Cybersecurity for Micro, Small & Medium Enterprises
www.cybermsme.eu

Mapping the cyber-threats for micro-, small and medium-sized enterprises in the EU

Collective report edited by Izabela Marcinkowska,

With contribution of country experts: CASE, Poland (Kataryna Karunska, Machteld Bergstra), CTS Customized Training Solutions Sp. z o.o. (Poland), Institut de Haute Formation aux Politiques Communautaires (Belgium), IDP SAS di Giancarlo Costantino (Italy), SC Gentlab SRL (Romania), Internet Web Solutions SL (Spain)

With the support of the Erasmus+ programme of the European Union. This document and its contents reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the
Erasmus+ Programme
of the European Union

TABLE OF CONTENTS

Executive summary

1. Introduction

Cybersecurity has emerged as one of the key topics on the global agenda amid the ever-accelerating technological transformation and rapid digital shift induced by the Covid-19 pandemic. Regardless of their size and sector, EU companies are increasingly becoming aware of the importance of cybersecurity and invest into tools and strategies to increase resilience and responsiveness to eventual cyber threats. The Covid-19 pandemic and rise of remote working have certainly contributed to the vulnerability of companies to cyber threats with a 667% spike in phishing attacks globally in the first months of the pandemic[1].

Micro-, small-, and medium-sized enterprises (MSMEs) which often lack both awareness and capacity to establish security risk management frameworks and deal with cyber threats as only 30% of SMEs report resorting to more than basic cybersecurity measures (ENISA, 2021). Low levels of awareness and commitments from management were thus identified as one of the prime factors undermining MSMEs resilience to cyber risks. Human factor is yet another structural challenge with about 84% of the cyberattacks in the EU relying on social engineering to lure people into divulging sensitive information or clicking on the link that may contain malicious files (ENISA, 2020).

Against this background, this report builds on the individual country reports (7. Annex. Country reports) and literature findings to define cybersecurity and cyber threats (section 2) and discuss current cybersecurity framework of the EU MSMEs, including main cyber threats (section 3), state of cyber awareness and preparedness of the MSMEs (section 4), as well as best practices at the policy and private levels (section 5). The last section of the report further elaborates policy recommendations to improve state cybersecurity of the EU MSMEs, while country-level policy recommendations are presented in the individual country reports.

2. The definition of cybersecurity and cyber-threats

Various definitions of cybersecurity can be found in dictionaries or in the use by organisations dealing with issues relating to the topic, such as NATO, CNSS and ITU. In 2016, ENISA published a report named ‘Definition of Cybersecurity, Gaps and overlaps in standardisation’[2], which aims to describe these diverging understandings in more detail and provide a guide for determining an appropriate understanding of the term ‘Cybersecurity’ to be used in the context of the intended use of the stakeholders and policy makers. ENISA mentions that cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers. Therefore, a contextual definition, based on one that is relevant, fits, and is already used by a particular organisation should be considered. Stakeholders and policymakers should, according to ENISA, consider the definitions as explained and choose the most appropriate considering their requirements. By

[1] Grandi, A. P., Sarri, A., Paggio, V. *What Europe’s SMEs need to do for a cyber-secure future*. World Economic Forum. 28 June 2021. Available at: https://www.weforum.org/agenda/2021/06/cybersecurity-for-smes-europe/.

[2] See more: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

referencing a specific definition clarity can be maintained. This report offers a few optional definitions that may be used in this project, being:

a) Terminology as defined by dictionaries

The Oxford Dictionaries – Online defines ‘cybersecurity’ as: The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. Merriam Webster defines ‘cybersecurity’ as: Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

b) Terminology as defined by organizations

ENISA: Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.

ITU (International Telecommunications Union): Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment. The general security objectives comprise the following aspects: availability, integrity - which may include authenticity and non-repudiation-, and confidentiality.

For this report, the following definition will be used, referencing the definition created by the ITU (International Telecommunications Union):

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

By contrast, cyber threat is *any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service*[3].

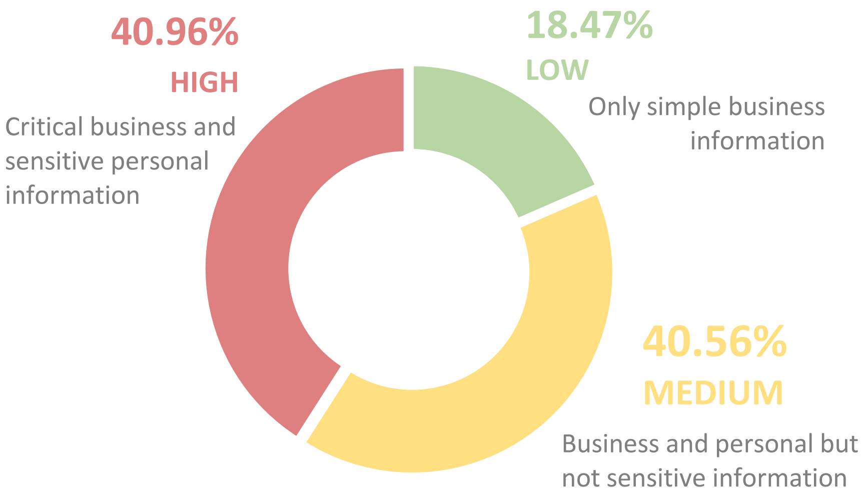
3. MSMEs’ cyber-threats framework

Being perceived as one of the main short-term global risks (World Economic Forum, 2021), breach of cybersecurity becomes a constant threat to most of the enterprises regardless of their size or sector. Despite being relatively less digitally intensive, MSMEs become increasingly exposed to the cybersecurity risks amid the accelerated digital transformation induced by the Covid-19 crisis (OECD,

[3] ENISA. Glossary. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.

2021). Thus, 8% of the respondents to the 2021 SMEs survey conducted by the European Union Agency for Cybersecurity (ENISA) reported having suffered from cybersecurity incidents in the aftermath of the Covid-19 pandemic. This represents a relatively high increase considering the short time frame and that the share of the respondents reporting experience of incidents in the last 5 years stood at 36% only (ENISA, 2021). Besides the increased dependency on information services, it is the processing of sensitive information (see Figure 1) through digital channels that makes MSMEs a likely target of the cyber-attacks.

Figure 1. Criticality and sensitivity of processed information as perceived by SMEs



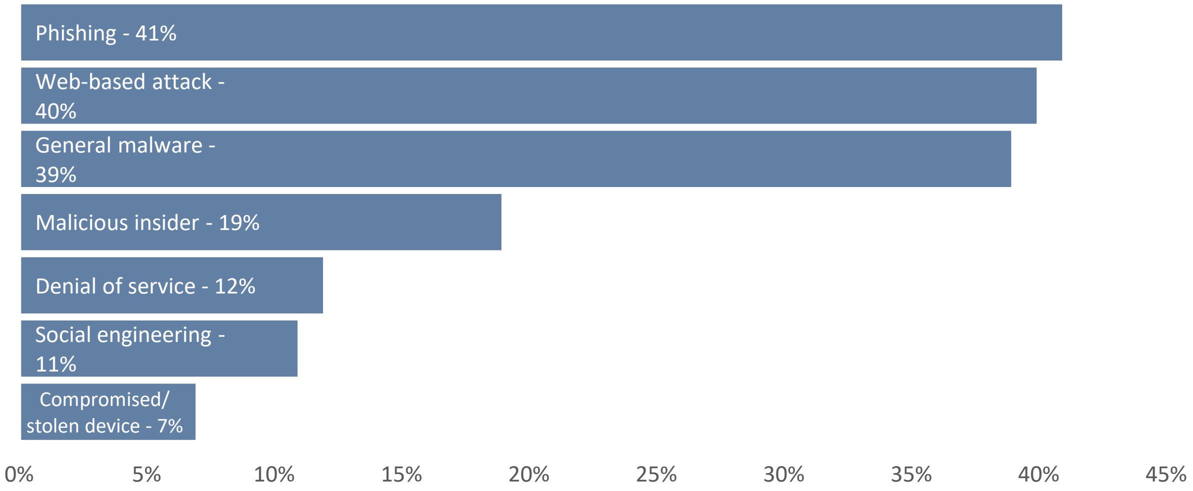
Source: ENISA, 2021.

The results of the 2021 survey also showcased phishing, web-based attacks, and malware as the most common sources of cybersecurity incidents among SMEs (see Figure 2) which is consistent with OECD (2021) findings that internet access increases the likelihood of cybersecurity incidents and a 667% spike in phishing attacks globally in the first months of the pandemic[4].

At the country level too, internet-based incidents, including phishing, malware, and web-based attacks, consistently appear as the most often threats across all economic sectors(see individual country reports in 7. Annex. Country reports for more details).

[4] Grandi, A. P., Sarri, A., Paggio, V. *What Europe's SMEs need to do for a cyber-secure future*. World Economic Forum. 28 June 2021. Available at: https://www.weforum.org/agenda/2021/06/cybersecurity-for-smes-europe/.

Figure 2. Cybersecurity incidents, by origin



Source: ENISA, 2021.

4. State of MSMEs' cyber-threats preparedness and awareness

Overall, the level of preparedness for cyber-threats remains limited across the EU with a perceived notion that cybersecurity is only relevant for large corporations or IT sector. In line with the common perception, large enterprises in the EU appear more likely to have a formally defined cybersecurity policy (Eurostat, 2020). Yet, the 2019 PwC report[5] shows that in Poland only 8 out of 100 firms were fully prepared for a cyberattack[6] with the majority of surveyed large companies (41% of the total sample) failing to fulfil the criteria.

The results of the 2019 Eurostat business survey showed that about 92% of the EU enterprises have adopted cybersecurity measures. Yet, the breakdown of the measures by type suggests that most of the enterprises focus on basic security controls only (see Figure 3). Similarly, the 2021 ENISA survey of the EU SMEs confirmed that 70% of SMEs use some form of basic security measures, including regular backups, antivirus, firewall, and systemic update of software, albeit only 30% of SMEs report resorting to more comprehensive cybersecurity measures (e.g., development of incident response structure or recovery plan, employment of the security officer, ISMS, removable media management, etc.)

The limited degree of preparedness is primarily driven by low levels of awareness on the matters of cybersecurity across the EU-27 (see Figure 3) with the lack of awareness and commitment from management being the common and most often cited challenge (ENISA, 2021).

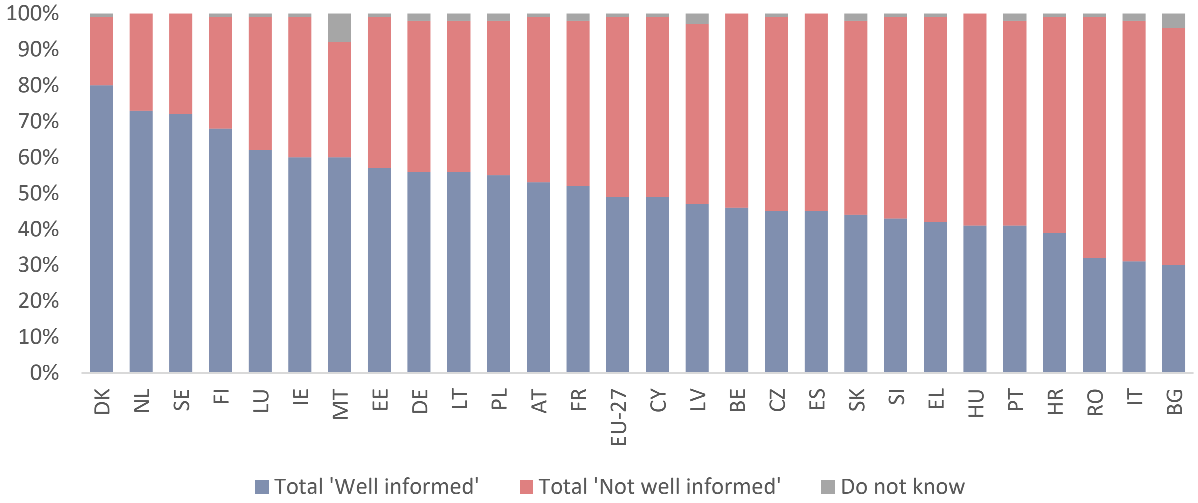
Other structural challenges that undermine greater preparedness of the MSMEs include (i) low cybersecurity awareness of the personnel; (ii) inadequate protection of critical and sensitive

[5] PWC (2018). Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście.

[6] i.e., (i) had sufficient IT security systems in place and a dedicated team of minimally 2 employees; (ii) allocated at least 10% of their budget to investments in this area; (iii) the board was regularly updated on the subject of cybersecurity through official reports; and (iv) there was a dedicated director or manager for cybersecurity in place.

information; (iii) lack of budget; (iv) lack of dedicated IT and cybersecurity specialists; (v) lack of suitable cybersecurity guidelines specific to SMEs; (vi) low management support.

Figure 3. Distribution of answers to the question: "How well informed do you feel about the risks of cybercrime?"



Source: Special Eurobarometer 499: Europeans' attitudes towards cyber security (2020).

Building on the low level of personal awareness, about 84% of the cyberattacks in the EU rely on social engineering to lure people into divulging sensitive information or clicking on the link that may contain malicious files (ENISA, 2020).

In this light, the 2017 Kaspersky report[7] also underlined the role of "human factor" as another important source of cybersecurity threats with over 70% of the 2016 incidents in large businesses and 60% of incidents in SMEs being due to human errors, malware, or both. The same year, the employees' accidental or incorrect actions alone caused 28% of large businesses and 20% of SMEs' system downtime. Yet, less than 30% of the SMEs in the EU-27 make their employees aware of their obligations in ICT security through compulsory training courses – almost twice less compared to large enterprise.

More importantly, however, the greater and the most frequent cyber-threats are also the ones on which the level of awareness is the lowest in the EU. Table 2 provides an overview of the state of awareness for each of the main cyber risks.

[7] Kaspersky, "IT Security Risks Survey", 2017, Available at https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083900/20170710_Report_Human-Factor-In-ITSec_eng_final.pdf

Table 2. State of cyber-threats awareness in the EU-27

Threat	Awareness level	Explanation
Malware	Very low	This is the number one cyber threat according to the latest figures available, as 400.000 detections of pre-installed spyware and adware on mobile devices were detected[8]
Web-based Attacks	Very low	This is the second most popular cyber threat according to the latest figures available, with the reported blocking of nearly 63 million malicious web requests related to formjacking (a web - based attack technique) in May 2019[9]
Phishing	Very low	This is the third most popular cyber threat according to the latest figures available: according to a study, 90% of organisations experienced targeted phishing attacks in 2019[10]
Web application attacks	Very low	This is the fourth most popular cyber threat according to the latest figures available, with an increase of 52% in the number of web application attacks in 2019, compared with 2018[11]
Spam	Very Low	This is the fifth most popular cyber threat according to the latest figures available, with 13% of data breaches caused by malicious spam[12]
Denial of service	Low	This is the sixth most popular cyber threat according to the latest figures available, with an increase of 241% in total number of attacks during Q3 2019 compared with the same period of 2018[13]
Identity theft	Low	This is the seventh most popular cyber threat according to the latest figures available, with at least 900 international cases of identity theft or identity-related crimes detected[14]
Data breaches	Low	This is the eighth most popular cyber threat according to the latest figures available, with an increase of 54% in the total number of breaches by midyear 2019 compared with 2018[15]
Insider threat	Low	This is the ninth most popular cyber threat according to the latest figures available, with 65% of the impact from insider threats includes damage to the organisation's reputation and finances[16]

[8] Malware Bytes (2020) "2020 State of Malware Report" Available at: https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

[9] Norton "What is Formjacking and How Does it Work?" Available at: https://us.norton.com/internetsecurityemerging-threats-what-is-formjacking.html

[10] Proof Point (2020) "2020 State of the Phish: Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike" Available at: https://www.proofpoint.com/us/securityawareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

[11] Sonicwall (2020) "Sonicwall Cyber Threat Report" Available at: https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

[12] Cisco (2019) "Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study" Available at: https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

[13] A10 Networks (2019) "Q4 2019 - The State of DDoS Weapons Report." Available at: https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

[14] ITIJ (2019) "2019 identity theft report released" Available at: https://www.itij.com/latest/news/2019- identity-theft-report-released 2. "Capital One

[15] ENISA (2020) "Data breach" Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-data-breach

[16] Egress (2019) "Insider Data Breach Survey 2019" Available at: https://scoopcms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmattersinsider-threat-research-report-a4-uk-digital.pdf

Botnets	Low	This is the tenth most popular cyber threat according to the latest figures available: since 2017, the number of newly detected botnet C&Cs has increased from 9,500 to 17,602[17]
Physical manipulation, damage, theft and loss	Medium	This is the eleventh most popular cyber threat according to the latest figures available, with 20% of cybersecurity incidents started or ended with a physical action[18]
Information leakage	Medium	This is the twelfth most popular cyber threat according to the latest figures available, with an 11% increase in data disclosures in 2019, compared with 2018[19]
Ransomware	Medium	This is the thirteenth most popular cyber threat according to the latest figures available, with an increase of 365% in detections in businesses in 2019, compared with the first half of 2018[20]
Cyberespionage	Medium	This is the fourteenth most popular cyber threat according to the latest figures available, with 20% of data breaches and 11,2% of incidents motivated by cyber espionage[21]
Cryptojacking	Medium	This is the fifteenth most popular cyber threat according to the latest figures available, with an increase of 9% of the activities between January and June 2019 when compared to levels seen in the last six months of 2018[22]

[17] Spamhaus (2020) "Spamhaus Botnet Threat Report 2019." Available at: https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

[18] Verizon (2019) "2019 Payment Security Report" Available at: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

[19] Verizon (2019) "Data Breach Investigations Report." Available at: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

[20] BDO (2019) "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare" Available at: https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyberthreat-report-focus-on-health

[21] DBR & Verizon (2020) "Data Breach Investigations Report 2020" Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-reportemea.pdf

[22] Yessi Bello Perez, TheNextWeb (2019) "Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019." Available at: https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-firsthalf-2019/

5. Identification of best practices as regards MSMEs support in the area of cybersecurity

5.1 Policy environment

EU level

The European Commission commitment under "An SME Strategy for a sustainable and digital Europe"[23] to:

- develop Digital Crash Courses for SME employees to become proficient in cybersecurity;
- launch a programme for "digital volunteers" to allow young skilled people and experienced seniors to share their digital competence with traditional businesses;
- launch Pact for Skills, with a dedicated component for SMEs;
- expand the network of Digital Innovation Hubs (DIH) as the main tool to foster the digital transformation of SMEs

The EU Skills for SMEs initiative launched in continuation of the Strategy which identified, designed and tested specific measures to support the development of cybersecurity skills in SMEs and set four streams of policy actions to reduce skills gap of SMEs. The later were followed by the EU supporting measures to policymakers, educators, and industry, and included the following:

- Stronger ecosystems: SMEs should be connected and embedded in regional or sectoral support structures;
- Strategic outlook development: SMEs ought to understand the strategic business opportunity that comes with the adoption of new technologies;
- Structured skills development, from vision to plan;
- Tailored training.

