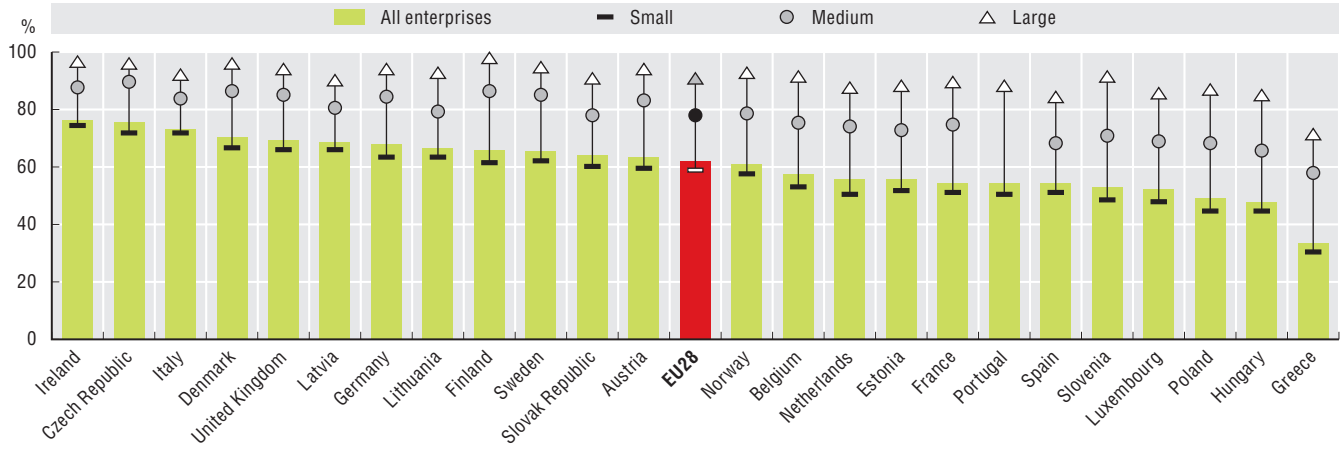


Source: OECD based on Eurostat (2019[4]), *Digital Economy and Society Statistics*, Comprehensive Database (accessed in March 2020).

StatLink https://doi.org/10.1787/888934192395

Figure 7.5. Enterprises making persons employed aware of their obligations in issues related to ICT security, by size, 2019

As a percentage of enterprises in each employment size class



Source: OECD based on Eurostat (2019[4]), *Digital Economy and Society Statistics*, Comprehensive Database (accessed in March 2020).

StatLink https://doi.org/10.1787/888934192414

Evolution of digital security policies

This section provides information about public policy initiatives by OECD countries in the area of digital security. It is based on the responses of the 12 countries that completed a questionnaire on digital security circulated during the summer of 2019. The term "countries" therefore refers to the countries that have completed the questionnaire.

Digital security strategies have become the norm in OECD countries as a whole-of-government challenge

In 2020, most OECD countries had a national digital security strategy. For most strategies, the overarching vision is to protect national and international security, support economic and social prosperity and/or foster trust and confidence in the digital environment. Preserving human rights and enhancing governmental co-ordination are less likely to be part of the strategy's overarching vision.

Capacity building and protecting critical infrastructures are usually the main pillars of the national digital strategies, as well as information sharing and international co-operation. For instance, in Denmark, as part of the digital security strategy, the government has established a portal

(*https://sikkerdigital.dk/*) dedicated to information sharing and co-operation. It provides information and specific tools for citizens, businesses and authorities regarding digital security, as well as advice on how to comply with legislation. The portal is regularly updated with warnings regarding current threats (e.g. ongoing phishing campaigns).

Most countries recognise that digital security is a whole-of-government challenge. Its implications range from technology and law enforcement to national security and economic and social prosperity. Therefore, the development of the digital security strategy typically involves several ministries and agencies across government.

To ensure policy coherence and reduce overlap across parties, digital security policies usually acknowledge the need for a co-ordination mechanism. However, there is no one-size-fits-all model. In Denmark, for example, the Agency for Digitisation (within the Ministry of Finance) and the Centre for Cyber Security (Ministry of Defence) jointly manage digital security. This role is handled in the Netherlands by the Ministry of Justice. In countries such as the United States, Latvia and Spain, a national council gathers representatives of all ministries and agencies involved.

Most countries acknowledge the importance of multi-stakeholder co-operation for successful implementation of a digital security strategy. However, such co-operation varies greatly across countries. Some governments co-operate only on an ad-hoc basis with specific trade associations, while others involve stakeholders more broadly from the design phase. For instance, Brazil created three working groups to help design the strategy. These focused on digital governance (regulation, research, education and innovation); prevention and mitigation of threats; and protection of government and critical infrastructures. Each group gathered experts from the government, academia and the private sector.

Among OECD countries, the scope of the co-operation varies. Overall, operators of critical infrastructures and organisations representing the technical community are often involved in developing the digital security strategy, as well as businesses more broadly. Civil society and SMEs are less often part of the process.

Digital security strategies have significant challenges for implementation and evaluation

Most countries recognise the need to articulate the digital security strategy with other high-level policy planning such as digital transformation and national security. However, these strategies are typically designed in silos, and often linked as an afterthought. This limits the ability of governments to articulate a strategic and comprehensive approach. In Japan, the government has integrated the digital security strategy into the framework of "Society 5.0". This consists of achieving a human-centred society that balances economic advancement with the resolution of social problems by a system that highly integrates the digital and physical spaces.

Most countries declare they regularly assess progress on the implementation of their digital security strategies. However, few have comprehensively measured activities related to digital security. Without stronger evidence, it is difficult to fully analyse the results of digital security strategies and identify their shortcomings.

Similarly, few countries have allocated a specific budget to implement their digital security strategy. Their ministries and agencies are expected to carry out digital security within their existing budget. As a result, many countries find it difficult to determine how much budget is dedicated to implement their digital security strategy overall.

Most countries have prioritised the need to increase the pool of digital security and risk management graduates and practitioners. However, this typically requires co-ordination with other ministries not often involved in digital security policy, such as education or research portfolios. In the United States, the National Institute of Standards and Technology (NIST), within the Department of Commerce, has launched the National Initiative for Cybersecurity Education (NICE). The initiative is a partnership between government, academia and the private sector to close the hiring gap in the cybersecurity workforce. To that end, it organises events such as the NICE Conference and expositions, working group meetings and free webinars.

Other key challenges for policy makers are promoting digital security risk management as a business priority for leaders in public and private organisations and encouraging greater information sharing.

To address those risks, and increase the level of risk ownership by the private sector, governments need to facilitate effective and trust-based multi-stakeholder partnerships.

Few governments have policies to support a digital security industry. This shows that digital security is still mainly perceived as a cost or a risk, and much less as an opportunity. More detail on such initiatives is provided below.

Beyond national strategies and policies, governments across the OECD are facilitating new forms of multi-stakeholder and international partnerships to enhance digital security. For example, the Paris Call for Trust and Security in Cyberspace was launched in 2018. As of March 2020, it had the support of 78 governments, 633 companies, 343 organisations and members of civil society, and 29 public authorities and local governments. This high-level declaration calls for increased co-operation to develop common principles in tackling new challenges, such as the digital security of products and the management of vulnerabilities. Similarly, groups of businesses launched both the Charter of Trust (Charter of Trust, n.d.[52]) and the Cybersecurity Tech Accord (Cybersecurity Tech Accord, n.d.[53]) in 2018. They call for increased co-operation to enhance the digital security of products (see below).