The 2020 joint declaration of the European Parliament and of the Council of the European Union on "The EU's Cybersecurity Strategy for the Digital Decade"[24] that underlined cybersecurity as an essential component of a resilient, green, and digital Europe, and put forward the following initiatives.

- reform the EU rules on the security of Network and Information Systems (NIS) with the aom to increase the level of cyber resilience of all relevant sectors and stakeholders;
- investment in the EU digital transition, with a special focus on support for SMEs and their cybersecurity awareness through, among other, the Revised Digital Education Action Plan;
- create a network of Security Operations Centres across the EU to (i) support public-private and cross-border cooperation in creating national and sectoral networks, and (ii) provide timely warnings on cybersecurity incidents to authorities, interested stakeholders, and the Joint Cyber Unit (a new creation too) before they can cause large-scale damage;
- promote a better use of the latest cybersecurity tools by SMEs –including, but not limited to, through dedicated activities under the DIHs.

[23] European Union: European Commission (2020) *An SME Strategy for a sustainable and digital Europe,* 10.3.2020 COM (2020) 103 final

[24] European Union: European Parliament and Council of the European Union (2020) *The EU's Cybersecurity Strategy for the Digital Decade,* 16.12.2020 JOIN(2020) 18 final

SMESEC by the SMESEC consortium for the European Commission, which provides high-quality cybersecurity solutions attractive to SMEs with a restricted budget as well as cybersecurity training and awareness for SMEs and all type of employees[25].

Make_SME_Digital for the European Commission, which provides the European Commission with a structured programme for the training of SME employees and unemployed persons with digital skills that are required in the modern work place, including cybersecurity skills[26].

Materials provided by the **EU Agency for Cybersecurity (ENISA)**, including the following:

- Tips for selecting and using online communication tools;
- Tips for cybersecurity when buying and selling online;
- Tips for cybersecurity when working from home;
- Top ten cyber hygiene tips for SMEs during covid-19 pandemic;
- Joint checklist for SME.

Country level

Cybersecurity Skills Initiative (CSI) by an Irish nationwide public-private coalition, which contains a comprehensive plan to train 5,000 people in cybersecurity skills and help 4,000 companies to tackle the cybersecurity skills issue over the next three years.

Polish National Platform for Cybersecurity (NPC)[27], a research program led by the National Research Institute regarding cyberspace (NASK)[28] in cooperation with the Polytechnic of Warsaw, the National Center for Nuclear Research, and the National Institute of Telecommunications. The NPC produced regular publications on cybersecurity, including a yearly overview of cyber-incidents[29].

PWCyber Cybersecurity Cooperation Program[30], a collaboration between the consulting firm PWC and the Polish Department of Cybersecurity, that aims to improve (i) public administration competences in the field of cybersecurity; (ii) exchange of information on cyberthreats; (ii) recommendations on cybersecurity; (iv) cybersecurity assessment and certification; and (v) dissemination of information on cybersecurity innovations. Main activities within the program include training materials to improve the skills of user and staff responsible for cybersecurity, trainings and workshop, awareness-raising campaigns, and competitions on best practices among participating companies.

[25] SMESEC project, available at: https://www.smesec.eu/ Accessed on 24.3.2021

[26] Make_SME_Digital project, available at: https://makesmedigital.eu/ Accessed on 24-03.2021

[27] https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/2088,Narodowa-Platforma-Cyberbezpieczenstwa-NPC.html.

[28] https://en.nask.pl.

[29] CERT Polska (2020). Security of Polish Cyberspace. Annual report 2019 on the activity of CERT Polska.

[30] https://www.gov.pl/web/cyfryzacja/wzmacniamy-wspolprace-w-ramach-programu-pwcyber.

"National Framework for Cybersecurity"[31] introduced in Italy to (i) support companies in the areas of cybersecurity and data protection, and (ii) prepare MSMEs to implement appropriate interventions for the development of new and implementation of the existing cybersecurity strategies[32].

Italian National Inter-University Consortium for Information Technology (CINI) that develops learning materials and training on cyber risk management under the supervision of the Italian Ministry for University and Research. It allows assess the level of exposure to cyber risks of private and public actors and prepare a response plan to possible attacks. The tools prepared for understanding the "cyber language" and security processes include the "National Framework for Cybersecurity" (2016) and the "Essential Controls of Cybersecurity" (2017).

Memorandum of understanding between the Agency for the Digitalisation of Italy (AgID) and the General Confederation of Italian Industry (Confindustri) in recognition of the importance of cybersecurity for business and support of initiatives aimed at training public administrations and private companies on cybersecurity. The Confindustria's Digital Innovation Hubs will thus allow to spread general awareness on cybersecurity issues across Italy, ensuring the creation of training opportunities and a greater synergy between the public and private sectors[33].

5.2 Private sector environment

Lufthansa Group[34] adopts comprehensive approach to cyber threats including:

- Employee sensibilisation and targeted training: the Group Data Protection Commissioner plans and recommends training measures, and then ensures that training obligations are met;
- Constant monitoring of the global IT security situation: conscious that the Group's business processes are supported by IT components in almost all areas, and that these inevitably entail risks for the stability of business processes, as well as for the availability, confidentiality and integrity of information and data, the Executive Board monitors closely monitors all developments;
- A group-wide cyber security program through which new technological tools and processes are introduced and/or adapted to the changing threat situation;
- A Security Operations Centre (SOC) on duty 24/7 to protect and secure the IT infrastructure;
- A Computer Emergency Response Team permanently on standby to provide a rapid response in the event of a security incident or cyber-attack;
- Regular checks, also on external service providers.

[31] CINI – Cyber Security National Lab and CIS - Sapienza Research Center of Cyber Intelligence and Information Security (Sapienza Università di Roma), "Framework Nazionale per la Cybersecurity e la Data Protection", 2019. Available at https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf

[32] CINI – Cyber Security National Lab, "The future of Cybersecurity in Italy: Strategic focus areas", 2018. Available at https://cybersecnatlab.it/wp-content/uploads/2020/03/White-Book-2018.pdf

[33] AGID, "Cybersecurity: nuove sinergie pubblico-privato sulla sicurezza cibernetica", 2018. Available at: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2018/06/22/cybersecurity-nuove-sinergie-pubblico-privato-sulla-sicurezza-cibernetica

[34] Lufthansa Group, Website: Data Protection and Information Security. Available at: https://www.lufthansagroup.com/en/responsibility/product-customer/data-protection-and-information-security.html Accessed on: 24.3.2021

KBC Bank[35] coordinates largely autonomous and well-established cybersecurity teams within national branches through an external provider and implementation of the IBM Security SOAR platform which, amongst others, provided playbooks for different incidents to enable consistent execution across the group.

Sodexo chose to complement its internal efforts with Qualys Vulnerability Management (VM)[36], which delivers a complete range of functionality, including network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking prioritized by business-risk profile.

6. Identification of policy recommendations

A detailed overview of country-specific policy recommendations is provided in the individual country reports (see 7. Annex. Country reports). The proposed recommendations can be systemised along three main pillars.

Strengthening **cyber awareness** among MSMEs by promoting better understanding of cybersecurity at large. This can be done through the dedicate awareness raising campaigns at the EU, national, and local level focused , among others, on the information regarding (i) the most common, dangerous, and disrupting cyber-threats; (ii) current trends in cybersecurity; and (iii) cyber risk management frameworks.

As the past experience shows, however, lack of engagement from MSMEs is the main challenges to the effectiveness of the campaign (ENISA, 2021). Thus, private-public partnerships and involvement of business networks are crucial to ensure that a campaign reaches and actively engages the MSMEs audience. Content and channels of the outreach campaign should be tailored to the MSMEs context and needs of each sector.

Strengthening **cyber resilience** among MSMEs by

- **creating MSMEs focused cybersecurity standards and guidelines**. Most of the available cybersecurity standards were formulated with the focus on large enterprises and fail to capture needs and capacities of MSMEs (ENISA, 2021). Development and proliferation of the guidelines fit to MSMEs context could thus be achieved through the engagement of MSMEs in all stages of conceptualization of standards and dissemination of the guidelines and templates among MSMEs.
- **promoting use of cyber risk management frameworks within MSMEs**. The efforts should focus on (i) adaptation of the frameworks to the MSMEs needs; (ii) raising awareness on the risk management frameworks, their applicability, and benefits; (iii) making cybersecurity more accessible.

Strengthening **cyber responsiveness** of MSMES by promoting voluntary and compulsory trainings among employees and supporting development of simplified security protocols that can be operationalized by MSMEs with limited extra costs.

[35] IBM, Website: https://www.ibm.com/case-studies/kbc-group-security-soar Accessed on: 23.2.2021

[36] Qualys, Website: https://www.qualys.com/customers/success-stories/sodexo-securing-enterprise-automated-vulnerability-management/ Accessed on 23.3.2021

7. Annex. Country reports

7.1. Europe

7.1.1. Introduction

Today, cybersecurity remains a central topic in the international and national agendas, and is gaining importance within the private sector. Large corporations and MSMEs are increasingly becoming aware of the need to equip themselves with the right tools and strategies to prevent and respond effectively to any cyber threat.

Based on ENISA's classification of the "top 15 cyber-threats in Europe", this report highlights main finings in terms of level of awareness and preparedness of EU MSMEs on cybersecurity and. As expected, while still maintaining its "EU relevance", the topic of cyber-readiness seems particularly urgent for micro and small medium enterprises established in Southern/Balkan regions and operating in non-ICT dominant sectors.

Our results suggests that the cyber-lag experienced by the vast majority of EU MSMEs is firstly and foremost and issue of culture and cultural understating. Despite the numerous initiatives implemented at EU level to increase the awareness on the topic, EU SMEs are still failing to comply with the very essentials of cybersecurity.

Our key takeaways recommend a strong focus on training and reskilling of workforce as key initiatives in the cybersecurity domain. Training is often privately run and focuses on unemployed people: furthermore, most initiatives that focus on retraining are short and provide basic rather than advanced skills. Existing initiatives recognise their limited potential in addressing skills gaps, therefore they serve only as temporary, immediate solutions.

7.1.2. Mapping out cyber-threats in Europe

ENISA's report "Threat Landscape 2020 – List of top 15 threats" represents the most reliable source to identify the most concerning and recurrent cyber-threats in Europe. These are ranked as follows:

1. Malware
2. Web-based Attacks
3. Phishing
4. Web application attacks
5. Spam
6. Denial of service
7. Identity theft
8. Data breaches
9. Insider threat
10. Botnets
11. Physical manipulation, damage, theft and loss
12. Information leakage
13. Ransomware
14. Cyberespionage
15. Cryptojacking

The report provides also for a useful assessment of cyber-risks distribution and frequency among sectors (Table1):

Table 1: distribution and frequency of cyber threats per sector

Sector	Most Popular Cyber-Threat	Frequency
Individual	Phishing Malware Information Leakage Data theaft	Stable
Multiple Industries	Web applications attacks Phising Malware	Increasing
Public Administration	Malware Phishing Web based attacks	Stable (slight decreasing)
Finance and Banking	Web application attacks Insiders and data abuse Malware Data theft	Stable
Health/Medical	Malware Insider and data abuse Web application attacks	Increasing
Education	Malware Ransomware Web based attacks	Stable (slight decreasing)
Information & Comm.	Web application attacks Insider and data abuse Malware	Stable
Professional/Dig. Services	Web application attacks Insider and data abuse Malware	Stable
Arts and Entertainement	Web application attacks Malware Phishing	Stable
Manufacturing	Malware Web application attacks Insider and data abuse	Stable

Notably, Member States differ greatly in terms of awareness, knowledge and ability to deploy strategies and programs pertaining to cybersecurity, which in turn affect the level of preparedness to tackle cyber threats, thereby defining what constitutes a threat itself.

This is mainly due to two factors:

- Industry: compared to labour-intensive sectors, capital-intensive sectors are much more prone to exploit digital technologies in their favour. As typically targeted by cybercriminals, capital-intensive industries dispose of consistent human skills and technologies able to safeguard them from external disruptors. On the other hand, the surface exposed to cyberattacks of firms and organisations operating in labour-intensive sectors is significantly higher with much lesser internal resources to tackle and overcome the same challenges. Consequently, Member States at higher labour-intensive coefficient face greater challenges compared to other capital-intensive economies

- Digital culture: it is no secrete that the level of digitalisation among Member States is very fragmented and heterogeneous. As this very same report indicates, there are several instrumental socio-economic conditions affecting the cyber-responsiveness and resilience of EU MSMEs. One among many is the ICT skills-shortage recorded among many Mediterranean and Balkan regions, preventing their national firms in acquiring and retaining professionals in the domain of cybersecurity. For instance, a 2018 study for the European Economic and Social Committee found that SMEs located in Northern Europe fare, on average, slightly better than their Southern counterparts, but that the overall level of preparedness is insufficiently low.

7.1.3. The level of awareness of cyber-attacks

In regards to the assessment of the level of awareness of cyber-threats, ENISA's reports comes in the handy once again:

Threat	Awareness level	Explanation
Malware	Very low	the ENISA reports this is the number one cyber threat according to the latest figures available, as 400.000 detections of pre-installed spyware and adware on mobile devices were detected[37]
Web-based Attacks	Very low	the ENISA reports this is the second most popular cyber threat according to the latest figures available, with the reported blocking of nearly 63 million malicious web requests related to formjacking (a web - based attack technique) in May 2019[38]
Phishing	Very low	the ENISA reports this is the third most popular cyber threat according to the latest figures available: according to a study, 90% of organisations experienced targeted phishing attacks in 2019[39]
Web application attacks	Very low	the ENISA reports this is the fourth most popular cyber threat according to the latest figures available, with an increase of 52% in the number of web application attacks in 2019, compared with 2018[40]
Spam	Very Low	the ENISA reports this is the fifth most popular cyber threat according to the latest figures available, with 13% of data breaches caused by malicious spam[41]
Denial of service	Low	the ENISA reports this is the sixth most popular cyber threat according to the latest figures available, with an increase of 241% in total number of attacks during Q3 2019 compared with the same period of 2018[42]
Identity theft	Low	the ENISA reports this is the seventh most popular cyber threat according to the latest figures available, with at least 900 international cases of identity theft or identity-related crimes detected[43]
Data breaches	Low	the ENISA reports this is the eighth most popular cyber threat according to the latest figures available, with an increase of 54% in the total number of breaches by midyear 2019 compared with 2018[44]
Insider threat	Low	the ENISA reports this is the ninth most popular cyber threat according to the latest figures available, with 65% of the impact from insider threats includes damage to the organisation's reputation and finances[45]

[37] Malware Bytes (2020) "2020 State of Malware Report" Available at: https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

[38] Norton "What is Formjacking and How Does it Work?" Available at: https://us.norton.com/internetsecurityemerging-threats-what-is-formjacking.html

[39] Proof Point (2020) "2020 State of the Phish: Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike" Available at: https://www.proofpoint.com/us/securityawareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

[40] Sonicwall (2020) "Sonicwall Cyber Threat Report" Available at: https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

[41] Cisco (2019) "Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study" Available at: https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

[42] A10 Networks (2019) "Q4 2019 - The State of DDoS Weapons Report." Available at: https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

[43] ITIJ (2019) "2019 identity theft report released" Available at: https://www.itij.com/latest/news/2019- identity-theft-report-released 2. "Capital One

[44] ENISA (2020) "Data breach" Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-data-breach

[45] Egress (2019) "Insider Data Breach Survey 2019" Available at: https://scoopcms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmattersinsider-threat-research-report-a4-uk-digital.pdf

Botnets	Low	the ENISA reports this is the tenth most popular cyber threat according to the latest figures available: since 2017, the number of newly detected botnet C&Cs has increased from 9,500 to 17,602[46]
Physical manipulation, damage, theft and loss	Medium	the ENISA reports this is the eleventh most popular cyber threat according to the latest figures available, with 20% of cybersecurity incidents started or ended with a physical action[47]
Information leakage	Medium	the ENISA reports this is the twelfth most popular cyber threat according to the latest figures available, with an 11% increase in data disclosures in 2019, compared with 2018[48]
Ransomware	Medium	the ENISA reports this is the thirteenth most popular cyber threat according to the latest figures available, with an increase of 365% in detections in businesses in 2019, compared with the first half of 2018[49]
Cyberespionage	Medium	the ENISA reports this is the fourteenth most popular cyber threat according to the latest figures available, with 20% of data breaches and 11,2% of incidents motivated by cyber espionage[50]
Cryptojacking	Medium	the ENISA reports this is the fifteenth most popular cyber threat according to the latest figures available, with an increase of 9% of the activities between January and June 2019 when compared to levels seen in the last six months of 2018[51]

Concerningly enough, the above table indicates that the greater cyber-threats are also the same with the lowest level of awareness. Considering the increasing hostility and complexity of cyber threats, and the increasing impact that the new technologies are having on everyday life (i.e. teleworking during the spread of the COVID–19) there is a growing focus on developing cybersecurity policies and actions, to achieve a high level of cyber awareness in the European context.

A key campaign to promote awareness throughout the EU is the European Cybersecurity Month (ECSM)[52]. Since 2012 and every year during the month of October, the European Commission and the ENISA support Member States and several partners (governments, universities, think tanks, NGOs, professional associations, private sector business) in the organisation of events scattered across the continent. The events organised range from conferences to trainings and workshops.

A number of other actions, led by the ENISA, also contribute to this goal:

- The Cybersecurity Higher Education Database, which helps people navigate the variety of opportunities in higher education linked to cybersecurity;
- The European Cybersecurity Skills Framework, which supports employability in cybersecurity positions by developing a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers across the EU;

[46] Spamhaus (2020) “Spamhaus Botnet Threat Report 2019.” Available at: https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

[47] Verizon (2019) “2019 Payment Security Report” Available at: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

[48] Verizon (2019) “Data Breach Investigations Report.” Available at: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

[49] BDO (2019) “BDO’s Fall 2019 Cyber Threat Report: Focus on Healthcare” Available at: https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyberthreat-report-focus-on-health

[50] DBR & Verizon (2020) “Data Breach Investigations Report 2020” Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-reportemea.pdf

[51] Yessi Bello Perez, TheNextWeb (2019) “Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019.” Available at: https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-firsthalf-2019/

[52] https://cybersecuritymonth.eu/

- The European Cyber Security Challenge, an annual event that facilitates collaboration and competition among young people.

7.1.4. Preparedness

Although the average level of cybersecurity is satisfactory, not all European countries have the same level of preparedness and awareness about cyber threats. According to a study conducted by the European Economic and Social Committee[53] in 2018, while Estonia and France represent excellence in cybersecurity in Europe and worldwide, countries such as Slovenia or Slovakia still show a general lack of preparation on the subject, representing a vulnerable point within the European cybersecurity panorama. Discrepancies are particularly evident between Mediterranean/Balkan regions and Norther territories.

Eurostat[54] data shows that in 2018, 13 % of EU companies experienced cybersecurity attacks/problems.

The most reported threats were:

- 10 % of enterprises reported the unavailability of ICT services (hardware or software failures), denial of service attacks, ransomware attacks;
- 6 % of enterprises reported the destruction or corruption of data due to infection with malicious software, hardware or software failures or unauthorized intrusion;
- 1% of enterprises reported the disclosure of confidential data (for instance due to intrusion, pharming or phishing attack, actions by own employees).

The data shows that large enterprises were most affected by cyber-attacks: 25% of large enterprises experienced such problems during 2018, compared to 18% of medium-sized enterprises and 12% of small enterprises.

In 2019, Eurostat interviewed around 153.500 enterprises (with 10 or more persons employed): the results were collected in the report "ICT Security in Enterprises"[55]. The survey shows that 92 % of EU enterprises have adopted security measures for cybersecurity.

The most widely used measures are:

- Keeping the software or operating systems up to date (87 %)
- Strong password authentication (76 %)
- Data backup to a separate location or cloud (76 %)
- Network access control (65 %)

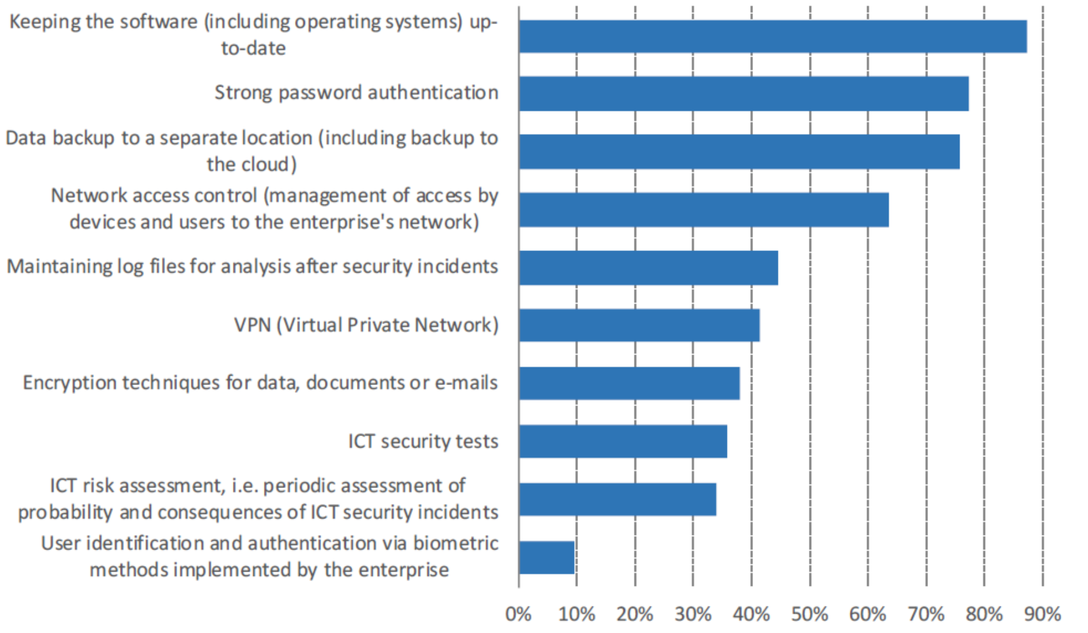
There are still few companies that report maintaining log files for analysis after security incidents (45 %) and use of Virtual Private Network - VPN (42 %). Encryption techniques for data, documents or e-mails were used by 38 % of enterprises. ICT security tests (35 %) and ICT risk assessment (33 %) were used less frequently by EU enterprises. User identification and authentication via biometric methods were used by 10 % of enterprises (Exhibit 1):

[53] European Economic and Social Committee, "Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks", 2018, available at https://hcss.nl/sites/default/files/files/reports/Cybersecurity%20ensuring%20awareness%20and%20resilience%20of%20the%20private%20sector%20acrros%20Europe%20in%20face%20of%20mounting%20cyber%20risks.pdf

[54] Eurostat, "ICT Security in Enterprises," 2020, available at http://ec.europa.eu/eurostat/statisticsexplained/index.php/ICT_security_in_enterprises.

[55] Eurostat, "ICT Security in Enterprises," 2020, available at http://ec.europa.eu/eurostat/statisticsexplained/index.php/ICT_security_in_enterprises.

Exhibit 1: Type of ICT measures adopted by EU enterprises in 2019



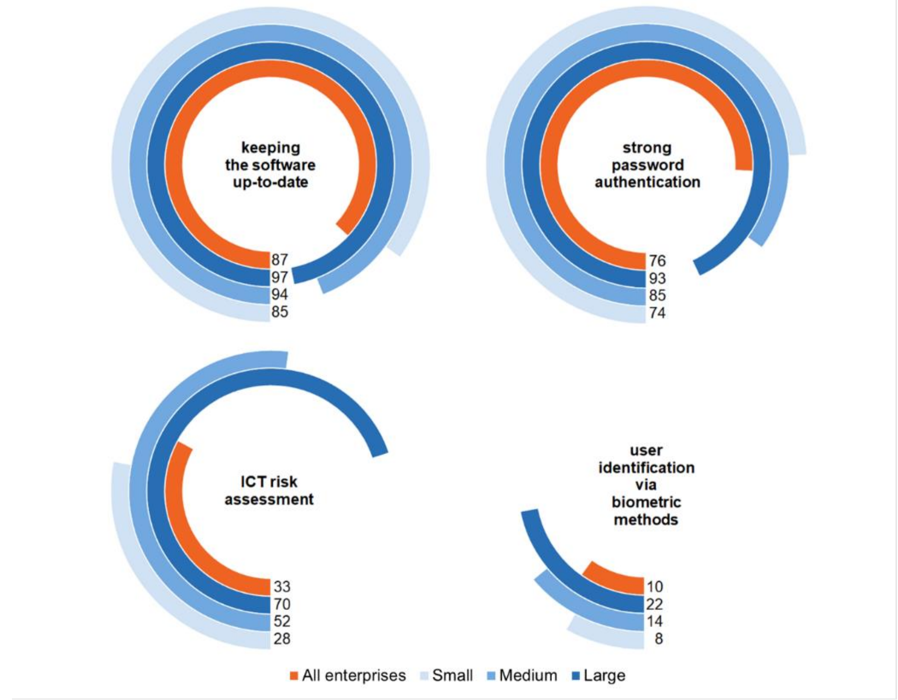
Source: Eurostat (2020)

According to the survey, companies usually adopt different cybersecurity schemes: whether ICT security activities are carried out by its own employees or by external consultants. In 2019, 65% of companies reported that ICT security activities were carried out by external providers, while 40% of companies reported that ICT security activities were carried out by their own employees. This different approach may affect the level of internal awareness and preparedness on cybersecurity issues and, above all, on the ability to respond quickly to possible cyber threats.

As for the ICT measures adopted by MSMEs, Exhibit 2 provides a great overview according to Eurostat data gathered in 2019.[56] The ICT security measure "keeping the software or operating systems up-to-date" is used by almost all companies. The second most popular measure is strong password authentication, but here the digital divide between SMEs and large businesses is already considerably bigger. The gap is even wider if one looks at the third most popular measure – the ICT risk assessment, which is used by 70 % of large enterprises, but only 28 % of small businesses. From MSMEs' perspective this is symptomatic of incompliance even with the vary basics of cybersecurity such as strong password authentication.

[56] Eurostat (2019) (isoc_cisce_ra)

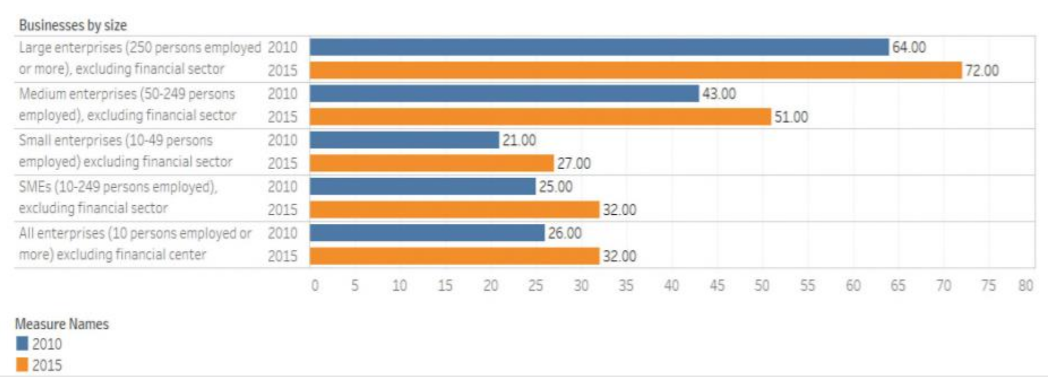
Exhibit 2. ICT Security Measures usage by company size



Eurostat (2019). isoc_cisce_ra

Another 2020 survey by Eurostat[57] shows that the larger companies are more likely to adopt an ICT security policy: 72% of large enterprises (250 or more persons employed) claim to have adopted an internal cybersecurity policy, the percentage drops to 51% for medium enterprises (50 to 249 persons employed), and to 27% for small enterprises (10 to 49 persons employed). The same survey shows, between 2010 and 2015, an increase in all companies (regardless of size) in the attention paid to the issue: a sign of growing awareness and concerning (Exhibit 3):

Exhibit 3: Percentage of EU companies having formally defined ICT security policy by company size



Source: Eurostat (2020)

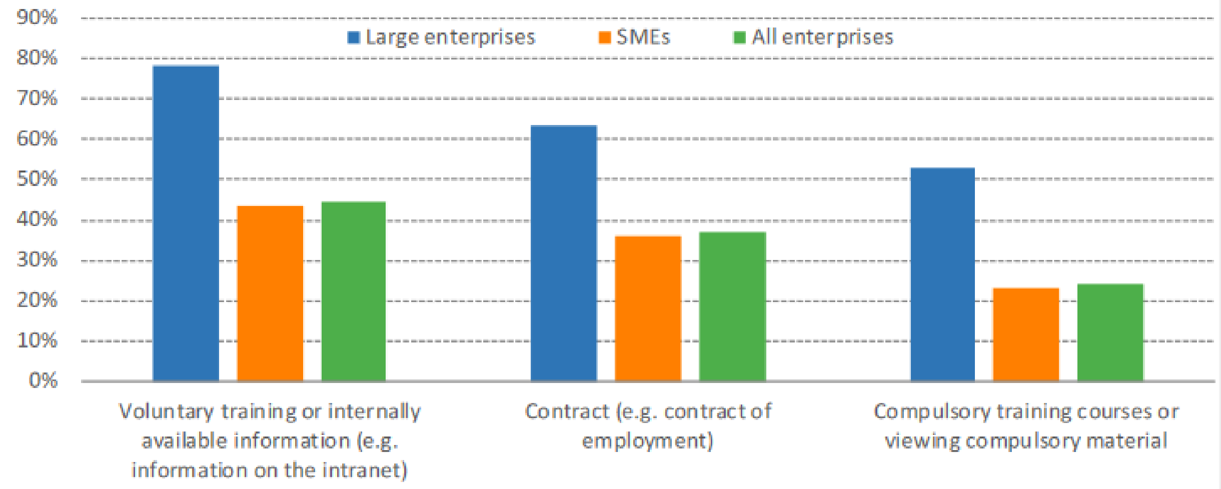
[57] Eurostat, "ICT Security in Enterprises," 2020, available at http://ec.europa.eu/eurostat/statisticsexplained/index.php/ICT_security_in_enterprises.

In case of MSMEs, not only the Technological dimension is neglected, but also the "human capital" one. In its "IT Security Risks Survey[58]" (2017), Kaspersky reported that 52% of businesses admit that employees are the weakness spot in the IT security system. Throughout a series of careless actions, they are able to put the enterprises IT security strategy at risk, underlined that "human factor" in IT security is still a central point and deserves proper attention.

According to the report, the majority of both SMEs and large businesses thinks employees are the biggest threat to cybersecurity, even if most of the times there is no malicious intent, and rightly so, as incident statistics go in this direction. Over 70% of large business and nearly 60% of SMEs had security issues in 2016 due to human errors, malware, or both. Employees' accidental or incorrect actions caused 28% of large businesses and 20% of SMEs' system downtime in 2016.

As Exhibit 4 shows, a little more than 40% of EU SMEs make their employees aware of ICT security obligations by offering voluntary training or sharing information internally. The figure for compulsory training is even more worrying, dipping at around 20%[59].

Exhibit 4. Percentage of enterprises that make persons employed aware of their obligations in ICT security issues.



Source: Eurostat (2019), survey on ICT usage and e-commerce in enterprises.

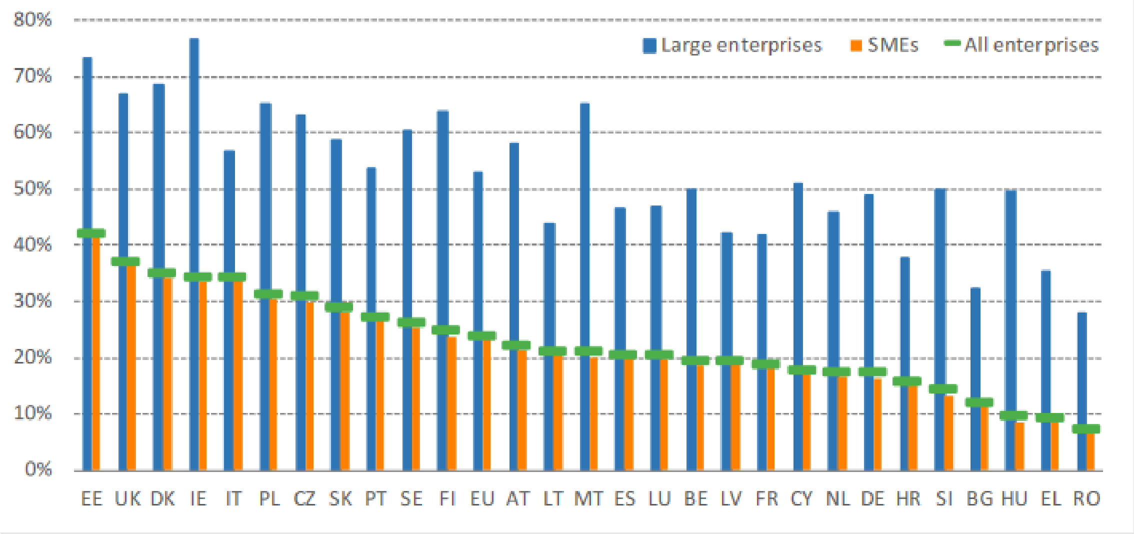
Additionally, these averages hide substantial cross-country differences. As Exhibit 5 shows, over 30% of SMEs provide compulsory training in Estonia, Denmark, Ireland and Italy, but less than 1 in 10 SMEs do in Romania, Greece and Hungary[60].

[58] Kaspersky, "IT Security Risks Survey", 2017, Available at https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083900/20170710_Report_Human-Factor-In-ITSec_eng_final.pdf

[59] The Digital Economy and Society Index (DESI) (2020)

[60] Eurostat (2019) Eurostat, Survey on ICT usage and e-commerce in enterprises

Exhibit 5: % of enterprises that make employees aware of their obligations in ICT security by compulsory training courses



Source: Eurostat, (2019). Survey on ICT usage and e-commerce in enterprises.

7.1.5. Best Practices

Policy Level

A brief perusal of EU documents and publications shows that Brussels is well aware of the need to bridge the SMEs' skills gap on cybersecurity across the continent.

The European Union[61] has been implementing a major strategy, deploying its work along three lines of action:

- Providing the EU's public and private sector the most reliable infrastructures and services to ensure resilience and capacity to respond to cyber – attacks;
- Support (through legislation and cooperation) Member States in defending their citizens, economic interests and national security;
- Fostering international cooperation for a global, open, stable and safe cyberspace.

Paramount in this regard is the European Commission Communication on "An SME Strategy for a sustainable and digital Europe"[62], which, even before the Covid-19 pandemic forced remote work for many employees, acknowledged that European SMEs were "very vulnerable to cyber threats". The strategy, amongst other things, commits the European Commission to:

- developing Digital Crash Courses for SME employees to become proficient in cybersecurity;
- launching a programme for "digital volunteers" to allow young skilled people and experienced seniors to share their digital competence with traditional businesses;
- launching a Pact for Skills, with a dedicated component for SMEs;
- expanding the network of Digital Innovation Hubs (DIH), which is the main tool to foster the digital transformation of SMEs

[61] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade", 2020

[62] European Union: European Commission (2020) *An SME Strategy for a sustainable and digital Europe,* 10.3.2020 COM (2020) 103 final

The production of the Strategy was accompanied by the Skills for SMEs initiative, which, launched by DG GROW, identified, designed and tested specific measures to support the development of cybersecurity skills in SMEs. The initiative also produced a paper[63] which sets forth four streams of action found to be crucial to bridging the SMEs' skills gap:

- Stronger ecosystems: SMEs should be connected and embedded in regional or sectoral support structures;
- Strategic outlook development: SMEs ought to understand the strategic business opportunity that comes with the adoption of new technologies;
- Structured skills development, from vision to plan;
- Tailored training.