Digital security agencies have taken steps to counter digital security risk related to COVID-19

Government agencies in charge of digital security across OECD countries have responded to the coronavirus crisis in several ways. They have raised awareness, monitored the threat landscape, provided assistance where appropriate and co-operated with all relevant stakeholders, including at the international level:

- The United States' Cyber and Infrastructure Security Agency (CISA) set up a new section on its website dedicated to security risks related to the COVID-19 crisis (*www.cisa.gov/coronavirus*).
- The European Commission, European Union Agency for Cybersecurity, Europol and the Computer Emergency Response Team for the EU Institutions, bodies and agencies co-operated to track malicious activities related to COVID-19 and alert their respective communities.
- The Canadian Centre for Cybersecurity published an alert recommending that Canadian health organisations involved in the national response to the pandemic remain vigilant and ensure they are engaged in digital security best practices.
- The Czech National Office for Cyber and Information Security (NÚKIB) ordered selected health care entities to enhance the security of key ICT systems. The agency offered consultations and support to these entities.

In addition, many businesses, as well as industry and professional groups, communicated to the public about digital security risks related to the COVID-19 crisis. Many of them created one-stop shops and resource libraries. This allows them to advise on specific topics such as secure telework.

Policies to encourage digital security innovation

Digital security innovation is an emerging trend in the OECD and other countries. More and more governments are implementing national strategies and opening centres to encourage innovation. Examples include Israel, Australia, the United Kingdom, Singapore, Germany, France and the European Union.

In 2014, Israel created CyberSpark, a digital security innovation campus located in Be'er Sheva (CyberSpark, n.d.[54]). CyberSpark brings together major stakeholders – academia, industry, venture capital and government – on the same campus to collaborate and share ideas. By working so closely, stakeholders can learn from one another. For example, it can often be difficult for academia to keep up with the pace of change in industry. If academia and industry reside together and speak regularly, they can learn from one another and find out what they need. As industry progresses, the campus can keep its curriculum up to date and graduates are more mature and better placed to contribute to the workforce. The government intends to grow the workforce in CyberSpark to 2 500 employees by 2026 and to attract the top global companies. EMC, Deutsche Telekom, PayPal, Oracle, IBM and Lockheed Martin have already set up offices (Israel Ministry of Foreign Affairs, 2015[55]).

Launched in 2017, the Australian Cyber Security Growth Network is an independent organisation, fully funded by government, which supports the development of a vibrant and globally competitive digital

security sector (AustCyber, n.d.[56]). It advises digital security companies, helping them identify sectoral challenges. In total, there are 300 digital security companies in its ecosystem, and the organisation provides USD 50 million to 15 projects.

In 2018, the United Kingdom's Department for Digital, Culture, Media & Sport, launched the London Office for Rapid Cybersecurity Advancement (LORCA), in partnership with Plexal, Deloitte and Queen's University Belfast. LORCA hosts digital security start-ups on its campus at Here East in London. Its mission is to support digital security innovators in scaling and developing solutions to meet industry's biggest challenges (LORCA, n.d.[57]). To that end, it selects start-ups for a 12-month scale-up programme that helps small and large organisations, investors, academics and the international community connect with each other. In 2020, LORCA had supported 45 start-ups since its creation, from 9 in its first cohort to 20 in its fourth cohort (2020).

Singapore established the region's first digital security entrepreneur hub, the Innovation Cybersecurity Ecosystem (ICE71), in 2018. Based in Singapore, ICE71 is a partnership between Singtel Innov8 (the venture capital arm of the Singtel Group) and the National University of Singapore (NUS) through its entrepreneurial arm NUS Enterprise (ICE71, n.d.[58]). ICE71 strengthens the region's growing digital security ecosystem by attracting and developing technologies to mitigate the rapidly increasing digital security risk. ICE71 runs programmes to support digital security start-ups from idea development to scaling, supported by the Cyber Security Agency of Singapore and the Info-Communications Media Development Authority. It has supported and empowered over 70 start-ups since its launch in March 2018 (ICE71, n.d.[58]).

The German government set up the Agency for Innovation in Cyber Security in 2018 to fund and promote ambitious research and development projects with high innovation potential in the area of digital security. Inspired by the Defense Advanced Research Projects Agency in the United States, the German agency was created under the leadership of the interior and defence ministries. It focuses on technologies for both civilian and defence uses to increase the country's independence in this area (BMI, 2020[59]). In addition, the German government has been funding Self-determined and Secure in the Digital World 2015-2020, a research programme on digital security involving the private sector.

France released a Cyber Campus Report in 2020, outlining plans for a centre for digital security and trust in France and in Europe (Van Den Berghe, 2020[60]). The Cyber Campus will aim to provide a multi-stakeholder platform to facilitate digital security innovation. It will involve actors from academia, the private sector, the government and start-ups. The digital security ecosystem campus, expected to open in 2021, is being developed with France's national digital security agency (Agence nationale de la sécurité des systèmes d'information).

In 2016, the European Union created the European Cyber Security Organisation (ECSO), a public-private partnership that co-ordinates EU innovation roadmaps and investments. It brings many different voices into the discussion: academia, industry, SMEs and member states (ECSO, n.d.[61]). ECSO helps identify priorities at European level, building on European strengths and focusing on European issues and impacts. It prioritises investments across many technical areas, such as AI, quantum computing and blockchain, as well as non-technical areas such as SMEs, women in cyber and youth in cyber.

An effective and comprehensive ecosystem is required to support digital security innovation. However, it can take time to build, particularly with technological development and disruptive technologies rising at exponential speed. Several ingredients make a successful digital security ecosystem: human capital, venture capital, strong linkages between key stakeholders and a supportive regulatory environment.

In most of these initiatives, the government plays a key role in establishing the ecosystems and ensuring co-ordination among the various stakeholders. Government can also support innovation by addressing the growing shortage of digital security professionals. For example, Canada promotes talent development by teaching programming and digital skills to children from a young age. This is part of its initiative to connect these students to industry (Public Safety Canada, 2018[62]).

Government can also promote sustainable linkages between academia, industry, government itself, entrepreneurs and financial actors. Regular communication between different stakeholders is key for the success of a digital security innovation ecosystem. This is especially true for communication that

delves deeply into an issue to find problems that need solving. In that respect, physical proximity is important, even in an age of online connectivity. Moreover, co-operation is crucial, not just within ecosystems but also between them. Ecosystems can work together to reduce national, regional and global risk. Global EPIC (Box 7.2) is an initiative to connect such ecosystems together across borders.

Box 7.2. Global EPIC, an international initiative to co-ordinate digital security innovation ecosystems

The Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC) promotes co-operation between digital security ecosystems across the world. What began with leaders of ecosystems coming together to discuss best practices today has over 27 members from 15 different countries and 3 continents. Its members' ecosystems were formed through academia, local government, industry hubs and sometimes a combination of the three. Through the organisation, ecosystem leaders can compare one another's frameworks and figure out what ideas are worth taking to their own ecosystems. The Global EPIC Soft-Landing Program is a means to strengthen ties between the ecosystems. It offers companies and entrepreneurs an opportunity to "soft land" in one of the Global EPIC ecosystems, providing a low-risk trial to companies and entrepreneurs entering a new international market. This allows them to access the resources needed to tap into commercial opportunities more readily.