For each of these streams, sub-goals were identified, as well as their supporting measures addressing policymakers, education providers, industry and other stakeholders. The paper also identifies a number of best practices, including:

- SMESEC by the SMESEC consortium for the European Commission, which provides high-quality cybersecurity solutions attractive to SMEs with a restricted budget as well as cybersecurity training and awareness for SMEs and all type of employees[64];
- Make_SME_Digital for the European Commission, which provides the European Commission with a structured programme for the training of SME employees and unemployed persons with digital skills that are required in the modern work place, including cybersecurity skills[65];
- Cybersecurity Skills Initiative (CSI) by an Irish nationwide public-private coalition, which contains a comprehensive plan to train 5,000 people in cybersecurity skills and help 4,000 companies to tackle the cybersecurity skills issue over the next three years.

The EU's commitment to bridge SMEs' cybersecurity skills gap has gained a new momentum in light of the ongoing Covid-19 pandemic, the latter having accelerated the digital transition. In this respect, worth of note are:

1. The European Commission's announcement[66], in May 2020, that it would commit nearly €41 million through Horizon 2020, the EU's research and innovation programme, to support 9 projects aimed at working on innovative cybersecurity and privacy solutions, some of which supporting SMEs
2. The European Commission Communication on "European Skills Agenda for sustainable competitiveness, social fairness and resilience"[67], adopted in July 2020, which commits the European Commission to supporting digital skills for all by strengthening, amongst other things, investments in cybersecurity. One way of doing this, the document recognises, is by promoting STEM pathways among young women
3. The Digital Europe Programme, which started this year and envisages 1.7 billion for cyber security, and foresees, amongst other things, investment in specialised training opportunities.

[63] European Union (2020) *Skills for SMEs Cybersecurity, Internet of Things and Big Data for Small and Medium-Sized Enterprises, 5.3.2020*

[64] SMESEC project, available at: https://www.smesec.eu/ Accessed on 24.3.2021

[65] Make_SME_Digital project, available at: https://makesmedigital.eu/ Accessed on 24-03.2021

[66] European Union: European Commission (2020) Press release *EU grants nearly €49 million to boost innovation in cybersecurity and privacy systems.* Available at: https://ec.europa.eu/digital-single-market/en/news/eu-grants-nearly-eu49-million-boost-innovation-cybersecurity-and-privacy-systems

[67] European Union: European Commission Communication (2020) *European Skills Agenda for sustainable competitiveness, social fairness and resilience*, 1.7.2020 COM(2020) 274 final

4. The joint declaration of the European Parliament and of the Council of the European Union on “The EU's Cybersecurity Strategy for the Digital Decade”[68], which, put forward in December 2020, reads that “cybersecurity is essential for building a resilient, green and digital Europe”. To do so, the Commission proposes:
    - to reform EU rules on the security of Network and Information Systems (NIS) –the core of the Single Market for cybersecurity, to “increase the level of cyber resilience of all relevant sectors, public and private, that perform an important function for the economy and society”
    - an unprecedented level of investment in the EU's digital transition, with a special focus on support for SMEs, as “over two-thirds of companies, in particular SMEs, are considered ‘novices’ in cybersecurity”
    - “to build a network of Security Operations Centres across the EU, and to support the improvement of existing centres and the establishment of new ones”, as well as “training and skill development of staff operating these centres”. In particular, it suggests supporting public-private and cross-border cooperation in creating national and sectoral networks, involving also SMEs. The purpose of this network is to provide timely warnings on cybersecurity incidents to authorities, interested stakeholders, and the Joint Cyber Unit (a new creation too), so as to act as a cybersecurity shield for the EU, with watchtowers able to detect potential threats before they can cause large-scale damage
    - to focus on promoting a better use of the latest cybersecurity tools by SMEs – including, but not limited to, through dedicated activities under the DIHs;
    - to make a general effort to upskill the workforce, to develop, attract and retain the best cybersecurity talent as a way to invest in protection against cyber threats. In this respect, the Revised Digital Education Action Plan will raise cybersecurity awareness among individuals and SMEs.

On a more practical level, a key player is the EU Agency for Cybersecurity (ENISA), which has offered hands-on advice for SMEs, publishing:

- Tips for selecting and using online communication tools;
- Tips for cybersecurity when buying and selling online;
- Tips for cybersecurity when working from home;
- Top ten cyber hygiene tips for SMEs during covid-19 pandemic;
- Joint checklist for SME.

Private Level

Naturally, large companies are better equipped to deal with cybersecurity challenges. Different companies choose different solutions. For example, within the **Lufthansa Group[69],** cyber threats are addressed by way of:

[68] European Union: European Parliament and Council of the European Union (2020) *The EU's Cybersecurity Strategy for the Digital Decade,* 16.12.2020 JOIN(2020) 18 final

[69] Lufthansa Group, Website: Data Protection and Information Security. Available at: https://www.lufthansagroup.com/en/responsibility/product-customer/data-protection-and-information-security.html Accessed on: 24.3.2021

- Employee sensibilisation and targeted training: the Group Data Protection Commissioner plans and recommends training measures, and then ensures that training obligations are met;
- Constant monitoring of the global IT security situation: conscious that the Group's business processes are supported by IT components in almost all areas, and that these inevitably entail risks for the stability of business processes, as well as for the availability, confidentiality and integrity of information and data, the Executive Board monitors closely monitors all developments;
- A group-wide cyber security program through which new technological tools and processes are introduced and/or adapted to the changing threat situation;
- A Security Operations Centre (SOC) on duty 24/7 to protect and secure the IT infrastructure;
- A Computer Emergency Response Team permanently on standby to provide a rapid response in the event of a security incident or cyber-attack;
- Regular checks, also on external service providers.

On the contrary, **KBC Bank**[70], which operates across Europe through fully owned banks and insurance companies with a high level of local autonomy in its core markets, did not see fit to create a large centralised department to oversee its incident response process. As each of its various entities already had well-established, and largely autonomous, cybersecurity teams, it decided to coordinate these by relying on an external provider and implemented the IBM Security SOAR platform, which, amongst other things, provided playbooks for different incident types to enable consistent execution across the group.

Similarly, **Sodexo** chose to complement its internal efforts with Qualys Vulnerability Management (VM)[71], which delivers a complete range of functionality, including network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking prioritized by business-risk profile.

In conclusion, having established that almost all SMEs now require some online interaction for their business transactions and that this makes them a potential prey for cyber threats as much as large companies are, the question is whether the solutions implemented by large companies can be of any use to EU SMEs. Understandably, the first obstacle to the adoption of such solutions is represented by the limited number of resources SMEs have at their disposal. A second obstacle has to do with the complexity arising from the fact that businesses differ from one another because of the products and services they sell. Naturally, this can be overcome considering the trade-off between accuracy and efficiency. Another factor, however, needs to be taken into account and has to do with the fact that the type of cyber threats EU SMEs and EU large business face may be different in nature.

[70] IBM, Website: https://www.ibm.com/case-studies/kbc-group-security-soar Accessed on: 23.2.2021

[71] Qualys, Website: https://www.qualys.com/customers/success-stories/sodexo-securing-enterprise-automated-vulnerability-management/ Accessed on 23.3.2021

7.1.6. Policy Recommendations

The ENISA's 8th annual ENISA Threat Landscape (ETL) 2020 report[72] clearly states that "[cyber] attacks are continuously expanding by becoming more sophisticated, targeted, widespread and often undetected". The Covid-19 pandemic now raging across the continent makes this even more of a pressing issue. The European Union is showing responsive to this need and has taken a number of measures to counter such attacks over the past years. However, despite all the efforts, EU SMEs remain largely unprepared to tackle these threats, and the main reasons appear to be of both financial and cultural nature:

1. First, even though the average cost of cybersecurity incidents is proportionally higher for SMEs than large businesses[73], SMEs perceive cybersecurity as a costly endeavour. When they qualify for EU funding, the administrative burden related to applying and subsequent reporting that this entail acts as an obstacle because it requires resources and abilities that SMEs often lack[74].

2. Second, the business culture in SMEs often neglects cybersecurity. This human aspect of cybersecurity has drawn considerable attention in last few years and studies have sought a link between security behaviours and types of people (e.g. gender, personality), but evidence is too scarce to make meaningful predictions. In addition to this, many studies rely on self-report measures, which often do not align with actual behaviour, and the models used are limited. There is a clear need to advance our understanding of the human aspects of cybersecurity, as there is growing evidence that improving users' understanding of the threat posed by cybersecurity breaches, or fear of the consequences, is not an effective way to change behaviour.[75]

In any case, even if massive and targeted awareness campaigns were to be conducted, the EU would still be confronted with a shortage of cybersecurity professionals. In 2019, the Information Systems Audit and Control Association found that nearly 60% of organisations have unfilled cybersecurity vacancies and that two times out of three it takes a minimum of three months to fill a position[76]. Not only this, but the shortage of cyber experts also concerns academia and the civil society, who would be responsible for educational activities. Data from DESI 2020 confirm so, where southern and Balkan regions show a significant shortage of ICT experts and professional profile sable to tackle cybersecurity challenges for organisation.

This focus on the human component of cybersecurity should not shift the attention away from security itself. Security ought to be not too complex nor to effortful, as this is the main driver of insecure behaviour. As ENISA aptly points out, "security needs to fit into work processes and tasks rather than disrupt them", and "trying to 'fix the human' without fixing the system won't work alone."[77]

[72] European Union Agency for Cybersecurity (ENISA) (2020). *From January 2019 to April 2020: The year in review. ENISA Threat Landscape*, available here: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-enisas-list-of-top-15-threats

[73] Hiscox (2017). *The Hiscox Cyber Readiness Report 2017*. London, United Kingdom: Hiscox Group, 5

[74] European Union: European Economic and Social Committee (2018) Cybersecurity: Ensuring awareness and resilience of the private sectoracross Europe in face of mounting cyber risks. The Hague Centre for Strategic Studies

[75] ENISA (2018). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*

[76] ISACA. (2019). *State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development.*

[77] ENISA (2018). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*

Public policies can go a long way into addressing SMEs' unpreparedness, but since Member States differ greatly in terms of awareness, knowledge and ability to deploy strategies and programs pertaining to cybersecurity, there is a clear need for EU action to ensure that a level playing field is maintained within the EU single market. Countries like Estonia, France and Norway lead by example, but many others lag considerably behind, with Slovenia and Slovakia bringing up the rear.

To conclude, Cyber-MSMEs partners welcome the upcoming Slovenian Presidency of the Council of the EU priority on cybersecurity, and suggest policy makers focus on:

- Making cybersecurity investments affordable for EU SMEs, also by way of reducing the administrative burden that access to EU funds entails;
- Investments in resources to advance the current understanding of the human aspect of cybersecurity, so as to be able to design targeted measures that will trigger long-term behavioural change;
- Measures to reduce the complexity of security, so that this fits into work processes without major disruption;
- Envisaging measures to favour the participation of women and minority groups in STEM;

In its The EU's Cybersecurity Strategy for the Digital Decade[78] (2020), the European Commission analyses and reviews the measures implemented at European level and anticipates future developments in the cybersecurity domain. Despite the number of initiatives and a general awareness in the cybersecurity field, Europe has not yet reached a sufficient level of cooperation with national authorities. National authorities do not systematically collect and disseminate data that could help the EU to develop situational awareness. Currently, there is only a limited "mutual operational assistance" among member states: there is no "operational mechanism" among member states, EU institutions, agencies and bodies, capable of guaranteeing an effective protection and response scheme in case of large - scale and cross - border cyber - attacks.

In addition, the regulatory environment in the field of cybersecurity is fragmented. Cybersecurity is a challenge shared by all EU Member States, so there is a need to implement shared capacity to address risks and threats. The EU is faced with heterogeneous security regulations and several levels of cybersecurity maturity in the Member States: these are obstacles to an effective cross - border collaboration. It is crucial that future regulatory changes are the same in all Member States so that EU enterprises are not subject to different levels of security[79].

Ensuring a high degree of EU coordination to compensate for the differences in Member States' preparedness to deal with these challenges. In the light of the new situation created by the spread of the COVID - 19, a continuous updating of the workforce is necessary. The development not only of "hard" but also of "soft" IT skills can only be achieved by developing initiatives aimed at spreading awareness and knowledge on the basic IT skills to the general working population. Despite the presence of initiatives aimed at training MSMEs staff on cybersecurity issues, there is still a perceived need to align, through communication between education providers and MSMEs, professional needs with training outcomes.

[78] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade", 2020

[79] European Economic and Social Committee, "Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks", 2018, available at https://hcss.nl/sites/default/files/files/reports/Cybersecurity%20ensuring%20awareness%20and%20resilience%20of%20the%20private%20sector%20acrros%20Europe%20in%20face%20of%20mounting%20cyber%20risks.pdf

Furthermore, the global pandemic of COVID-19 has shown the importance of collaboration and coordination at global level also in the area of cybersecurity. The increasing awareness of enterprises on possible cyber threats has led cyber criminals to adapt their attack's schemes[80]. As described in the report "Emerging trends"[81] by ENISA (2020), cybercriminals are taking advantage of the pandemic: they are increasingly well-prepared and use more sophisticated tools. This result, which is a sign of a general response of the enterprises to cyber threats, also shows the need to constantly implement cybersecurity procedures and tools, adapting IT systems to new conditions.

The future workforce needs to possess both knowledge, skills and life-learning mindset to quickly adapt to market needs and technological advances. Elements that can train the future workforce in digital skills (i.e. logical thinking, critical analysis, coding and algorithms) require an adaptation of the current educational system[82].

7.2. Poland

7.2.1. Introduction

In today's world, effective protection of a company's IT systems, data and information is a critical element of ensuring a stable business. This holds true for big companies as well as MSMEs. This report will focus on the state of cybersecurity for MSMEs in Poland: it identifies the main cyber-threats that companies face, describes the level of awareness and preparedness to deal with these threats, highlights best practices introduced by the public and private sector and lists policy recommendations to mitigate risks that are currently not sufficiently dealt with.

In Poland, the government has identified the efficient and safe operation of information systems and means of electronic communication as a key factor in the growth of the Republic of Poland. The Cybersecurity Strategy of the Republic of Poland 2019-2024[83] states that 'any significant disruption to the functioning of cyberspace, whether global or local, will have an impact on economic activity, citizen's sense of security and safety, the efficiency of public sector institutions, production and service processes, and as a result on national security in general'. Therefore, the government designated the protection of information systems and information processes as a challenge for all entities of the national cybersecurity system, from businesses providing IT systems to public authorities and entities dealing with cybersecurity at the operational level. In its latest annual report, Security of Polish Cybersecurity 2019[84], CERT Polska, the Polish national computer emergency response team, indicated an increase in cyber-incidents in Poland. This highlights that managing cyber-risks – ensuring awareness, preparedness and the sharing of best practices- is of vital importance to all companies, big and small.

[80] INTERPOL, Global Assessment Report on COVID-19 related Cybercrime, 2020

[81] ENISA, "Emerging trends", 2020

[82] European Commission, "Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity for SMEs – interim report", 2019, available at https://www.digitalsme.eu/digital/uploads/March-2019_Skills-for-SMEs_Interim_Report_final-version.pdf

[83] Ministry of Digital Affairs (2019). Cybersecurity of the Republic of Poland for 2019-2024. Available at: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024.

[84] CERT Polska (2020). Security of Polish Cyberspace. Annual report 2019 on the activity of CERT Polska. Available at: https://en.nask.pl/eng/reports/reports/3835,CERT-2019-Report-PL.html.

7.2.2. Mapping out cyber-threats in Poland

Numbers on cybersecurity threats in Poland are reported on a yearly basis, with the latest available data covering the year of 2019. In its 2019 report, Security of Polish Cyberspace, CERT Polska reported that a gradual increase in the number of cyber incidents and reports has been observed for many years and that the year 2019 was 'record-breaking' in that respect. In 2019, CERT Polska analysed 22,343 reports and recorded a total of 6,484 cybersecurity incidents. This is nearly double the number of incidents (3,739) recorded in 2018. The most common type of attack handled by CERT Polska was phishing, constituting more than half (54,2%) of all incidents. Compared to 2018, the number of phishing incidents went up by 10 percentage points. The second most frequently reported incident related to malicious software incidents, encompassing 14,9% of incidents. Occupying third place as a proportion of the total number of incidents handled are incidents concerning illegal and abusive content including spam, accounting for 12,1% of the incidents. Compared to the previous year, an 88% increase in this category was observed. Table 1 lists the incidents handled by CERT Polska in 2019 by type.

Phishing

Two kinds of this type of scam were most popular among cyber-criminals, the first being Facebook phishing. Criminals pretended to be the owner of a Facebook account and sent private messages to the user's friends asking for transfer of money using the BLIK mobile payment system. The second most frequently reported phishing scam of 2019 consisted of criminals pretending to be PayU or DotPay quick payment providers, with criminals sending emails or SMS messages to random individuals on a mass scale with information about a payment to be completed, such as an additional fee for a parcel. When the victims filled out their banking login and password, scammers intercepted the data and gained access to the victim's bank account.

Malicious software

2019 witnessed a lot of campaigns attacking Polish users on a mass scale. The most common form was the distribution of emails containing fake invoices, documents or information, carrying the name of known companies and including files with a script, document or Internet address leading to malicious software.