Source: Global EPIC (n.d.[63]), *Global EPIC*, *https://globalepic.org/* (accessed on 6 April 2020).

Initiatives to improve digital security of products and better manage vulnerabilities

All products that contain code are vulnerable, to some extent

With the digital transformation, more and more products contain code and can interconnect. Any product that contains code also contains vulnerabilities. According to estimates, there are between 20 and 100 flaws in every 2 000 lines of code (Dean, 2018[64]). This can come down to one flaw in every 2 000 lines if "security-by-design" guidelines are followed (DCMS, 2018[65]). To put things in perspective, an average iPhone app has around 50 000 lines of code. Meanwhile, Android has around 12 million lines and Windows 10 counts more than 50 million. On average, 46 vulnerabilities were discovered and publicly disclosed every day on the United States' National Vulnerability Database in 2018 and 2019, including for widely used products such as Android, iOS or Windows (NIST, 2020[66]).

However, all vulnerabilities are not critical. According to an automatic analysis of 1.4 million software applications, 85% contain at least one vulnerability, but it is critical in only 13% of cases (Veracode, 2019[67]). Similarly, not all vulnerabilities are easily exploitable. For some, exploitation requires physical presence and human interaction, while others can be exploited remotely.

Several high-profile attacks have highlighted significant gaps in the digital security of products. They showed the damages that can result from the exploitation of critical vulnerabilities if these are not timely and appropriately mitigated.

In 2016, the Mirai malware enrolled millions of connected devices, from routers to security cameras and printers, into a botnet. The botnet was then used to launch massive DDoS attacks. This affected actors of the Internet infrastructure such as Domain Name System service provider Dyn and cloud provider OVH. Mirai leveraged the lack of basic features of many IoT products, which often let users keep weak and factory default passwords.

In 2017, WannaCry and NotPetya affected thousands of organisations in OECD countries, including Renault, Honda, Boeing, Merck, Maersk and the United Kingdom's National Health Service. Total costs amounted to several billion euros. Both malwares leveraged vulnerabilities in Windows operating systems. For the products it still supported at the time, Microsoft provided a patch fixing the vulnerability several weeks before the attack began. This, however, did not stop the global spread of the virus. In fact, many organisations did not deploy the security update in a timely manner, leaving their information systems vulnerable.

In other cases, the organisations that fell victim to WannaCry were using an operating system (e.g. Windows XP) that had reached its "end of life" (i.e. the end of commercial support). For these products, no security updates were available before the attack. Facing considerable pressure from public opinion, the company considered it had a responsibility to protect the thousands of organisations left vulnerable to the malware. Therefore, the day after the WannaCry attack began, Microsoft provided an emergency update for products it no longer supported.

The decision was controversial. Some experts believed it could give end-users added incentive to continue using products after the end of commercial support. Others consider the source code of products that have reached their end of life should be released to the public, allowing the community of users to maintain it.

WannaCry highlighted the considerable gap between the end of commercial support and when users actually stop using their systems. The gap leaves many products vulnerable since security updates are no longer available. While the effects of this gap have mostly affected the software industry to date, they will also be significant for IoT products in years to come.

A market failure prevents optimal outcomes to emerge

Across the product ecosystem, stakeholders' incentives to take responsibility for the digital security of products are often misaligned. Digital security features are often at odds with other factors such as usability and price, which consumers may value more. In innovative and emerging markets such as the IoT, producers typically value time-to-market and cost reduction over digital security. Following security-by-design and by-default guidelines requires resources, including time, talent and money. Smaller or less digitally mature companies may lack these funds or be unwilling to invest in digital security. In more mature markets such as computers or smartphones, producers are likely to shorten their products' lifecycle and accelerate their "end of life". This allows them to focus resources on developing new products rather than maintaining those that have been on the market for a few years already.

The Mirai malware highlighted significant information asymmetries and negative externalities in the IoT market. In the absence of clear information (e.g. labels), customers often struggle to assess the level of digital security of purchased products. In the long term, this may lead to adverse selection. Producers who invest in digital security, unable to differentiate their products from competitors, might exit the market. The case of DDoS attacks also illustrates the impact of negative externalities. Product owners are often unaware their devices are enrolled in a botnet, and do not bear the costs of the attacks.

These elements typically lead to a market failure, which could explain why many products have a suboptimal level of digital security.

Stakeholders are taking steps to address product-related challenges

Several industry players have established multi-stakeholder coalitions to address gaps in digital security.

The Charter of Trust, launched in 2018, gathers companies with different roles along the value chain. They aim to create a reliable foundation for trust in the digital environment on the basis of ten shared principles. These companies include Airbus, Allianz, Dell, IBM, Mitsubishi Heavy Industry, SGS, Siemens, Total and TÜV SÜD.

In parallel, 120 ICT sector companies such as ARM, Cap Gemini, Cisco, Cloudfare, HP, Hitachi, Microsoft, Salesforce and Telefónica joined the Cybersecurity Tech Accord to partner on initiatives that improve the security, stability and resilience of cyberspace. Lastly, supporters of the Paris Call for Trust and Security in Cyberspace launched by France at the 2018 Internet Governance Forum agreed to strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.

In OECD countries, governments increasingly recognise the need to improve product transparency to reduce information asymmetries. Some governments have encouraged voluntary labelling to help consumers choose products with a higher level of digital security. At the same time, the labels aim to incentivise manufacturers and designers to follow industry best practices.

Finland, Japan and Germany have all begun to promote labels. In November 2019, the Finnish government partnered with industry to launch an IoT security label. The German government also plans to launch a

labelling scheme in 2020 for routers. In other countries, governments are considering the generalisation of product certifications to reduce information asymmetries. In Japan, the Connected Consumer Device Security Council (CCDS), a business association to improve the security of consumer devices including IoT devices, started a voluntary labelling program for IoT devices in October 2019.

Facilitating multi-stakeholder partnerships is also an important tool for governments in countries such as the United States and the Netherlands.

In the United States, the National Telecommunications and Information Administration (NTIA) holds multi-stakeholder discussions to encourage software developers to provide a "software bill of materials". This is similar to a list of ingredients that would indicate the code components of a product.

The Dutch government has launched a multi-stakeholder initiative to monitor and enhance the digital security of connected devices. The initiative enables information sharing between stakeholders, including manufacturers/vendors and end-users. In this way, distributors can consider removing products from the shelves. For their part, consumers can be incentivised to patch or deactivate their products if critical vulnerabilities are discovered. The partnership involves actors such as the University of Delft, the Dutch Ministry of Economic Affairs and a non-profit association of Dutch ISPs.

Other governments in the OECD have funded and/or facilitated the development of multi-stakeholder partnerships to tackle the issue of botnet. These include *botfrei* in Germany and the National Operation Towards IoT Clean Environment in Japan. At the European level, the Cybersecurity Act (Regulation (EU) 2019/881) is a key EU initiative to improve the digital security of ICT products, services and processes by creating a voluntary cybersecurity certification framework.

Finally, some governments are willing to go beyond voluntary frameworks. They recognise a suboptimal level of digital security in many products would pose significant risks to consumers, SMEs and the economy more broadly. These governments are mandating basic security features for all IoT products through regulatory requirements.