Type of incident	Number of incidents	%
I. Abusive and illegal content, including:	812	12,5%
Spam	786	12,1%
Other	26	0,4%
II. Malicious software, including:	969	14,9%
Trojan	69	1,1%

Other	900	13,9%
III. Information gathering, including:	95	1,5%
Scanning	44	0,7%
Other	51	0,8%
IV. Intrusion attempts, including:	77	1,2%
Login attempts	29	0,4%
Other	48	0,8%
V. Intrusions, including:	160	2,5%
Unprivileged account compromise	39	0,6%
Other	121	1,9%
VI. Availability, including:	57	0,9%
Distributed Denial of Service (DDoS)	33	0,5%
Other	24	0,4%
VII. Information content security, including:	41	0,6%
Unauthorised access to information	20	0,3%
Other	21	0,3%
VIII. Fraud, including:	4086	63,0%
Phishing	3516	54,2%
Other	570	8,8%
IX. Vulnerable services, including:	102	1,6%
Open for abuse	8	0,1%
Other	94	1,5%
X. Other	85	1,3%
Total	6484	100,0%

Table 1: Incidents handled by CERT Polska in 2019 according to type. Source: CERT Polska (2019).

Illegal and abusive content (including spam)

The most commonly handled incidents in this category were so-called sextortion scams retaining to mass-distribution of email messages claiming that the sender possesses erotic content with the victim and demanding a ransom for deleting the content. Another variant of this scam contained blackmailing messages which included the victim's mobile phone number and PESEL, making the situation more credible in the eyes of the victim.

Incidents by economic sector

Table 2 shows the incidents handled by CERT Polska in 2019 according to economic sectors. Most of incidents were reported by individuals (18,7%). Wholesale and retail trade also constitutes a sector in which incidents are common (9,6%), often relating to cases involving a fake store. The media sector occupies a high place, involving frequent phishing attacks with the aim of stealing user's credentials to websites such as Netflix and Facebook. The banking sector (16,3%) faced a substantial number of attacks, mainly in the form of payments scams described previously. In terms of serious incidents, being those which could affect the availability of an essential service, CERT Polska recorded 9 incidents, with 6 in the banking sector and 3 occurring in the energy, healthcare, and digital infrastructure sectors.

Economic sector	Number of incidents	%
Individuals	1212	18,7%
Banking	1057	16,3%
Media	748	11,5%
Wholesale and retail trade	624	9,6%
Digital infrastructure	550	8,5%
Finance	500	7,7%
Other services	480	7,4%
Public administration	336	5,2%
Education	62	1,0%
Transport	61	0,9%
Healthcare	53	0,8%
Postal and courier services	49	0,8%
Production	46	0,7%
Construction and real estate management	31	0,5%

Energy	28	0,4%
Logistics and distribution	19	0,3%
Culture and protection of national heritage	9	0,1%
Hotels, restaurants, catering	9	0,1%
Tourism	8	0,1%
Water supply	5	0,08%
Insurance	5	0,08%
Physical culture	4	0,06%
Religious denominations and national minorities	3	0,05%
Agriculture	3	0,05%
Waste management	2	0,03%
Fishery	2	0,03%
Chambers of commerce and industry	0	0,0%
Other	578	9%
Total	6484	100%

Table 2: Incidents handled by CERT Polska in 2019 according to economic sectors. Source: CERT Polska (2019).

Effects of cyber-attacks

In 2017, 44% of Polish firms reported significant financial losses due to cyber-attacks. However, the effects of an attack are not only measured in financial terms. Another way to illustrate the effects are to show how the functioning of a company is inhibited by an attack. In 2017, 62% noted an interruption in their functioning, of which in 26% of the cases the interruption lasted longer than one work-day and 40% of attacks disrupted firms' operations for over three hours[85]. This has significant impact on companies, because during this time companies can be either fully excluded from or loss part of their key operations: client support, sales or production.

Other effects reported were leaks of client data (10%), lack of access to websites (20%), damage to reputation (18%), lack of access to email or other applications (16%) and id-theft of an employee or client (9%).

[85] PWC (2018). Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście. Available at: https://www.pwc.pl/pl/publikacje/2018/cyber-ruletka-po-polsku-5-edycja-badania-stanu-bezpieczenstwa-informacji-pwc.html.

7.2.3. The level of awareness of cyber-attacks

This chapter will outline how the most recent available research rates the awareness of cyber-attacks on big and small companies in Poland as well as which actions are undertaken to promote awareness and to which audiences they are directed. In the fall of 2017, PwC conducted an online survey among 127 Polish experts responsible for IT and information security to examine the level of awareness and preparedness of Polish business regarding cyber-threats. Of the surveyed professionals, 24% represented small companies, 35% mid-sized companies and 41% large companies. The top-5 business sectors among the respondents were technology (16%), production industry (16%), financial services (11%), telecommunication (10%) and the energy sector (8%).

Of those surveyed, 65% indicated that their companies had been confronted with cyber-incidents in the past 12 months. According to PwC this number is subject to underreporting, as especially in large companies cyber-incidents are a 'taboo' subject leading to its existence only being made known to a very selective group of employees.

Causes of security incidents	Mentioned by % of respondents
Fault of a user	41%
Use of data/information	24%
Faulty configuration of components	21%
Phishing attack	20%
Use of known programming vulnerabilities	18%
Use of an employee	15%
System faults	13%
Use of websites	13%
Use of applications	13%
Use of IT system	12%

Table 3: Causes of security incidents. Source: PwC 2018.

Table 3 shows the causes of security incidents as reported by the respondents. The majority of cases relate to a fault of the user or a known vulnerability in some form: a fault of the user (41%), faulty configuration of components (21%), use of known programming vulnerabilities (18%) and the use of an employee (15%). As for who is responsible for these incidents, 33% of the respondents list that the main source of cyber risks are current employees, 13% name former employees, 6% mention consultants or subcontractors, 2% name former suppliers and 28% point to hackers.

According to a 2019 report by Cyfrowa Polska[86] the awareness of cybersecurity risks relating to the use of communication devices (mobile and stationary phones) is limited, with most Polish firms indicating

[86] Cyfrowa Polska (2019). Cyberbezpieczenstwo w Polsce. Available at: https://cyfrowapolska.org/wp-content/uploads/2019/01/Raport_cyberbezpieczeństwo_2019.pdf.

that they believe primarily computers should be protected against cyber-attacks. When asked which devices should be protected according to Polish businesses, almost 90% of respondents named computers, almost 80% mentioned servers, and a little of 70% listed laptops, tablets and mobile devices. Only 20% of respondents report knowing that other forms of electronic devices should be protected, such as printers, even though printers are often the only device through which one could communicate with other work stations within a firm. This means that through a printer one could get access to content which for example is out of reach for lower employees. Moreover, while the majority of Polish employees declare that they are aware that their electronic devices used for professional purposes should be protected, only 40% in practice reports thinking about this and using the necessary protective mechanisms.

Another area in which there appears to be a lack of awareness is the knowledge of financial losses related to cyber-attacks. As mentioned in the previous chapter, 44% of Polish firms report significant financial losses due to cyber-attacks, while 40% noted a interruption in their functioning for over three hours[87]. While some attacks may indeed carry little financial effects, it could also be the case that respondents are either not aware of the financial costs or companies do not have the tools to adequately measure the financial losses associated to attacks.

Increasing the level of public awareness of cyber threats is one of the main aims of the Cybersecurity Strategy of the Republic of Poland 2019-2024[88]. In the strategy, the government states that, in cooperation with NGO's, academia and private sector, the public administration will continue with actions to raise public awareness of cyber threats. Among these are educational actions regarding the rights and freedoms in the digital environment and the rights of cyberattack victims. More information on the actions taken by the Polish government is included in chapter X on Best practices.

In a 2019 analysis of the psychological aspects of cybersecurity[89], NASK, the national Polish research agency for cybersecurity, highlighted that there is substantial difference between objective and subjective assessments of cybersecurity. Objective assessments rely on measurable, mathematical interpretations of the likelihood of risks occurring, while subjective assessments are based on psychological reactions and perceptions of risk and control. In the field of cybersecurity, users portray both unrealistic forms of subjective security as well as insecurity. For example, one can point at users completely resigning from the use of the electronic banking system due to a single incident on the one hand. More commonly however, users feel completely secure, for example when downloading illegal programs, although this both breaks the law and carries the risks of catching an infection with malicious software. This artificial feeling of security combined with the feeling of anonymity can lead users to break the rules meant to secure the use of electronic devices or systems.

7.2.4. Preparedness

This chapter will show how well Polish firms are protected against cyber-attacks, which actions companies undertake to mitigate cyber-threats and whether there are any blind spots witnessed in Poland that indicate that preparedness is not sufficient.

[87] PWC (2018). Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście.

[88] Ministry of Digital Affairs (2019). Cybersecurity of the Republic of Poland for 2019-2024.

[89] NASK (2019). Psychologiczne aspekty cyberbepieczeństwa. Available at: https://cyberpolicy.nask.pl/psychologiczne-aspekty-cyberbezpieczenstwa/.

When compared to firms globally (83%), Polish firms are less likely to see cybersecurity as a key element of the functioning of the company (58%). Activities in this area often limit themselves to the formal adherence to regulations, especially those concerning the protection of personal data[90]. While the attention to cybersecurity in Poland often focusses on the protection of personal data, over half the surveyed firms report that their preparedness to deal with the EU data regulations (GDPR) is below 30% of the desired level.

Overall, a 2019 report by PwC[91] shows that in Poland only 8 out of 100 firms are fully prepared for a cyberattack, meaning that they have sufficient IT security systems in place, a dedicated team of minimally 2 employees, that they dedicate at least 10% of their budget to investments in this area, that the board is regularly updated on this subject using reports and that there is a dedicated director or manager in place for cybersecurity. While many of these criteria are difficult to reach for micro-, small- and medium-sized companies, it is telling that even the majority of surveyed large companies (which made up 41% of the surveyed companies) don't manage to fulfil this target.

According to PwC, among many firms the conviction exists that cyber-threats will not affect them. Overall, one can observe a lack of preventative and protective action as well as a lack in willingness to share knowledge about attacks occurring to firms. More knowledge sharing across firms could help the victims to better tackle the aftermath of an incidents, as well as protect potential victims to future attacks. Of the Polish firms surveyed, 65% declare having a cybersecurity strategy in place, while 54% of firms claim to have a fixed process in place to respond to incidents. While having a strategy and a process prepared is valuable, because it allows for a systematic approach to tackling issues as well as the identification of concrete goals, it is important that these plans are also implemented in practice, which is not always the case.

When it comes to IT security systems put in place as protection, about half of firms report having introduced firewall protection, a web proxy for filtering movement, advanced protection against malicious programming or a next general of firewall. Of these security systems, the traditional firewall and intrusion detection systems are no longer seen as effective, unable to protect against common threats such as *Advanced Persistant Threats* or common phishing attacks.

IT security implemented in firms	Mentioned by % of respondents
Firewall application	53%
System to detect intrusions (IPS/IDS)	52%
Filtering movement WWW (web proxy)	51%
Advanced protection against malicious programming (sandboxing/antyAPT)	46%
Next generation Firewall	46%

Table 4: IT security implemented by firms. Source: PwC (2018).

[90] PWC (2017). Digital IQ 2017. Cyfrowy wyścig firm. Available at: https://www.pwc.pl/pl/publikacje/2017/digitaliq2017.html.
[91] PWC (2018). Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście.

Another weak point in terms of preparedness of Polish firms relates to having in place dedicated personal dealing with IT security. Of medium-sized and larger companies, 20% report not having any particular person responsible for IT security. A larger percentage, 59%, notes not having hired a manager or director responsible for IT security. This however is not only due to a lack of prioritizing IT security in firms, but also to the situation on the Polish labour market. In 2018, the lack of Polish IT personnel was estimated at 40-50.000 full time jobs, with cybersecurity experts being among the most sought-after experts.

7.2.5. Best practices

This chapter will provide an overview of best practices implemented by national or local programs to supports MSMEs in cybersecurity, more specifically listing what policies, measures and initiatives have bee implemented so far. This chapter relies heavily on the Cybersecurity Strategy of the Republic of Poland 2019-2024[92], which brings together a large array of public and private initiatives. These initiatives can be divided into five objectives:

- The development of the national cybersecurity system;

- Increasing the level of resilience of information systems of the public administration and private sector, and achieving the capacity to effectively prevent and respond to incidents;

- Increasing the national capacity in the area of cybersecurity technology;

- Building public awareness and competences in the area of cybersecurity;

- Building a strong international position of the Republic of Poland in the area of cybersecurity.

- To achieve these objectives, the Cybersecurity Strategy gave rise to initiatives with a predominant focus on education, research and public-private partnerships, several examples of which will be presented below.

Education

The Cybersecurity Strategy stresses that actions will be taken to increase the level of cybersecurity competences of research and higher education institutions. By means of legal instruments, the government will stir higher education institutions to provide cybersecurity teaching as part of first- and second-cycle studies, doctoral schools and post-graduate programmes. To enhance the competitiveness of Polish entrepreneurs on the global market, the government shall also support the development of digital competences of Polish business and ensure assistance in applying for funding of innovative solutions as well as assistance regarding access to new markets.

Examples of educational activities are:

Baza Wiedza (Knowledge Database)[93]: a free online portal offering information on a variety of issues relating to cybersecurity, targeted at individuals as well as employees and business owners. For example, this portal contains guidance on how work safely remotely, the security of videoconferencing tools, securing your mobile devices, among many others.

[92] Ministry of Digital Affairs (2019). Cybersecurity of the Republic of Poland for 2019-2024.

[93] https://www.gov.pl/web/baza-wiedzy.

Poradnik Bezpieczna Szkola[94]: a manual for schools on how to deal with cybersecurity relating to their students, buildings and equipment.

Szkolenia z dostepnosci cyfrowej [95]: free schooling for accessing the internet and operating online, aimed at civil servants and open to all interested parties. While not directly connected to cybersecurity, supporting general digital skills can have a positive effect on cybersecurity.

Schooling on cybersecurity for civil servants[96]: offered by the Department of Cybersecurity, aimed at three different levels: cyber-hygiene for all employees, cybersecurity for all IT employees and cybersecurity for IT specialists.

Research

Apart from educational activities, the Polish government supports the development of research programmes in cooperation with the scientific and academic community, aiming to assess the effectiveness of protections and resilience to cyber-threats and develop new methods of detecting new types of cyber-threats as well as measures to counteract these attacks.

Examples:

One main example of activities in this sphere regards the National Platform for Cybersecurity (NPC)[97], a research program led by NASK, a National Research Institute regarding cyberspace[98] and involving other parties – the Polytechnic of Warsaw, the National Center for Nuclear Research and the National Institute of Telecommunications.

NASK, being government-funded, itself also publishes a large number of publications on cybersecurity, including a yearly overview of cyber-incidents[99].

Public-private partnerships

The Polish government also supports collaboration between the public and private sector on the topic of cybersecurity. A key example of this is the PWCyber Cybersecurity Cooperation Program[100], a collaboration between the consulting firm PWC and the Polish Department of Cybersecurity, focusing on five topics:

- Enhancing public administration competences in the field of cybersecurity;
- Exchange of information on cyberthreats;
- Preparing recommendations on cybersecurity;

[94] https://www.gov.pl/web/edukacja-i-nauka/bezpieczenstwo-fizyczne-i-cyfrowe-uczniow--poradnik-men.
[95] https://www.gov.pl/web/dostepnosc-cyfrowa/o-szkoleniach-z-dostepnosci-cyfrowej.
[96] https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen.
[97] https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/2088,Narodowa-Platforma-Cyberbezpieczenstwa-NPC.html.
[98] https://en.nask.pl.
[99] CERT Polska (2020). Security of Polish Cyberspace. Annual report 2019 on the activity of CERT Polska.
[100] https://www.gov.pl/web/cyfryzacja/wzmacniamy-wspolprace-w-ramach-programu-pwcyber.

- Preparation and conduct of cybersecurity assessment and certification;

- Disseminating information on innovations in cybersecurity.

This program builds on a few basic assumptions: it's non-binding, voluntary nature, the lack of financial commitments, a confidentiality clause for designated information and the possibility of other partners joining. A number of concrete activities include:

- Sharing and developing training materials to improve the skills of user and staff responsible for cybersecurity;

- The organization of trainings and workshop events;

- Conducting awareness-raising campaigns, organizing competitions on best practices in the use of products and services that enhance cyber security;

- Companies that joined PWCyber include a range of global IT companies such as Cisco, Ericsson, Nokia, Samsung and DELL as well as Krypton Polska and Dynacon, two Polish companies.

7.2.6. Policy recommendations

Overall, a lack of awareness and preparedness of cybersecurity risks can be observed among Polish companies, with only 8% of companies deemed to be sufficiently prepared. This report highlights a number of lessons that can be used to improve policy in the field of cybersecurity, in particular relating to MSMEs.

Lesson 1: Offer more training to employees and business relations.

Many of the cyber-threats witnessed by companies could have been avoided by better training or management of employees, since the majority of threats are caused by either own employees of companies or individuals working with the companies as suppliers or consultants. Only 28% of the threats are reported to be caused by hackers. In other words, the real threat is often internal.

Lesson 2: Introduce better measurement of the financial losses related to cyber-threats.

This report shows that companies may underestimate the financial losses of cyber-incidents, possibly because IT experts do not have the means to accurately measure them. One proxy that could be used is the number of hours that a cyber-incident induced an interruption in business operations, such as sales and customer support. Once companies measure the financial losses more carefully, the real cost may become visible, motivating them to take actions in mitigating these risks in the future.

Lesson 3: Share information about cyber-risks among companies:

Companies appear hesitant to share information about cyber-incidents occurring to them with other companies and even within companies, with only a very select group of employees being informed about incidents occurring. This may lead to a false sense of safety among employees and works against companies and employees learning from each other how to prevent future attacks.

Lesson 4: Pay attention to securing electronic devices other than computers, such as printers:

The majority of Polish companies have the impression that cybersecurity mostly related to computers, with only 20% indicating that other devices such as printers can pose a significant risk. This constitutes a blind spot in the awareness of cybersecurity risks.

Lesson 5: Make use of more advanced protection measures:

There are indications that too many companies use traditional protection measures such as older generation Firewall systems or intrusion detection systems. These are shown not to bee effective against risks like phishing attacks, which constitute the main form of cyber-threat.