Both the United Kingdom and Japan have gone beyond voluntary frameworks. In the United Kingdom, the government plans to mandate manufacturers and vendors to implement the first three principles of the government's guidelines for IoT security. These guidelines, developed in 2018, are "no default passwords", "updatability" and "vulnerability disclosure policy". In Japan, the regulator has also imposed regulatory requirements. Since April 2020, IoT products connected directly to the networks of telecommunications operators in Japan are required to incorporate certain basic functions (e.g. a firmware update mechanism, access control and incentives for users to change default passwords and IDs).

Responsible vulnerability management and disclosure is receiving increased policy attention

Every piece of software has undiscovered or latent vulnerabilities. Threat actors, such as criminals and other ill-intentioned players, are eager to discover those vulnerabilities through exploiting them through malware. Therefore, discovering vulnerabilities, fixing them and reducing their overall number is equally important for digital security risk mitigation as tackling threats (i.e. arresting cybercriminals). Both approaches are necessary and complementary.

Vulnerabilities can affect the code of a product. When a vendor becomes aware of a vulnerability in its product's code, it can develop a patch (or fix) that modifies this code. It can then distribute the patch to users through security updates. However, product users remain potentially vulnerable to an incident exploiting the vulnerability until they apply the patch, either automatically or manually.

Vulnerabilities can also be specific to the way a user implements the product, such as its configuration and settings. For example, if a user sets a weak password in equipment, it creates a vulnerability that can be exploited. An important number of such vulnerabilities are also found where users do not use patches to fix their products' vulnerabilities. In 2018, according to one security product vendor, 81% of systems had at least one known vulnerability, 72% had more than one and 20% of systems had more than ten (Edgescan, 2019[68]).

Malicious actors are actively searching for both types of vulnerabilities. Product vulnerabilities for which no patch or mitigation technique is available are called "zero-days". Attacks leveraging zero-

days are significantly more likely to succeed because they are more difficult to detect and mitigate. Since zero-days are rare and highly effective, they have a high value for attackers. They use them only against targets worth the risk of detection; once the vulnerability is discovered, it spoils the possibility of future attacks. Attackers generally prefer to exploit known product vulnerabilities for which a patch may be available but not implemented by users.

Therefore, both vendors and users share a responsibility to mitigate vulnerabilities. However, they also face obstacles. For example, vendors can view the discovery of vulnerabilities, as well as developing and distributing patches, as less profitable than developing new features. For some organisations, patch management is costly, complex and risky. It can potentially destabilise their information systems by introducing new code that has not been sufficiently tested in their environment.

Fortunately, a large community of security researchers, often called "white hats" or "ethical hackers", are also hunting vulnerabilities and eager to disclose them to help reduce digital security risk. Security researchers can significantly contribute to increasing digital security of products. According to a 2016 survey in the United States, the vast majority of researchers (92%) generally engage in some form of co-ordinated vulnerability disclosure (NTIA, 2016[69]). This represents a huge potential resource for vendors.

Although many white hats hunt vulnerabilities as a hobby or for the common good, many others do it as part of their professional security work. They can belong to the private sector or civil society. The survey shows that most researchers are interested in receiving some sort of reward. These range from simple acknowledgements, to the possibility of communicating about it publicly (e.g. in conferences, academic publications, etc.), to financial retribution and, possibly, job offers (NTIA, 2016[69]).

However, vulnerability disclosure can become counterproductive if not carried out appropriately. If security researchers publicly disclose a vulnerability, malicious actors can exploit it for offensive purposes. If patches are not yet ready, or products are not yet patched on the users' side, attacks are most likely to be successful. Furthermore, researchers may offer vulnerabilities on the black market rather than disclosing them to vendors in view of being fixed. This enables actors to purchase and operationalise them for offensive purposes, increasing digital security risk for all legitimate actors.

Product vendors can also fail to handle a vulnerability reported to them by a security researcher. The researcher may then consider public disclosure to put pressure on the vendor to fix the vulnerability. For example, a security researcher reported a serious vulnerability in the Myspace website in 2017. The vulnerability allowed an attacker to log in to any one of the 3.6 million Myspace active users' accounts in a few easy steps. After three months of inaction from the company, the researcher publicly disclosed the vulnerability in a blog post. The vulnerability was fixed within a few hours. The company never got back to the researcher (Spring, 2018[70]). A 2019 report shows that 93% of the Forbes Global 2000 do not offer a means for contacting them to disclose a critical vulnerability (HackerOne, 2019[71]).

Through co-ordinated vulnerability disclosure (CVD), product vendors and users, as well as security researchers, work co-operatively to find solutions that reduce the risk associated with a vulnerability. CVD aims for public disclosure of a vulnerability only after mitigations are available to end-users to reduce their window of exposure. CVD is widely recognised as a good practice to ensure that researchers and vendors act in a responsible manner for vulnerability disclosure. It is detailed in international standards such as ISO/IEC 29147 and 30111.

Unfortunately, there are obstacles to broad adoption of CVD. Many policy makers are not yet sufficiently aware of the need to remove such obstacles and encourage responsible behaviour by all stakeholders. For example, discovering vulnerabilities can expose researchers to legal risks and threats of proceedings by vendors; they have been accused of breaching terms of services, or having committed a cybercrime. There are numerous cases of vendors or service providers threatening researchers with legal proceedings after they have reported a vulnerability instead of co-operating with them to fix it as soon as possible.

In the above-mentioned survey, 60% of researchers cited the threat of legal action as a reason they might not work with a vendor to disclose a vulnerability (NTIA, 2016[69]). In 2016, for example, researchers at a US security company reported a serious vulnerability to one of the largest global consulting and auditing companies. Three days later they received a cease-and-desist letter (Whittaker, 2018[72]). In another case, a researcher reported a dental software company in the United States had left unencrypted

sensitive health information of 22 000 patients at risk of access by others. The US Federal Bureau of Investigation raided the researcher's home and arrested him (Doe, 2016[73]).

A number of policy initiatives are encouraging the adoption of CVD. The Dutch National Cybersecurity Centre (NCSC-NL, 2018[74]), for example, adopted CVD guidelines. In addition, both the United States NIST Cybersecurity Framework (version 1.1) and the European Union Cybersecurity Act (European Union, 2019[75]) have included CVD guidelines.

At the time of writing, the United States Department of Homeland Security was also developing a binding operational directive. It would require each federal government agency to develop and publish a vulnerability disclosure policy and maintain supporting procedure (DHS, 2019[76]). The OECD also recommends operators of critical activities adopt such a policy (OECD, 2019[77]) (Box 7.3).

Box 7.3. The OECD *Recommendation of the Council on Digital Security of Critical Activities*

Adopted in December 2019, the OECD *Recommendation of the Council on Digital Security of Critical Activities* sets out a range of policy recommendations. They aim to ensure that policies targeting operators of critical activities focus on what is critical for the economy and society without imposing unnecessary burdens on the rest. These recommendations support adherents in:

- adapting their overarching policy framework
- ensuring that operators reduce the digital security risk to critical functions to a level acceptable for society in an effective manner
- promoting and building trust-based partnerships
- improving co-operation at the international level.

The Recommendation also clarifies how this public policy area relates to broader national risk management/critical infrastructure protection policy.

Source: OECD (2019[77]), *Recommendation of the Council on Digital Security of Critical Activities*, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456*.

Digital security and artificial intelligence

An AI system is defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments (OECD, 2019[78]). According to security expert Bruce Schneier, "there is no doubt that AI will transform digital security. We just don't know how and when" (Schneier, 8 January 2019[79]).

Some elements confirm that we may be on the verge of a transformation in digital security through AI. However, it is still difficult to distinguish facts from marketing-driven speculations, and assess where the industry stands on the hype cycle. It seems too early to presume that AI has created a paradigm shift in digital security. Such a transformation may take place step-by-step rather than through a single brutal and radical change. Nevertheless, if AI is to transform digital security, it will likely do so by both supporting and challenging it.

AI can help improve digital security

There can be many benefits to the use of AI to protect information systems. For example, AI-enabled digital security systems can be trained to identify behaviour of malware before entering IT systems. It can also be taught to detect such malware before they inflict damages. In that respect, these systems can be faster than traditional approaches and research on AI for digital security is becoming an important trend.

In addition to helping manage the increasing volume of vulnerabilities, AI can assist stretched and overworked digital security teams. This is especially useful given the shortage of skilled digital security professionals. AI can automate basic digital security tasks such as identifying the nature, source and

intent of attacks and monitoring of high volumes of security data. In this way, security teams can devote more time to more sophisticated threats. Automation can also decrease the likelihood of human errors and negligence occurring.

Despite the efficacy of AI and automation in helping understaffed digital security teams, highly skilled employees will still be required for high-level analysis. For example, AI can help detect anomalous behaviours in a system. This may reveal the presence of a sophisticated intruder that a classic security system or a trained human would not otherwise notice. However, humans will still be needed to eliminate false positives. They will also need to determine the appropriate response to detected sophisticated attacks. In addition, AI's abstract and highly dimensional nature may make it unclear why or how something was detected. For this reason as well, human oversight is important (National Academies of Sciences, Engineering, and Medicine, 2019[80]).

Digital security efforts by governments can benefit from using AI. For example, since 2018, the Korean Ministry of Science and ICT (MSIT) has been establishing an AI-based cyber incident response system. MSIT applies AI to systems such as detection, analysis and information sharing to help humans respond to security alerts and incidents.

According to some experts, the deployment of AI-powered security applications can reduce costs. In a survey of 850 IT executives, covering 7 sectors and 10 countries, 64% said that AI lowers the cost to detect and respond to breaches. This, in turn, reduces the overall time taken to detect threats and breaches by 12%, on average (Capgemini Research Institute, 2019[81]). Almost two in three security executives said they are planning to employ AI by 2020, compared to one in five organisations pre-2019. This indicates that AI in security is rapidly becoming more widespread. Meanwhile, 69% of organisations said that employing AI is necessary to respond to digital security attacks. A Ponemon Institute survey sponsored by IBM found that AI significantly reduced the time and cost of dealing with digital security threats. It indicated that deploying AI could save more than USD 2.5 million in operating costs (Ponemon Institute, 2018[82]). These surveys, however, are sponsored by companies with a vested interest in deploying AI solutions or renewing the market for IT security products.

AI can also help develop code with fewer vulnerabilities. Computer code is prone to human error; many digital security attacks result from flaws in software code. Given the billions of lines of code written every year and the re-use of third-party proprietary libraries, detecting and correcting errors in software code is a daunting task for the human eye.

Some research projects use AI systems to prevent or detect software security vulnerabilities. Mozilla, for example, uses an AI coding assistant developed by Ubisoft, the gaming company. It aims to make the Firefox code-writing process more efficient and prevent introduction of bugs (Zorz, 2019[83]).

AI techniques related to products' digital security vulnerabilities can be grouped in three categories: detection, repair and specification analysis. While AI techniques have become quite useful in this area, researchers have found they still tend to be limited in scope. As a result, they provide a collection of tools that can augment, but not replace, careful system development to reduce vulnerability risks (Kommrusch, 2018[84]).

AI can also create new digital security challenges

Notwithstanding the benefits of AI for digital security, the technology also introduces new risks. Like many tools, AI can be weaponised in various ways. In that sense, it can be viewed as a double-edged sword.

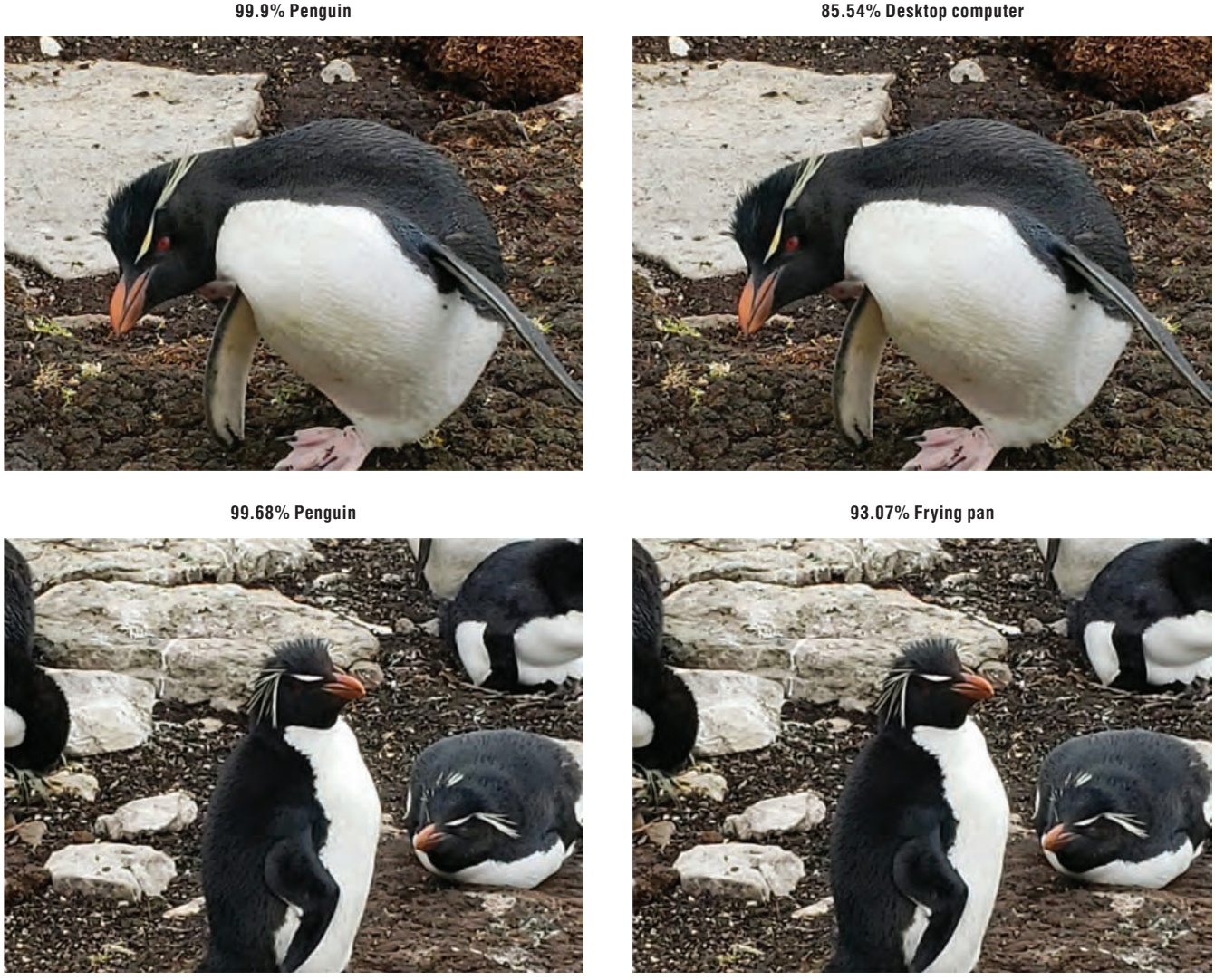
AI-powered security techniques are not perfect and sophisticated attackers can bypass them. Researchers assessed machine and deep learning approaches to problems in digital security, such as intrusion detection, malware analysis and spam detection. They found that, while these techniques support security, each approach was vulnerable to adversarial attacks (Apruzzese et al., 2018[85]). In addition, attackers can also use AI technologies meant to identify and fix vulnerabilities in software to hunt for new vulnerabilities. They then exploit these gaps to attack information systems.