Lesson 6: Include small-, micro- and medium-sized companies in the activities falling under the Cybersecurity Strategy of the Republic of Poland:

The Polish government, in cooperation with the private sector, has initiated a large number of activities to increase awareness of and preparedness for cybersecurity. While highly useful, these initiatives focus mainly on government employees or larger, mainly globally operating, companies. In particular, the sharing of training material and organizing workshops and competitions could be extended to MSMEs. In addition, more research could be supported among MSMEs, to uncover the specific risks that smaller- and medium-sized companies face.

7.3. Romania

7.3.1. Introduction

Romania, as a full member of both NATO and the EU, is playing an increasingly important role in cybersecurity and cyberdefense, both regionally and internationally. Romania promotes an open and competitive national information and communication technologies market that works hand in hand with the public cybersecurity structures.

The evolving of the cyber environment generates development opportunities for the information society, but also risks to its functioning. The existence of vulnerabilities of information systems, which can be exploited by organized groups, makes the security of cyberspace a major concern for all the entities involved. At European level, several steps have been taken to adopt new policies against cybercrime and to ensure the cybersecurity. The Directive on security of network and information systems (NIS Directive)[101], adopted by the European Parliament and the Council of the European Union on July 6, 2016, entered into force in August the same year, and benefits from a 21-month period to be implemented by Member States. The objective of the NIS Directive is to ensure a high common level of networks and information systems security in the EU and it requests essentials service operators and digital service providers to adopt appropriate measures for risk management, and to report serious security incidents to the competent national authorities. For implementation of the NIS Directive by the autumn of 2018, Romania has the obligation to set up competent national authorities, single points of contact and intervention teams in the event of cybersecurity incidents, and to establish the security requirements and incident notification to be applied to essential service operators and digital service providers. At national level, the Cybersecurity Strategy of Romania was adopted in 2013, with the aim of defining and maintaining a secure cyber environment with a high degree of safety and security. This strategy aims to adapt the normative and institutional framework to dynamics of threats

[101] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

of the virtual environment, to set and apply minimum security requirements for national cyber infrastructures, to ensure their resilience and to develop cooperation at national and international level.

Achieving the cybersecurity strategy underpins the coordination of action plans aimed at ensuring cybersecurity, cooperation between all entities involved, both public and private sector, prioritization of national critical infrastructures securing and dissemination of information, expertise and good practice in order to protect cyber infrastructures.

The evolution of organized crime in Romania in the recent years is closely linked to the evolution of cybercrime and the increasing use of information and communication technology in committing offenses. The development of the cybercrime phenomenon in Romania is manifested under several aspects:

- The increase of the number of registered cases regarding cybercrime;

- Preoccupation of offenders to identify new modes of operation;

- Reorienting criminal groups to cybercrime.

In Romania cybercrime is manifested under the following aspects: cyberattacks that aim to compromise various networks and computer systems through multiple ways and tools (malware, ransomware, DDoS or defacement attacks), computer fraud, consisting of fictitious goods auctions, compromising users' accounts on e-commerce sites, or creating phishing sites for collecting bank data and credit card fraud, consisting of compromising ATMs and extracting confidential information from customers' cards.

Romania adopted the Cybersecurity Strategy in 2013, with a common approach at the level of the European Union, in order to provide a prompt response to the cyber-attacks. The purpose of Romania's cybersecurity strategy is to define and maintain a safe cyberspace with a high degree of resilience and confidence. This strategy presents the main principles and directions for action to prevent and combat vulnerabilities, and threats to the cybersecurity of Romania.

The main objectives set by Romania's cybersecurity strategy are:

- Adapting the normative framework to the new threats present in the cyberspace;

- Substantiating and applying the minimum-security requirements for protection of national cyber infrastructures;

- Ensuring the resilience of cyber infrastructures;

- Carrying out information and public awareness campaigns on threats and cyber risks;

- Developing cooperation between the public and private sectors at national and international level.

In order to ensure normality in the cyberspace of Romania, cybersecurity strategy focuses on the following directions:

- Establishing a conceptual, organizational and action framework to ensure cybersecurity. To establish this framework, a National System of Cybersecurity is set up, there is established a minimum set of security requirements for national cyber infrastructures and cooperation between the public and private sectors is developed, for the mutual exchange of information in the field of cybersecurity;

- Developing risk management and response capabilities to cyber incidents at national level. These capabilities are developed by implementing an early warning and alert mechanism on the event of cyber-attacks through increasing the resilience of infrastructures, by developing CERT-type structures and by stimulating cybersecurity research and development activities;

- Promoting cybersecurity methods. Within this direction, there are developed awareness programs of the human factor regarding the vulnerabilities, threats and risks present in the virtual space, the development of educational programs on the safe use of computing equipment and training of persons working in the field of cybersecurity;

- Developing cooperation on cybersecurity. In this respect, it is aimed at the conclusion of international cooperation partnerships in case of ample cyberattacks and participation in international events and conferences in cybersecurity.

The purpose of Romania's cyber security strategy is to define and maintain an secure virtual environment, with a high degree of resilience and confidence, based on national cyber infrastructures, which would constitute an important support for national security and good government, to maximize the benefits for citizens, businesses and the Romanian society as a whole. Romania's cyber security strategy sets out the objectives, principles and major directions for action for understanding, preventing and counteracting cyber security threats, vulnerabilities and risks and to promote Romania's interests, values and national objectives in cyberspace. To ensure coherence and actionable efficiency, the strategy seeks to achieve the national security target concerning "achieving cyber security", while respecting the principles and characteristics of the National Defense Strategy and National Strategy for the protection critical infrastructure.

For ensuring Romania's cyber security, the strategy sets the following objectives:
a) adapt the regulatory and institutional framework to the cyberspace threats dynamics;
b) establish and implement security profiles and minimum requirements for national cyber infrastructures, relevant in terms of the proper functionality of the critical infrastructures;
c) ensure the resilience of cyber infrastructure;
d) ensure security through understanding, preventing and fighting vulnerabilities, risks and threats to cyber security of Romania;
e) take advantage of the opportunities to promote the national interests, values and objective in the cyberspace;
f) promote and develop cooperation between the public and private sectors at national and international level in the field of cyber security;
g) develop a security culture by raising awareness of the population concerning the vulnerabilities, risks and threats originating from cyberspace and the need to ensure protection of their information systems;
h) active participation in the initiatives of international organizations which Romania is part of in defining and establishing a set of international confidence-building measures concerning use of cyberspace.

7.3.2. Mapping out cyber-threats in Romania

1. Threats, vulnerabilities and risks

Specific threats to cyberspace are characterized by sharp asymmetry and dynamics and a global nature, which makes them difficult to identify and counter through measures proportional with impact risks materialize.

Romania is currently facing threats to its critical infrastructure, originating from cyberspace. This is due to an increasing interdependence between cyber infrastructure and infrastructure such as that belonging to banking, transport, energy and national defense sectors. The globality of cyberspace is likely to increase the risks affecting both citizens, businesses and the government.

In general, cyber infrastructures may be affected by technical threats (i.e., deficiencies or technical failures), human threats (i.e., operating errors, actions voluntary) or natural threats (i.e., extreme weather, natural disasters).

Threats to cyberspace can be classified in several ways, but the most commonly used are those based on motivational factors and impact on society. In this regard, we can consider cybercrime, cyber terrorism and cyber war, having as source both state actors and non-state actors.

Threats from cyberspace materialize - by exploiting vulnerabilities of human, technical and procedural nature - most often in the form of:

- cyber attacks against the infrastructure supporting public functions or information society services, whose disruption or damage could constitute a danger to the national security;
- unauthorized access to cyber infrastructures;
- modification, deletion or deterioration of computer data or unauthorized illegal restriction of access to such data;
- cyber espionage
- causing patrimonial damage, harassing and blackmailing individuals and businesses, public and private.

The main actors who create threats in cyberspace are:

- persons or organized crime groups that exploit cyberspace vulnerabilities to obtain property or non-property benefits;
- terrorists or extremists who use cyberspace to conduct and coordinate terrorist attacks, communication activities, propaganda, recruitment and training, etc. fundraising for terrorist purposes;
- state or non-state actors which initiate operations in cyberspace, with the purpose of intelligence gathering in the governmental, military, economic fields or of ensuring the materialization of other threats to national security.

2. Opportunities

At the same time, cyberspace, which became a new area of interaction within modern society, offers a number of opportunities generated by its very specificity. Thus, the following opportunities which Romania can take advantage through cyberspace of have been identified:

- Supporting policies and promoting the national interests;
- Developing and supporting the business environment;
- Improving the quality of life through the development of the information society services;
- Improving knowledge and the support for national policy decisions in the Information age through ensuring adequate cyber capabilities and tools;
- Increasing knowledge and prediction capacity for early warning of national security risks and threats;
- Increasing technical capacity and human resource skills to achieve national security objectives.

SME cybersecurity statistics for 2020

The ongoing global pandemic of COVID-19 is changing things for small businesses and organizations around the world. An August 2020 INTERPOL report indicates that small companies cannot (currently) be the main target of cybercriminals: "In order to maximize financial damage and gain, cybercriminals move their target from individuals and small companies to large corporations. , governments and critical infrastructure, which play a crucial role in the pandemic response. At the same time, due to the sudden and necessary global change in teleworking, organizations have had to rapidly implement systems, networks and applications for remote work. As a result, criminals take advantage of the increased security vulnerabilities that result from working remotely to steal data, generate profits and cause disruption. "

But just because larger organizations are their main targets does not mean that SMEs should also let their guard down. Many types of cyber attacks and other dangers still pose a risk to small and medium-sized businesses.

1. $ 7.68 million: the average cost of an internal cyber incident for SMEs

Well, that figure definitely starts this list with an explosion. The costs associated with the impact of internal threats vary greatly depending on the size of the organization and the purpose of the attack. Research conducted by IBM and the Ponemon Institute in The Cost of Insider Threats Global Report 2020 shows that small organizations (those with fewer than 500 employees) spend an average of $ 7.68 million on each such incident.

2. 43% of SMEs lack any type of cyber security defense plans

What if I told you that more than two out of five companies in the US and the UK that have 50 or fewer employees do not have any kind of cyber security defense plan? Yes, that's right. A January 2020 study by BullGuard shows an annoyingly large number of companies choosing to be reckless. In essence, they risk massively securing their data and that of their customers.

3. One in five SMEs does not use any security protection for end-users

The Bull Guard's study of 3,083 SMEs shows that 23% of small businesses in the UK and US neglect the use of security mechanisms for end-users. In addition, 32% of respondents who use endpoint security protections state that they rely solely on free consumer-level cyber security solutions.

4. 60% of SMEs ignore the risks of attack and security breaches

Additional data from the BullGuard survey still takes us away from our hope for the future of some SMEs. Despite the fact that almost one in five (18.5%) small companies face cyber attacks or data breaches, 60% of SME owners surveyed believe that their business is not a likely target of cybercriminals.

However, if you read virtually any recent cyber security reports or articles, you would know that no company is "too small" or "too big" for a cyber criminal not to be interested in it. Like a modern version of Goldilocks, it would have no problem trying to defend each company's cyber defense to find a "correct" target.

Paul Lipman, CEO of BullGuard, says: “Small businesses are not immune to cyber attacks and data breaches and are often specifically targeted because they often fail to prioritize security. Trapped between inadequate consumer solutions and overly complex enterprise software, many small business owners may be inclined to bypass cybersecurity. However, it takes a single attack to bring a business to its knees. "

It seems that many SMEs are too confident in the security of their data and their organizations as a whole. Although we have not reached the level of the "ostrich strategy" here too much, we are sure that we are getting closer.

5. 28% of the data breaches reported in 2019 involved victims among small companies

Nearly one in three data breaches included in the Verizon 2020 Data Breach Investigations Report (DBIR) calculations involved small businesses. This means that these organizations need to do more to protect not only their digital assets and web presence, but also to protect the security and privacy of their customers.

Wondering if 28% is a good value? Well, it's not great - it's 28% too big, if you ask us! - but it is still better than before. This number is down from 43% for data breaches for SMEs, reported by Verizon in the 2019 DBIR.

6. Phishing is a major threat to more than 30% of small organizations

Phishing has been the main enemy of SMEs for several years - and this year is no different. The 2020 Verizon DBIR report shows that phishing is the most important threat, followed by the use of stolen credentials and password extraction.

7. 85% of MSPs report ransomware as the biggest malware threat for SMEs in 2019

In the Global State of the Channel Ransomware Report, Datto reported that four out of five Managed Service Providers (MSPs) identified ransomware attacks as the most important malware threat to SMEs. But there seems to be a significant difference of opinion regarding the threat of ransomware attacks: "89% of MSPs are 'very concerned' about the ransomware threat and 28% say their SME customers feel the same way." . This is despite the fact that one in five SMEs reported being the victim of a ransomware attack.

8. 63% of SMEs report that they have suffered a data breach in the last 12 months

Data from a 2019 study by Keeper Security and Ponemon Institute show that the number of small and medium-sized companies that suffered data breaches increased to 63% in fiscal year 2019. In the previous two fiscal years, participants reported 58% in fiscal year 2018, respectively 54% in fiscal year 2017.

9. 46% of SMEs with less than 1,000 employees had 5-16 hours of downtime related to data breaches in 2019

Cisco 2020 CISO Benchmark Study report data indicates that downtime due to data breaches is an issue for all organizations with up to 10,000 employees. According to their data (as cited in the Cisco report "Securing What's Now and What's Next"), small and medium-sized organizations with 250-449 employees reported the following:

- 43% experienced 0-4 hours of downtime,
- 45% experienced 5-16 hours of downtime and
- 12% experienced 17-48 hours of downtime.

10. 47% of SMEs report that keeping data safe is the biggest challenge

The results of the VIPRE SMB Security Trends survey indicate that almost half of CISO and IT professionals surveyed consider data security to be the biggest challenge to IT security. The next major obstacles they identified include preventing data loss (42%) and raising awareness of employee safety (41%).

11. 70% of SME employees' passwords were stolen or lost

Seven out of 10 employees were victims of password theft, according to 2019 data from Keeper Security and Ponemon Institute. We hope that those companies have had at least access control policies to limit the potential impact of such compromised credentials, but we have good reason to doubt it. Here's why…

12. Credentials (52%) represent the most compromised type of data in 2019

Compromised credentials continue to be an issue for both SMEs and other types of companies. The 2020 Verizon DBIR report reports that more than half of small businesses reported compromised credential issues in 2019. But who says Verizon is responsible for these attacks on small businesses?

13. 74% of SME data gaps involve external actors

By far, the vast majority of data breaches targeting small businesses in 2019 were committed by external threats, according to Verizon DBIR 2020.

14. 83% of data breaches against SMEs are financially motivated

Verizon DBIR 2020 data indicates that nowadays, most cybercriminals target primarily cryptocurrencies and fraud by phone, fax, e-mail, text, or social media. To put it simply, eight out of 10 data breaches are financially motivated. The other reasons they notice for the reason why cybercriminals launch cyber attacks on small businesses or commit data breaches are:

- Espionage (8%),
- Fun (3%) and
- Resentments (3%).

15. 22% of SMEs switch to remote work without a cybersecurity threat prevention plan

We live in a time when the global pandemic COVID-19 has forced the hands of companies around the world to allow employees to work from home at unprecedented rates. But what does this mean for small business cyber security preparations? Research by Alliant Cybersecurity shows that one in five small companies have started working remotely without a clear cyber security mitigation or prevention policy.

Now, consider that more than half (52%) of these SMEs indicate that they did not regularly allow their employees to work remotely before the pandemic. Given this, it is easy to imagine what kind of Pandora's box opens in terms of vulnerabilities and cybersecurity risks.

Unfortunately, what makes matters worse are the findings from the aforementioned Keeper Security / Ponemon Institute survey. Their data show that 39% of respondents to the SME survey report that their organizations do not have incident response plans. So this means that when (not if) the mess proverbially hits the cooling system, they won't have a plan to help them respond to cybernetic events.

7.3.3. The level of awareness of cyber-attacks

Why SMEs are believed to be more vulnerable to cyber attacks and data breaches

Small companies are the engines of the economy. For example, the latest data from the US Small Business Administration (SBA) reports that there are 31.7 million small businesses registered. In addition, a significant part of the country's workforce includes 60.6 million employees in small businesses.

Historically, there has been this common notion that small companies are at greater risk for cybercrime because they do not have the resources - funds, staff, time, etc. - to properly monitor and mitigate cyber threats. However, the findings of Verizon DBIR 2020 indicate that the gap between SMEs and larger organizations may be somewhat closed in terms of detecting security incidents and their responsiveness. This is partly due to the increasing use of the cloud, software as a service (SaaS) and other modern resources available by SMEs.

Unfortunately, for consumers, some business owners and executives are still convinced that their business is too small to be of interest to hackers. As you read earlier, this direct approach is the case for companies that have experienced cyber attacks and data breaches in the past! This means that they may not put their time, money, training and other resources in place to protect their business and therefore their customers.

7.3.4. Preparedness

Romania aims at ensuring of normality and reducing the risks in cyberspace seizing opportunities by improving knowledge, capabilities and mechanisms decision. In this regard, efforts will focus on the following directions:

1. Establishing the conceptual, organizing and actional framework required for ensuring cyber security:
- constituting and operationalizing a national cyber security system;
- completing and harmonizing the national legal framework in the field, including setting up and appling minimum security requirements for national cyber infrastructures;
- developing cooperation between the public and private sector, including through stimulating reciprocal information exchange concerning threats, vulnerabilities and risks, as well as cyber incidents and attacks.

2. Developing national risk management and reaction capabilities in the field of cyber security, based on a national programme and including the following aspects:

- consolidating, at the level of competent authorities, the potential of understanding, preventing and countering threats and minimizing risks associated with making use of the cyberspace;
- ensuring tools for developing public-private cooperation in the field of cyber security, including for the purpose of creating efficient early warning, alert and response mechanisms concerning cyber incidents;
- stimulating research, development and innovation capabilities in the field of cyber security<
- increasing the resilience level of cyber infrastructures;
- developing CERT-type entities in both the public and private sector.

3. Promoting and consolidating the security culture in the cyber field
- Development of awareness raising programs at the levels of the population, public administration and
private sector concerning threats, vulnerabilities and risks specific to the use of cyberspace;
- Development of educational programs, within the compulsory education cycles, concerning the safe use of the internet and computing equipment;
- Appropriate professional training to people working in cyber security and the widespread promotion of professional certifications field;
- The inclusion of elements relating to cyber security in the professional training programs for managers in the public and private sectors.