Digital security incidents can affect all information systems, including those relying on AI. However, AI systems may also be vulnerable to new types of attack techniques that leverage the specificity of AI. For example, machine learning relies on data for its system to train itself.

Data poisoning, adversarial input and model attack – which involve the inputting of bad data points – can harm an AI-enabled system. It can either render it defunct or merely disrupt its learning process, forcing it to give a wrong output. In the latter case, the results could be severe depending on the activity supported by the AI system. For example, supply chains reliant on AI could cause the drastic undersupply of a product. Moreover, the algorithm might otherwise appear to be working, leaving the attack undetected.

Figure 7.6 shows an example of adversarial input. A small perturbation, carefully calculated and invisible to the human eye, is added in an image of a penguin. This would enable an attacker to make an AI system recognise the image with high confidence as a desktop computer or frying pan. Many researchers have explored how to attack a physical system using such techniques. For example, McAfee researchers discovered the impact of minuscule modifications to speed limit signs. These subtle changes could allow an attacker to influence the autonomous driving features of the vehicle, controlling the speed of the adaptive cruise control (Povolny and Fralick, 19 February 2020[86]).

Figure 7.6. Example of a fooled AI system using adversarial input



Note: The penguin is detected as a desktop computer (85.54%) or a frying pan (93.07%) following pixel perturbations in each image that are invisible to the human eye.

Source: Povolny and Fralick (19 February 2020[86]), "Introduction and application of model hacking", *https://www.mcafee.com/blogs/other-blogs/mcafee-labs/introduction-and-application-of-model-hacking/*.

AI-powered deep fakes can be generated using a sample of data based on machine learning. For example, a malicious actor could mine information about someone on the Internet through social media to generate email messages for phishing attacks that are difficult to detect (National Academies of Sciences, Engineering, and Medicine, 2019[80]). LyreBird is a company that uses AI to generate fake audio of an individual using sample recordings (WIRED, 2018[87]). Malicious actors could use such technologies to support social engineering techniques, deceiving employees into providing their credentials to attackers or transferring money into the bank account of someone pretending to be their boss. This practice, carried out mostly by email, is called "business email compromise" (BEC). The total known worldwide losses to BEC scams hit USD 12.5 billion between October 2013 and May 2018, with a total number of known victims reaching 78 617 (FBI, 2018[88]). AI could significantly increase this dangerous trend.

The use of AI for digital security can raise costs for adversaries, forcing them to find more sophisticated techniques that might be more susceptible to discovery (National Academies of Sciences, Engineering, and Medicine, 2019[80]). Adversaries are not yet using much AI, primarily because other cheaper techniques continue to be effective (National Academies of Sciences, Engineering, and Medicine, 2019[80]). As the cost of AI drops, it is likely that malicious actors will increasingly leverage AI to enhance their attack potential, starting with sophisticated cybercrime and state-sponsored groups. The outcome of both defenders and attackers using AI techniques is not yet clear. However, it may accelerate the digital security arms race between malicious and legitimate actors.

References

ANSSI and BSI (2018), *ANSSI/BSI Common Situational Picture, Vol. 1*, Agence nationale de la sécurité des systèmes d'information, Paris and Bundesamt für Sicherheit in der Informationstechnik, Bonn, *https://www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf*. [12]

Apruzzese, G. et al. (2018), "On the effectiveness of machine and deep learning for cyber security", *2018 10th International Conference on Cyber Conflict (CyCon)*, *http://dx.doi.org/10.23919/cycon.2018.8405026*. [85]

AustCyber (n.d.), *AustCyber*, website, *https://www.austcyber.com/* (accessed on 21 October 2020). [56]

Avanan (2019), *Global Phish Report*, Avanan, New York, *https://www.avanan.com/hubfs/2019-Global-Phish-Report.pdf*. [7]

Beedham, M. (2019), "Ethereum Classic hackers steal over $1.1M with 51% attacks", The Next Web, 8 January, *https://thenextweb.com/hardfork/2019/01/08/ehtereum-classic-51-percent-attack/*. [40]

BMI (2020), "Agentur für Innovation in der Cybersicherheit" ["Agency for Innovation in Cybersecurity"], Bundesministerium des Innern, für Bau und Heimat, Berlin, 29 August, *https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/08/cyberagentur.html*. [59]

Canellis, D. (2018), "Major cryptocurrency exchange delists Bitcoin Gold following $18M hack", The Next Web, 3 September, *https://thenextweb.com/hardfork/2018/09/03/bittrex-delists-bitcoin-gold/*. [39]

Capgemini Research Institute (2019), *Reinventing Cybersecurity with Artificial Intelligence*, Capgemini Research Institute, Paris, *https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf*. [81]

Charter of Trust (n.d.), *Charter of Trust*, website, *https://www.charteroftrust.com/* (accessed on 31 March 2020). [52]

Chokshi, N. (2019), "Hackers are holding Baltimore hostage: How they struck and what's next", *The New York Times*, 22 May, *https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html*. [29]

Cimpanu, C. (2020), "IOTA cryptocurrency shuts down entire network after wallet hack", ZDNet, 16 February, *https://www.zdnet.com/article/iota-cryptocurrency-shuts-down-entire-network-after-wallet-hack/*. [38]

Cimpanu, C. (2019), "Bithumb cryptocurrency exchange hacked a third time in two years", ZDNet, 30 March, *https://www.zdnet.com/article/bithumb-cryptocurrency-exchange-hacked-a-third-time-in-two-years/*. [36]

Cimpanu, C. (2018), "Ransomware attack blacks out screens at Bristol Airport", ZDNet, 16 September, *https://www.zdnet.com/article/ransomware-attack-blacks-out-screens-at-bristol-airport/*. [17]

CISA (2020), "Alert (AA20-049A) Ransomware impacting pipeline operations", webpage, *https://www.us-cert.gov/ncas/alerts/aa20-049a* (accessed on 21 October 2020). [34]

CISA (2018), "Alert (TA18-201A) Emotet malware", webpage, *https://www.us-cert.gov/ncas/alerts/TA18-201A* (accessed on 21 October 2020). [46]

CISO MAG (2019), *7 Times Ransomware Became a Major Healthcare Hazard*, CISO MAG, *https://www.cisomag.com/7-times-ransomware-became-a-major-healthcare-hazard/* (accessed on 21 October 2020). [22]

Crane, C. (2019), "Polymorphic malware and metamorphic malware: What you need to know", The SSL Store hashed out blog, 21 May, *https://www.thesslstore.com/blog/polymorphic-malware-and-metamorphic-malware-what-you-need-to-know/*. [45]

Cybersecurity Tech Accord (n.d.), *Cybersecurity Tech Accord*, website, *https://cybertechaccord.org/* (accessed on 21 October 2020). [53]

CyberSpark (n.d.), *CyberSpark*, website, *http://cyberspark.org.il/* (accessed on 31 March 2020). [54]

DARK Reading (2020), "NRC health ransomware attack prompts patient data concerns", *DARK Reading*, 21 February, *https://www.darkreading.com/attacks-breaches/nrc-health-ransomware-attack-prompts-patient-data-concerns/d/d-id/1337116*. [24]

DCMS (2018), "Guidance data ethics framework", webpage, *http://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework* (accessed on 21 October 2020). [65]

Dean, B. (2018), *Strict Products Liability and the Internet of Things*, Center for Democracy and Technology, Washington, DC, *https://cdt.org/wp-content/uploads/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf*. [64]

DHS (2019), *Draft Binding Operational Directive 20-01 – Develop and Publish a Vulnerability Disclosure Policy*, Cybersecurity and Infrastructure Security Agency, Washington, DC, 27 November, *https://cyber.dhs.gov/bod/20-01/* (accessed on 21 October 2020). [76]

Doe, D. (2016), "FBI raids dental software researcher who discovered private patient data on public server", The Daily Dot, 29 February, *https://www.dailydot.com/layer8/justin-shafer-fbi-raid/*. [73]

ECSO (n.d.), "ECSO Cybersecurity Response Package", webpage, *https://ecs-org.eu/* (accessed on 21 October 2020). [61]

Eddy, N. (2020), "Ransomware attacks in 2019 forced some health systems to pay up", Healthcare IT News, 2 January, *https://www.healthcareitnews.com/news/ransomware-attacks-2019-forced-some-health-systems-pay*. [21]

Edgescan (2019), *2019 Vulnerability Statistics Report*, Edgescan, Dublin, *https://www.edgescan.com/wp-content/uploads/2019/02/edgescan-Vulnerability-Stats-Report-2019.pdf*. [68]

European Union (2019), *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, *https://eur-lex.europa.eu/eli/reg/2019/881/oj* (accessed on 21 October l 2020). [75]

Eurostat (2019), *Digital Economy and Society Statistics*, Comprehensive Database. [4]

FBI (2018), "Business e-mail compromise the 12 billion dollar scam", Public Service Announcement, Federal Bureau of Investigation, Washington, DC, 12 July, *https://www.ic3.gov/media/2018/180712.aspx*. [88]

Gallagher, S. (2019), "Louisiana was hit by Ryuk, triggering another cyber-emergency", Ars Technica, 21 November, *https://arstechnica.com/information-technology/2019/11/louisiana-was-hit-by-ryuk-triggering-another-cyber-emergency/*. [31]

Garrity, M. (2019), "15 notable ransomware attacks on healthcare providers in 2019", Becker's Health IT, 18 December, *https://www.beckershospitalreview.com/cybersecurity/15-notable-ransomware-attacks-on-healthcare-providers-in-2019.html* (accessed on 21 October 2020). [23]

Global EPIC (n.d.), *Global EPIC*, website, *https://globalepic.org/* (accessed on 21 October 2020). [63]

Goodin, D. (2019), "Johannesburg's network shut down after second attack in 3 months", Ars Technica, 25 October, *https://arstechnica.com/information-technology/2019/10/johannesburgs-network-shut-down-after-second-attack-in-3-months/*. [32]

Google (2020), "Safe Browsing", webpage, *https://transparencyreport.google.com/safe-browsing/overview?unsafe=dataset:1;series:malwareDetected,phishingDetected;start:978220800000;end:1581840000000&lu=unsafe* (accessed on 21 October 2020). [9]

Goud, N. (n.d.), "Ransomware attack on Cleveland Hopkins International Airport", Cybersecurity Insiders, *https://www.cybersecurity-insiders.com/ransomware-attack-on-cleveland-hopkins-international-airport/* (accessed on 21 October 2020). [19]

Greenberg, A. (2018), "The untold story of NotPetya, the most devastating cyberattack in history", WIRED, 22 September, *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*. [13]

HackerOne (2019), *The Hacker-Powered Security Report 2019*, HackerOne, San Francisco, *https://www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019*. [71]

Héritier, C. (2019), "Protéger nos villes des cyberattaques", *Les Echos*, 25 October, *https://www.lesechos.fr/idees-debats/cercle/opinion-proteger-nos-villes-des-cyberattaques-1143037*. [28]

ICE71 (n.d.), *ICE71*, website, *https://ice71.sg/* (accessed on 21 October 2020). [58]

Insurance Journal (2020), "Christmas ransomware attack hit New York airport servers", *Insurance Journal*, 15 January. [20]

Israel Ministry of Foreign Affairs (2015), "Cabinet approves benefits for National Cyber Park in Be'er Sheva", Government of Israel, Jerusalem, 6 September, *https://mfa.gov.il/MFA/InnovativeIsrael/Economy/Pages/Cabinet-approves-benefits-for-National-Cyber-Park-in-Beer-Sheva-6-Sep-2015.aspx*. [55]

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 21 October 2020). [25]

Kommrusch, S. (2018), "Artificial intelligence techniques for security vulnerability prevention", ArXiv.org, 14 December, *https://arxiv.org/pdf/1912.06796.pdf*. [84]

Korosec, K. (2019), "New Orleans declares state of emergency following ransomware attack", Tech Crunch, 14 December, *https://techcrunch.com/2019/12/14/new-orleans-declares-state-of-emergency-following-ransomware-attack/*. [30]

Liska, A. (2019), *Early Findings: Review of State and Local Government Ransomware Attacks*, Recorded Future, Boston, Massachusetts, *http://www.recordedfuture.com*. [33]

LORCA (n.d.), *LORCA*, website, *https://www.lorca.co.uk/* (accessed on 21 October 2020). [57]

Malwarebytes Labs (2020), *2020 State of Malware Report*, Malwarebytes Labs, Santa Clara, California, *https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf*. [42]

McKay, T. (2019), "Florida City fires IT employee after paying $460,000 bitcoin ransom to hackers", Gizmodo, 1 July, *https://gizmodo.com/florida-city-fires-it-employee-after-paying-460-000-in-1836031022* (accessed on 21 October 2020). [49]

National Academies of Sciences, Engineering, and Medicine (2019), *Implications of Artificial Intelligence for Cybersecurity*, National Academies Press, Washington, DC, *http://dx.doi.org/10.17226/25488*. [80]

NCSC-NL (2018), *Coordinated Vulnerability Disclosure: The Guideline*, National Cyber Security Centre, Ministry of Justice and Security, The Hague, *https://english.ncsc.nl/binaries/ncsc-en/documents/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline/WEB_Brochure-NCSC_EN.pdf*. [74]

Netscout (2020), "Cloud in the crosshairs", *Netscout Threat Intelligence Report 15th Annual Worldwide Infrastructure Security Report*, Netscout, Westford, Massachusetts, *https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf#page=9&zoom=auto,-123,360*. [2]