4. Develop international cooperation on cybersecurity
- Concluding agreements of international cooperation to improve response capacity in the event of major cyber attacks;
- Participation in international programs in the field of cyber security;
- Promoting the interests of national cyber security cooperation formats to which Romania is a party.

Cyber attacks on small businesses are not cheap - IBM reports that only the costs associated with incidents of internal threats amounted to an average of $ 7.68 million. Here is a list of the most important SME cybersecurity statistics for 2020 that you need to know.

You may have heard the cyber security statistics of small companies, often quoted, which are something like "60% of small companies that suffer a cyber attack stop working in six months".

7.3.5. Best practices

How to protect your business from cyber security attacks on SMEs

Creating a cyber attack protection system is not just an option, but a necessity to maintain the vitality and profitability of your business, and in this regard you will first need to make a number of investments.

To create multi-layer protection you need to consider some solutions and methods that should be used, including:

- Firewalls, antivirus and security solutions for end users
- Network penetration testing
- Cyber security audits
- Computer, device, and password usage policies
- Policies and procedures for access management and control
- Email security solutions (such as anti-phishing solutions, spam filters, email signing certificates)

- Training of employees in the field of cyber security and phishing simulations
- Disaster response and disaster recovery plans
- Current data backups

But what are some of the most common defense methods that SMEs implement? According to a recent survey by The Manifest: "The most popular cybersecurity measures for small businesses include limiting employee access to user data (46%), data encryption (44%), imposing strong user passwords (34%) and training employees on data security and best practices (34%). ”

7.3.6. Policy recommendations

Romania undergoes a continuous process of strengthening cybersecurity nationwide, both from a legal, institutional, and procedural point of view, and efforts are being made by the authorities with responsibilities in this field.

Ensuring the cyber security is based on cooperation at national and international level to protect cyberspace by coordinating the actions of national guidelines and measures at international level in cooperation formats to which Romania is a party.

Given the dynamism of global developments in cyberspace and our objectives in the development of the information society and implementation of large-scale electronic services, it is necessary to develop a national program in detail, which - based on benchmarks provided by this strategy - to ensure development and implementing concrete cybersecurity projects.

It is necessary to implement at national level the minimum standards of procedural and cyber security infrastructures, to substantiate the effectiveness of the actions protection against cyber attacks and to limit the risk of incidents with significant potential impact.

The current legislative regulations, as well as the degree of their operationalization at the level of the Romanian public institutions, currently do not allow the prevention and countering of medium and high-level cyber threats with maximum efficiency. Strengthening the legislative framework in the field of cybersecurity is a national priority, so that optimal conditions for rapid response to cyber incidents can be ensured.

In 2016, Romanian National Computer Security Incident Response Team collected and processed 110,194,890 cybersecurity alerts, with 61.56% more than in 2015 and 154.89% more than 2013. In addition to the growing number of cybersecurity alerts, we can see that the most common forms of malware in Romanian computer systems were detected many years ago and, although they hould have been eradicated, they continue to infect old and outdated operating systems in Romania.

Romania is a cybersecurity incident generator, with a transit (proxy) role for attackers, according to CERT-RO annual reports, but it has also become lately a target of APT, DDoS or ransomware cyber-attacks.

The Global Cybersecurity Index 2017 has as a modeling approach 5 strategic pillars on cybersecurity, namely: legal/judicial, technical, organizational aspects, capabilities, and cooperation. From the point of view of the country index, Romania needs the following:

- Updating the regulatory framework;
- Developing / adopting standards for organizations;
- Adopting security assessment metrics;
- Improving the legislative framework for vocational training, research and development programs, startups;
- Signing bilateral and multilateral agreements.

Many of the cyber defense systems used by critical infrastructure operators in Romania are outdated and ineffective to avoid or counteracting possible attacks. In the absence of adequate measures and coordination of critical infrastructure security efforts, these systems remain extremely vulnerable, unauthorized individuals being able to gain control over vital systems for the functioning of a state. In this respect, it is absolutely necessary to periodically analyze, monitor, assess and optimize the critical infrastructure domain by starting a process of identification of critical infrastructure at the level of public administration.

The rapid evolution of the domain and of the various vital sectoral components requires the updating of the national strategy on the protection of critical infrastructure, in accordance with the European and international recommendations in the field.

In the general context of discussions on cybersecurity at the national level, we highlight the importance of a conceptual separation of the main directions of action: cyber defense, cybercrime, national security, critical infrastructure and emergencies, international cyber diplomacy, and Internet governance. It is necessary to clearly define the roles and responsibilities of each responsible national institution.

Another segment requiring to be developed is the professional training in the field and taking of actions on awareness/understanding of the field at the level of the decision makers within the public organizations.

Research and education in the field of cybersecurity must be priorities of public policies. Strengthening information security research, improving education, and developing trained workforce are essential to achieving the overall cybersecurity policy objectives. Research and education policies will be effective only if they include the multilateral and multidisciplinary nature of cybersecurity as a fundamental and ubiquitous element in culture, approaches, technical systems, and infrastructures.

International cooperation plays a key role in this area, as cybersecurity challenges go beyond boundaries, extending to globally interconnected systems. Collaboration with European and international entities is absolutely necessary, whether it is about educational establishments, research centers, private companies or government institutions. Cooperation between institutions, organizations and the cybersecurity community can be useful in finding and fixing vulnerabilities. A proven cooperation mechanism is, for example, the coordinated disclosure of vulnerabilities.

The adoption of coherent public policies at Member State level on coordinated disclosure of vulnerabilities and coordinated cross-sectoral action/cooperation mechanisms will provide the necessary ecosystem to ensure the security of the community.

The opening of communication channels, the setting up of working and public consultation groups, the involvement of civil society and the public-private partnership are key directions that public policies should focus on.

In conclusion, the adoption of comprehensive and updated cybersecurity legislation to support the development of state defense capabilities is a national priority. Ensuring a secure cyberspace is the responsibility of both the State and the competent authorities, the private sector and civil society. For the development of the cybersecurity culture, the most important levers are: education and research, public-private partnerships, and cooperation mechanisms at the European level.

7.4. Spain

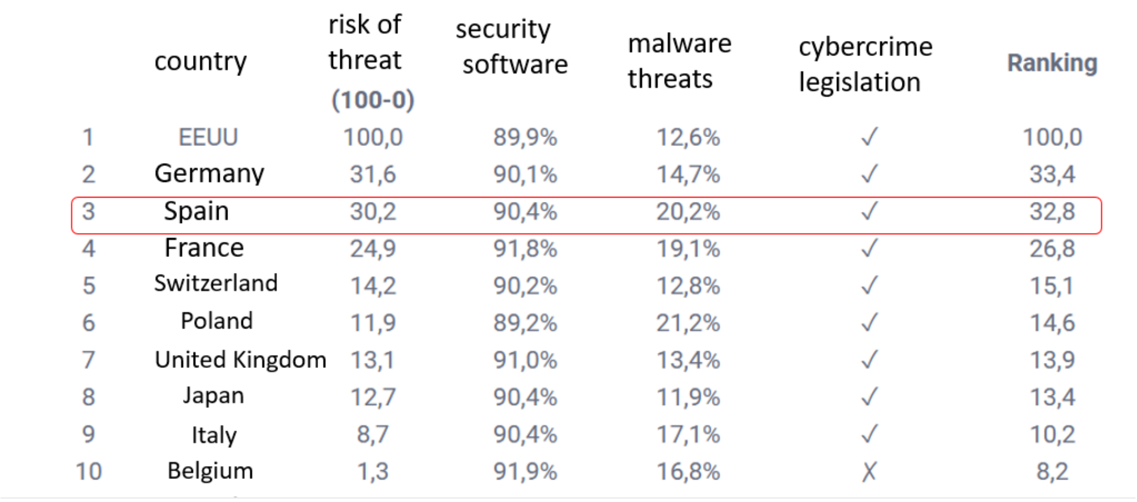
7.4.1. Introduction

Cybersecurity and the protection of businesses of all types and sizes from cyber-attacks have become a top priority worldwide. In Spain, cyber-attacks cause significant damages daily, some of which are irrecoverable. These cyber-attacks target large corporations and SMEs, and micro-enterprises, which are more fragile because they do not have the infrastructure, resources, or staff specialised in protection against cyber threats and because the average Spanish businessman is not very aware of the danger. The Spanish State Security Forces and Corps recorded a total of 218,302 alleged criminal acts related to or committed through information and communication technologies (ICT) in 2019.

The figure, 80% of which corresponds to fraud, represents an increase of 35.8% concerning the cybercrimes detected the previous year. The data given comes from the Statistical Crime System (SEC) compiled in the 7th Report on Cybercrime[102] produced by the State Secretariat for Security. Out of the 218,302 known potential cybercrimes in 2019, 88.1% (192,375) are digital fraud. The data recorded during the 2016-2019 historical series show that cybercrime is a phenomenon in constant growth in Spain, as highlighted in the study. COVID-19 has confined most Spanish population, causing increased web traffic for personal reasons (leisure, communication and entertainment) and work (teleworking and videoconferencing). In this context, cyber-attacks in Spain have increased by 125% in the last year.

7.4.2. Mapping out cyber-threats in Spain

In terms of cyber-threats, in Spain, there are no differences between the main cyber threats highlighted in the European context. However, the peculiarity of Spain that we can highlight is the frequency of attacks. We can highlight a higher number of cyberattacks in comparison with other EU countries. In that sense, the research published by Ironhack: "Analysis: the countries most threatened by cybercriminals and hackers in 2020"[103], highlights Spain as the third most attractive country in the world for cybercriminals. Spain is only behind the United States and Germany.



	country	risk of threat (100-0)	security software	malware threats	cybercrime legislation	Ranking
1	EEUU	100,0	89,9%	12,6%	✓	100,0
2	Germany	31,6	90,1%	14,7%	✓	33,4
3	Spain	30,2	90,4%	20,2%	✓	32,8
4	France	24,9	91,8%	19,1%	✓	26,8
5	Switzerland	14,2	90,2%	12,8%	✓	15,1
6	Poland	11,9	89,2%	21,2%	✓	14,6
7	United Kingdom	13,1	91,0%	13,4%	✓	13,9
8	Japan	12,7	90,4%	11,9%	✓	13,4
9	Italy	8,7	90,4%	17,1%	✓	10,2
10	Belgium	1,3	91,9%	16,8%	✗	8,2

[102] http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b

[103] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

In terms of threats, email is the leading vehicle for attacks. Phishing is the favorite cyber threat of cybercriminals. According to the analysis carried out by S21sec's intelligence team[104], Spain is the world's leading country in receiving emails with malicious content. Our country has received 8.38% of the world's total amount of cyber-attacks with malicious emails, attachments or links.

Cyber-attacks against companies worldwide and, in particular, those carried out in Spain, have increased exponentially during the past year 2020. The need to use telework formats due to the pandemic situation without adequate security measures or the absence of a solid security culture among employees is an opportunity that cybercriminals are not letting pass. Email is the primary means of attack. Phishing (fraudulent emails that impersonate companies and public bodies) is a favourite cyber threat for cybercriminals. An analysis carried out by the company S21sec on the evolution of phishing during the first half of 2020 confirmed that phishing increased by 350% compared to 2019.

Phishing is the most popular type of cyber-attack in Spain. These emails often contain attachments infected with malicious software (malware). Cybercriminals impersonate both government agencies and private companies to get hold of victims' data or take control of their computers. It should be the best known of the threats, but the figures put Spain as the third most frequent recipient of this type of fraudulent messages in the world. So we can conclude that awareness is not very high or that the level of awareness of these dangers does not always correspond to the way people act.

Ransomware and Double Extortion Ransomware:

Ransomware is a computer virus hidden inside another file or program that blocks access to information. Recently, it has evolved significantly and now uses a new attack modality known as "double extortion". Cybercriminals extract files before encrypting computers and threaten to publish them on the dark web if a ransom is not paid. Hospitals and institutions related to the medical sector have become the primary target, mainly due to the large amount of sensitive data they store with a low level of protection, which, coupled with the healthcare crisis, left them unprotected.

Ransomware is one of the cyber-attacks that most affects companies and puts their data and business continuity at risk (53% of Spanish companies were victims of a ransomware attack during 2019). In Spain, ransomware is considered a threat to large corporations. Small businesses are often not seen as potential victims or interesting enough for cybercrime. A clear mistake, and yet another reason why SMEs are the target of attacks, knowing that security investment is lower

Business email imposters

In Spain, awareness of the existence and danger of fraudulent corporate emails is growing. Mainly due to the media's informative efforts and the companies themselves used to carry out these attacks. These emails are becoming more elaborate and truthful, and this appearance of officialdom often allows them to achieve their objective.

Cloud-targeted attacks: The cloud has been a critical technology in Spain in enabling companies to migrate to remote working. However, the need to fast transfer or even create from zero infrastructures

[104] https://www.s21sec.com/es/2020/09/23/la-suplantacion-de-identidad-o-phishing-el-ataque-favorito-de-los-ciberdelincuentes-en-espana/

that will allow telecommuting means, in many cases, this has not been done with complete security. According to the Cloud Security Report 2020[105], 52% of companies consider that the risk of security breaches is greater in cloud environments than in corporate environments, something that cybercriminals are taking advantage of to infiltrate corporate networks and access sensitive information, spread malware campaigns, etc.

The "State of Cloud Security 2020" report, conducted among more than 3,500 IT managers in 26 countries, including 139 Spanish companies, reported having suffered a ransomware attack and other malware in the public cloud in the last 12 months, among other incidents. A new report on cybersecurity sets alarm bells ringing for businesses in Spain and worldwide, finding that 57% report having suffered a security incident in the public cloud.

Insider threats: The Insider Threat is traditionally identified directly with the problems caused to the organisation by disloyal employees. However, the Insider Threat is broader and encompasses all those cases in which there is an exfiltration of information or any other type of hostile action that harms a company and originates or arises from within the company. This covers such figures as partners, suppliers, subcontractors and others who handle and access data and information. In addition, there is the possibility that the hostile internal actor may be unwittingly acting through carelessness or ignorance of how to proceed, or because he is being manipulated, without being aware of it, by an external attacker.

Spanish SMEs are not very aware of the dangers of **Insider threats**. This type of cyber-attack is growing as a result of Covid-19 and teleworking. It occurs mainly because an employee, perhaps at a low level, does not suspect that he may be the key to access the company.

The Insider Threat is one of the most damaging threats to an organisation, as it often exposes the weakest or most sensitive aspects of the organisation. Knowing it well and from the inside, the insider knows what data to handle, how to handle it and the right time to cause the most damage. On the other hand, collective corporate morale suffers significantly from this type of action, which also generates confusion, doubts and mistrust among a company's staff and management. The low danger awareness of this type of risk can be explained by the fact that SMEs generally do not consider themselves threatened by cybercriminals.

7.4.3. The level of awareness of cyber-attacks

Awareness, training, investment, and overconfidence, the main cybersecurity issues for businesses in Spain. Defending a company's IT systems in times of teleworking and an upsurge in cyber threats requires the implementation of accurate security services and tools to detect and respond to incidents. But just as important as going to market is creating a cross-cutting cybersecurity culture that involves all employees, from the board of directors to the bottom of the pyramid. However, Spanish companies are failing in this area.

Spanish companies, mainly SMEs, have little cybersecurity culture. This is the conclusion of a recent report by the Cyber Risk Culture (CRC) area of PwC Spain[106]. A total of 86% of the Spanish organisations surveyed - 50 to be precise - consider that their employees do not have sufficient training in this area. The study places them at 2.8 out of a range of values from 1 to 5, which implies significant room for

[105] https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx

[106] https://www.pwc.es/es/publicaciones/transformacion-digital/estado-cultura-ciberseguridad.html

improvement. According to the report, the Spanish business sector is becoming aware of the need to establish a cybersecurity culture, training and awareness plan.

The report highlights that the companies with the highest level of cybersecurity culture are those with more than 10,000 employees. The reasons: they have a greater amount of resources and a higher degree of exposure to risks and threats derived from the human factor.

Considering that the Spanish business sector is characterised by the predominance of SMEs (more than 94%), the challenge is even more significant since not investing in cybersecurity in the coming years, either due to lack of budget or lack of knowledge, will have serious consequences. On the other hand, around 95 % of cyber-attacks suffered by companies have their genesis in the human factor, either through ignorance or error. "A culture of cybersecurity in companies helps to make information security recommendations understood as an integral part of employees' work, habits and behaviour, incorporating them into their daily actions," the report says. Cybersecurity culture helps to understand that information security recommendations are an integral part of employees' work and behaviour, incorporating it into their daily actions. Tailoring the right approach allows the culture to develop naturally from the behaviours and attitudes of individuals as part of the wider corporate spectrum.

Anticipation is the fundamental rule for SMEs to avoid cyber-attacks. The entire workforce must be aware of the importance of security. In SMEs, where employees are not as hierarchical as in large companies, and almost all employees have access to all content and databases, security can be more vulnerable. While human failure is often the main gateway for these attacks, there are often technological holes that are solved by staff training and awareness.

A well-designed system must be in place: perimeter security, firewalls, antivirus, routers configured most securely, system updates, etc., are the essential elements to start with. Still far from a true digital transformation, small and medium-sized companies cannot develop security systems, either in terms of financial resources, personnel or time. Experts, therefore, point to the usefulness of outsourcing these services. A sector that is growing at 13% annually and employs hundreds of thousands of people worldwide. Hiring a specialist to draw up a security plan and identify the important assets to be protected and the risks of not doing so is one of the most useful measures. Moreover, this person will be in charge of responding to the problem, should it occur. A common option is to partner with other small and medium-sized enterprises to split the cost and make it more affordable to meet this investment.

Overconfidence is another of the weaknesses of Spanish companies. In recent months, marked by massive teleworking in the wake of the Covid-19 pandemic, the cloud has become the mainstay of business continuity. However, companies are once again overconfident when it comes to implementing cybersecurity measures. A Trend Micro study shows that while 88% of companies have accelerated their migration to the cloud, only 55% of executives are adding security to protect it. This means that there is still a lack of understanding among organisations about how to secure the cloud.