Netscout (2019), *Worldwide Infrastructure Security Report*, Issue 4, Netscout, Westford, Massachusetts, *https://www.netscout.com/sites/default/files/2020-02/SECR_001_EN-2001_Web.pdf*. [1]

NexusGuard (2019), *Threat Report: Distributed Denial of Service (DDoS) Q3*, NexusGuard, San Francisco, *https://www.nexusguard.com/hubfs/Q3%202019%20Threat%20Report/2019Q3_Threat%20Report.pdf*. [3]

NIST (2020), *National Vulnerability Database*, (database), *https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=last3years* (accessed on 21 October 2020). [66]

NTIA (2016), *Vulnerability Disclosure Attitudes and Actions*, National Telecommunications and Information Administration, Washington, DC, *https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf*. [69]

OECD (2020), *The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage*, OECD, Paris, *http://www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf*. [51]

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/eedfee77-en*. [78]

OECD (2019), *Recommendation of the Council on Digital Security of Critical Activities*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456*. [77]

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*. [50]

Osborne, C. (2019), "Canadian Nunavut government systems crippled by ransomware", ZDNet, 5 November, *https://www.zdnet.com/article/canadian-nunavut-government-systems-crippled-by-ransomware/*. [26]

Palmer, D. (2020), "Ransomware attacks are now targeting industrial control systems", ZDNet, 4 February, *https://www.zdnet.com/article/ransomware-attacks-are-now-targeting-industrial-control-systems/*. [35]

PhishLabs (2019), *2019 Phishing Trends and Intelligence Report: The Growing Social Engineering Threat*, PhishLabs, Charleston, South Carolina, *https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf* (accessed on 21 October 2020). [8]

Ponemon Institute (2018), *The Value of Artificial Intelligence in Cybersecurity*, Ponemon Institute, Traverse City, Michigan, *https://www.themsphub.com/app/uploads/2018/09/ibm-ai-report-final-1_41017541USEN.pdf*. [82]

Povolny, S. and C. Fralick (19 February 2020), "Introduction and application of model hacking", McAfee blogs, *https://www.mcafee.com/blogs/other-blogs/mcafee-labs/introduction-and-application-of-model-hacking/*. [86]

Public Safety Canada (2018), *National Cyber Security Action Plan (2019-2024)*, Public Safety Canada, Ottawa, *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx*. [62]

RT World News (2017), "Ransomware virus plagues 100k computers across 99 countries", RT World News, 12 May, *https://www.rt.com/news/388153-thousands-ransomeware-attacks-worldwide/*. [14]

Saraogi, V. (2019), "Five times airports were involved in cyberattacks and data breaches", Airport Technology, 24 July, *https://www.airport-technology.com/features/five-times-airports-were-involved-in-cyberattacks-and-data-breaches/*. [18]

Schneier, B. (2019), "Machine learning to detect software vulnerabilities", Schneier on Security blog, 8 January, *https://www.schneier.com/blog/archives/2019/01/machine_learnin.html*. [79]

Seals, T. (2020), "U.N. weathers storm of Emotet-TrickBot malware", threatpost, 15 January, *https://threatpost.com/un-weathers-emotet-trickbot-malware/151894/*. [48]

SelfKey (2020), "A comprehensive list of cryptocurrency exchange hacks", SelfKey, 13 February, *https://selfkey.org/list-of-cryptocurrency-exchange-hacks/*. [37]

Senzee, T. (2019), "What happened in ransomware attack on Port of San Diego", San Diego Reader, 10 April, *https://www.sandiegoreader.com/news/2019/apr/10/city-lights-happened-ransomware-port-san-diego/*. [16]

Spring, T. (2018), "The vulnerability disclosure process: Still broken", threatpost, 5 September, *https://threatpost.com/the-vulnerability-disclosure-process-still-broken/137180/* (accessed on 21 October 2020). [70]

Symantec (2019), *ISTR Internet Security Threat Report Volume 24*, Symantec, Tempe, Arizona, *https://docs.broadcom.com/doc/istr-24-2019-en* (accessed on 21 October 2020). [5]

The Morning Call (2018), "City of Allentown computer systems hit by virus that will require nearly $1M fix", 20 February. [47]

Trend Micro (2019), *2019 Midyear Security Roundup: Evasive Threats, Pervasive Effects*, Trend Micro, Tokyo, *https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf* (accessed on 21 October 2020). [43]

Trustwave (2019), *Trustwave Global Security Report 2019*, Trustwave, Chicago, *http://trustwave.azureedge.net/media/16096/2019-trustwave-global-security-report.pdf* (accessed on 21 October 2020). [41]

Tsonchev, A. (2018), "Troubled waters: Cyber-attacks on San Diego and Barcelona's ports show risk of IT/OT convergence", Computing, *https://www.computing.co.uk/sponsored/3064194/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports-show-risk-of-it-ot-convergence* (accessed on 30 October 2020). [15]

Van Den Berghe, M. (2020), *Campus Cyber: Fédérer et faire rayonner l'écosystème de la cybersécurité*, Agence nationale de la sécurité des systèmes d'information, Paris, *https://www.ssi.gouv.fr/uploads/2019/10/campuscyber-rapport.pdf* (accessed on 21 October 2020). [60]

Venafi (2018), *Venafi Research Brief: The Risk Lookalike Domains Pose to Online Retailers*, Venafi, Salt Lake City, *https://www.venafi.com/sites/default/files/2018-09/Venafi-Research-Retail-Lookalike-Domains-1809.pdf* (accessed on 20 October 2020). [10]

Veracode (2019), *The State of Software Security Today Volume 9*, Veracode, Burlington, Massachusetts, *https://www.veracode.com/sites/default/files/pdf/resources/reports/state-of-software-security-volume-9-veracode-report.pdf*. [67]

Verizon (2019), "2019 Data Breaches Investigations Report", webpage, *http://veriscommunity.net/veris_webapp_min.html* (accessed on 21 October 2020). [6]

Vitard, A. (2020), "Les services administratifs du Grand Est sont paralysés par une cyberattaque depuis une semaine", L'Usine digitale, 21 February, *https://www.usine-digitale.fr/article/les-services-administratifs-du-grand-est-sont-paralyses-par-une-cyberattaque-depuis-une-semaine.N932494* (accessed on 21 October 2020). [27]

Webroot (2019), *2019 Webroot Threat Report*, Webroot, Broomfield, Colorado, *https://www-cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf* (accessed on 21 October 2020). [11]

Whittaker, Z. (2018), "Lawsuits threaten infosec research — just when we need it most", ZDNet, 19 February, *https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/* (accessed on 21 October 2020). [72]

WIRED (2018), "How Lyrebird uses AI to find Its (artificial) voice", WIRED, *https://www.wired.com/brandlab/2018/10/lyrebird-uses-ai-find-artificial-voice/* (accessed on 30 October 2020). [87]

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*. [44]

Zorz, Z. (2019), "Mozilla will use AI coding assistant to preemptively catch Firefox bugs", Help Net Security, 15 February, *https://www.helpnetsecurity.com/2019/02/15/mozilla-ubisoft-ai-coding-assistant/* (accessed on 21 October 2020). [83]

Note

1. *https://coronavirus.jhu.edu/map.html*.