7.4.4. Preparedness

Recently in Spain, there has been a paradigm shift to be taken into account. "Companies used to try to avoid attacks at all costs, but nowadays it is assumed that they are inevitable and work more and more to react quickly to them so that they do not achieve their objectives. The cybersecurity concept among Spanish SMEs is mainly linked to protection or reaction to attacks. However, most of them are not aware of having suffered them. According to the report "Cybersecurity in Spain" prepared by The

Cocktail Analysis for Google[107]: "Another particular element is that 99.8% of Spanish companies are SMEs, most of which do not consider themselves an attractive target for cyber-attacks". As a result, they tend to be less aware of threats." Almost 3 million companies in Spain have little or no protection against hackers. In Spain, we can make a distinction between large companies and small companies.

Large companies are investing more and more in protecting themselves from cybercriminals, while SMEs and micro-enterprises do not do so, partly for economic reasons, due to lack of knowledge and also because they do not consider themselves to be targets of threats. Therefore, we can say that Spanish SMEs are insufficiently prepared for cyber-attacks. The report also defines the main measures and actions by SMEs in terms of cybersecurity, according to the companies surveyed:

- 2-step verification system: 36% have this measure in place in their email, 36% have this measure in place in their email;

- HTTPS protocol: 71% implement it on their website and more than 80% in e-commerce;

- Device updates: 85% of companies keep track of operating system updates;

- Changing passwords: 58% change their passwords every 3 months or more frequently;

- SSL certificate (e-commerce): around 57% use it;

- Two-factor authentication at checkout (e-commerce): almost 53% implement it.

These measures have proven to be effective, but some of them, such as two-step verification, changing passwords, ssl certificates or two-factor authentication, are not sufficiently implemented. Only 36 % of the SMEs surveyed have basic security protocols, such as two-step verification for corporate email. 30 % of the websites do not have the HTTPS protocol.

7.4.5. Best practices

A cyber crisis can be defined as a cybersecurity event that has a significant impact on the organisation's business and requires quick decisions to be made with limited information. The likelihood of its occurrence will depend on the degree of prior preparation of the organisation. Thus, it will be minimal if many preventive measures have been taken; and progressively higher, the less preventive work has been carried out beforehand.

It is, therefore, essential to carry out preliminary work to ensure that the organisation is prepared when a crisis arises. This includes risk analysis, the development of associated action plans and the definition of the appropriate management structures. The aim of all this is to estimate the most likely type of cyber-attack in order to anticipate the problem by designing a way to manage it.

Good practices are considered key components of a successful model for dealing with a crisis; that's why we have selected several good practices in Spain, mainly related to cybersecurity training for workers. The stakeholders involved are State institutions, which create macro programmes with significant economic allocations that are distributed throughout the national territory, business organisations, private companies and regional and local government.

[107] https://drive.google.com/file/d/18TNjaDus-lrSl5gL5Wt-Z4DOsKXtQ46m/view

1. In Spain we have the **INCIBE** Instituto Nacional de Ciberseguridad (National Institute of Cybersecurity).[108]

One of its main functions is protecting companies: offering threat information, awareness campaigns, specific training for companies according to their activity sector.

2. Activa Ciberseguridad [109]is a programme of Innovation in Cybersecurity for SMEs promoted by the General Secretariat for Industry and SMEs within the Connected Industry 4.0 Strategy framework.

The objective is for SMEs to determine their current security level and establish the level they need to achieve to protect their corporate systems and information**.**

Activa Ciberseguridad is a free programme consisting of four complementary actions aimed at SMEs.

Initial Diagnosis Phase 1: Gathering of information on the company and its sector and analysing the company's current situation in terms of cybersecurity to detect needs and possibilities for improvement.

- **Diagnosis Phase 2:** Compliance analysis/cybersecurity audit.

- **Implementation Phase 3:** Proposal for the implementation of a Cybersecurity Plan in the company.

- **Monitoring Phase 4:** Monitoring of the measures implemented and assessment of other initiatives.

3. Cybersecurity Programme Spanish Chamber of Commerce:[110]

Aimed at SMEs and the self-employed.

They provide solutions to improve business competitiveness through the incorporation of new technologies, such as:

- Identity and password management

- Detection and elimination of malware

- Patch and vulnerability management

- Virtual Private Networks

- Antivirus, firewalls, ransomware

[108] https://www.incibe.es/

[109] https://www.industriaconectada40.gob.es/programas-apoyo/Paginas/ACTIVA-Ciberseguridad.aspx

[110] https://www.camara.es/innovacion-y-competitividad/cibersegurdad

How it works:

- Needs analysis: technicians analyses the level of use of the business's technologies and recommend different options for improvement.

- Implementation of solutions: the company chooses which supplier will be in charge of the project and the Chambers of Commerce will process the grants.

Prices:

- Diagnosis: free of charge for the self-employed or SME.

- Implementation of the plan: The Chambers of Commerce subsidies up to 85% (depending on the autonomous community) for investments of a maximum of €4,000 in technological development.

4. Google with Cybersecurity:

Google and Cybersecurity: Google kicks off its cybersecurity support programme for SMEs in Madrid

The company is launching its free face-to-face training plan for Spanish SMEs in the capital. It hopes to raise awareness among companies in more than 15 locations on the peninsula about the importance of protecting their business against cyber threats.

Google and Cybersecurity is a training programme to raise awareness among small and medium-sized companies about the importance of protecting themselves against cyber-attacks.

5. Vodafone

Phishing email campaigns to raise awareness of social engineering attacks:

This service consists of an assessment for employees. They are tested through a simulated phishing campaign to measure their cyber resilience and awareness of this type of attack.

Before initiating phishing awareness services, the company will agree on the rules of engagement, the campaign's scope, and the "attack story".

Once the phishing campaign starts, emails are sent, and activity is monitored to check the campaign's progress.

Afterwards, the collected statistics and activity data are analysed. The result allows companies to know the level of awareness of employees and work on actions to increase the organisation's cybersecurity level.

"The threat of a cyber-attack on our company is the same, whether it is a large or small firm. What varies is the number of users, systems and services available". (Alberto Hernández - Managing Director of INCIBE, Spain's National Institute for Cybersecurity)[111]. The type of threats also "tend to be the same", adds the director of the Spanish National Institute of Cybersecurity. Therefore, both SMEs and large companies are equally vulnerable. They are exposed to the same chances of being attacked by a hacker in both cases. The key, then, is not who cybercriminals can attack, but how can we protect ourselves? Cyber-attacks on companies: are we aware of the danger we are running?

Size does matter when it comes to awareness. Large companies are aware of the vulnerability of their networks. In fact, 52% of them consider it "very important" to invest money from their budget in security systems. Only 12% do not consider it necessary.

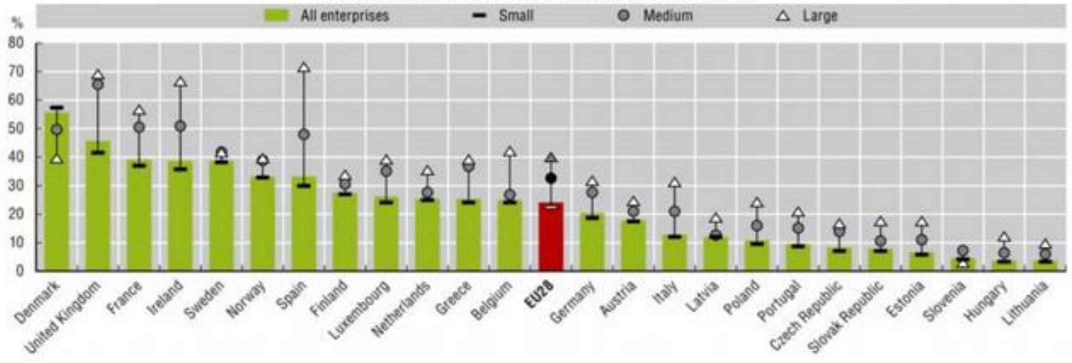
On the other hand, small businesses invest little in it. And this is a mistake. No company, regardless of its size, is exempt from being the target of a cyber-attack. There are more than 10 billion Internet-connected devices in the world, and any one of them can be hacked. Some of the measures to prevent or minimise the impact of cyber-attacks adopted by large companies in Spain are:

Insurance policies:

Spain is one of the European countries where most companies take out policies against cyber attacks: 72% of large companies are covered against cyber incidents. Specifically, Spain ranks sixth among countries with the highest percentage of companies insured against cybersecurity incidents. 33% of Spanish firms have taken out some type of insurance to protect themselves against this type of situation. The percentage of companies with this type of cover rises to 72% in the case of large companies -with more than 250 employees- and is even higher in the case of large companies with more than 250 employees.

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

As a percentage of enterprises in each employment size class



OCDE/Eurostat

Detection and action protocols:

Large companies plan and implement complex protocols to manage cyber risks.

[111] https://ticnegocios.camaravalencia.com/servicios/tendencias/ciberataques-en-empresas-importa-el-tamano/

On 14 August 2020, Mapfre, Spain's largest insurer with more than 6.5 million customers, suffered a ransomware attack[112]. In just 24 hours, it carried out an action movie-worthy deployment to counter the threat. These were some of its immediate measures.

- Implementation of action protocols
- Incident management protocol put in place
- crisis committee meeting
- Implementation of continuity plans
- Establishment of an alternative communication channel between security and technology areas
- Mass shutdown of non-essential devices and servers
- Creation of backup copies
- Isolation of some network segments
- Cutting connections with third party companies
- Reduction of remote connections.

Thanks to protocols and trained and committed staff, they were able to deal with the threat in record time.

Staff specialised in cyber risks:

These are real examples of the profiles that a large Spanish company is currently looking for in the job market:

Cyber threat detection and security

Threat monitoring analyst

Cybersecurity analyst

Cybersecurity Specialist

Cyber incident coordinator

Cybersecurity risk policies:

Approved by boards of directors. They are usually integrated into the corporate governance rules.

The Cybersecurity policy's overall objective is to define and formalise the general frameworks, which will help companies mitigate Cybersecurity risks.

The Cybersecurity Policy aims to effectively manage the security of the information handled by the company's IT systems and the assets involved in its processes.

They usually include a Cybersecurity Governance Model in order to support the objectives and principles of the risk policy.

- Identify risks

[112] https://www.elmundodemapfre.com/2020/12/03/24-horas-clave-frente-al-ciber-ataque/

-Protect against threats

-Detect threats

- Respond to cybersecurity incidents -Respond to cybersecurity incidents

-Recover and restore any affected services.

7.3.6. Policy recommendations

- **Do not neglect Cybersecurity when teleworking.** Among the causes most frequently mentioned by specialists in recent months, teleworking is one of the main ones. Applying few (or no) security measures when working from home leaves companies, including SMEs, in a very vulnerable situation.

- **Back-ups, up to date**. This is one of the steps most remembered by experts but also forgotten by companies and users. Carrying out a good policy of frequent backups is one of the most important security measures, especially in the face of ransomware, as it will allow encrypted data to be recovered.

- **Pay attention to data hosted in the cloud**. Data in the cloud is also a prime target. Six out of ten successful attacks (59%) involve data in the public cloud.

- **Active security software and solutions.** For SMEs, it is often impossible to have an IT or cybersecurity department, which means not knowing (or not being able to take care of) the technology to do so. Increasingly, security suites are becoming easier to use and manage, but there is also the option of outsourcing the service and having appropriate and well-managed technology.

- **Pay attention to email**. It is one of the company's communication tools, but it is also the main entry point for ransomware. You can rely on tools to detect fraudulent e-mail and especially pay attention to awareness.

- **Improve the training of the entire workforce.** This is an essential element for all companies, including SMEs. Technology is key, but on many occasions, threats end up "sneaking in", and knowing how to detect them is vital. Ransomware drills should be carried out periodically and specific training to help them recognise this type of malicious attack before it can cause damage that is often irreparable.

7.5. Italy

7.5.1. Introduction

Findings from this assessment indicates that Italian micro and small-medium enterprises (henceforth MSMEs) are mostly unaware of cybersecurity and impacts of cyber-threats for their businesses. The first section of this brief report gives insights on what is the nature of cyber-threats faced by Italian companies and their distribution among small and large companies. Following findings highlighted that, although large companies are much more exposed to cybercriminal activates, their surface remains much more resilient and robust compared to micro and small companies. The reasons can be reconducted to two main factors: investments on education and training on cybersecurity for employees; the availability of skilled IT personnel able to tackles the cyber-challenges and threats coming from the online domains.

By analysing the level of “awareness” of Italian MSMEs, what emerges is an overall cultural and business detachment from cybersecurity as operative priority and managerial function. Based on national surveys and results, employers and employees of small organisations admit their incompliance even with the very basics of cybersecurity – in the false belief that cyber-readiness is an issue pertaining to big organisations only. Consequently, their level of "preparedness" to cyber-resilience remains very low: for the most, they rely on outdated technologies or simply outsource the function with very little understating of the most suitable solutions for their specific needs.

Since 2017, cybersecurity is gaining considerable attention from the national policy level, however the fact that Italian MSMEs are still cyber-tardive is indicative of a fracture between the level of policy and the domain of practice. The cyber-lag experienced by the vast majority of MSMEs operating in non-IT and/or labour-intensive sectors is symptomatic of a much grater digital-skills gaps that affects national economy and society as a whole.

7.5.2. Mapping out cyber-threats in Italy

According to CLUSIT' "2021 Report on ICT Security in Italy", analysist recorded a rising 20% of malicious attacks, so much so to label 2020 as the worst year for cyber-hygiene and cybersecurity in the three-year period from 2018. Cyber-attacks and cyber-breaches are increasingly sophisticated and the heterogeneity of the phenomenon makes it difficult to addresses it from a unique perspective.

One of the most comprehensive mapping[113] of cyber-threats recorded on the Italian territory was performed in 2018 by the Cybersecurity National Laboratory (CINI). In total, 15 cyberthreats have been listed based on their level of diffusion and recurrency (Table 1):

Table 1: The Italian Landscape of cyber-threats

1.	Malware
2.	Web based attack
3.	Web application attack
4.	Denial of Service
5.	Botnet
6.	Phishing
7.	Spam
8.	Ransomware
9.	Insider Threat
10.	Physical manipulation/damage/theft/loss
11.	Exploit kit
12.	Data breach
13.	Identity theft
14.	Information
15.	Leakage

Source: CINI

In reference to private sector, the threats identified above may vary in terms of distribution impact depending specifically on a series of key factors identified below:

1. **Perpetrators of cyberattacks**. CINI confirms that the smaller the organisation the less sophisticated the cyber-attacker. Reportedly, smaller enterprises fall victim of (aspiring) cyber criminals – so called script kiddie – while larger enterprises are usually victim of more

[113] CINI, The future of Cybersecurity in Italy: Strategic focus areas, 2018. Available at: https://www.consorzio-cini.it/images/Libro-Bianco-2018-en.pdf

structured cyber-criminal organisations. The objectives behind these attacks may vary depending on the specific, and sometimes personal, motivations of the source. For cybercriminals in general, they go from: a pure showing-off of hacking skills to brag about with "cyber colleagues"; the mere sake of generating disruption and chaos; to lesser "innocent" intentions such as business espionage and extortion.

2. **Industry: capital vs labour-intensive**. Although it is true that the most cyber-exposed sector is represented by Finance, ones should consider that the organisations occupying the credit industry and affiliates can typically rely on robust IT systems and networks of knowledge to pre-assess and countermeasure risks and threats coming from the digital domain. Dataset[114] published by the National Institute of Statistics (ISTAT) confirm in fact a large disparity in terms of cyber and ICT proficiency between large firms and non-IT specialised MSMEs. This contributes also to give a geographical connotation to the phenomenon: Central-North MSMEs operate for the most in capital-intensive sectors and are much more prone and familiar with the exploitation of digital means in general and cyber-risk management models than Southern MSMEs – which typically operates in sectors and industries much less IT-driven (i.e. agriculture and farming)[115].
3. **Firms' size**. Recent studies provide elements to establish correlations between size of the enterprise and type of cyber threats. The Table 2 below describes the vulnerability to specific cyber threats that can generate business disruption in enterprises grouped in four categories depending on the number of employees.

Table 2: Distribution of cyberattacks per firm size and level of disruption

Violations with higher probability to generate business interruptions > 24h	1	Ransomware	Improper file sharing	Ransomware	Ransomware
	2	ID theft	ID theft	Spyware	ID theft
	3	Phishing	Ransomware	Data breach	DDoS
	4	Spyware	Malware for mobile	ID theft	Data Breach
	5	Malware for mobile	Malware	Improper file sharing	Malicious Spam
	6	Data Breach	Spyware	Malware	Malware
	7	Improper file sharing	Data Breach	Malware for mobile	Phishing
	8	Malicious Spam	DDoS	Phishing	Improper file sharing
	9	DDoS	Phishing	Malicious Spam	Malware for mobile
	10	Malware	Malicious Spam	DDoS	Spyware
N. of employees		250 > 499	500 > 999	1.000 > 9.999	> 10.000

Source: CISCO Cybersecurity Report Series 2020

Note: no available data for < 250

The above table is indicative of the fact that the disruptive potential of cyber threats does not depends on the nature of the threats per se, but rather on the organisational contexts. For instance, Improper file sharing seems to be the very first concern for just a category of large enterprises and much less damaging for SMEs. The same goes also for Spyware which are perceived with much more concern among SMEs than vary large corporations.

[114] ISTAT, ICT usage in Enterprises, July 2020. Available at: https://www.istat.it/en/archivio/177152; Enterprises classified by use of ICT and economic indicators, March 2020. Available at: https://www.istat.it/en/archivio/239664

[115] Osservatorio Agenda Digitale, Il posizionamento dell'Italia e delle sue regioni sul DESI, December 2020. Available at: https://www.osservatori.net/it/prodotti/formato/report/posizionamento-italia-regioni-desi-2020-report

Despite representing the Group of Seven, the Italian SMEs and industry ecosystem suffers from a historical digital lag that prevents the emergence of a cybersecurity culture among micro- and small/medium businesses.
Already in 2019, the Italian CSIRT (Computer Security Incident Response Team) reported Phishing and Malware as the most diffused cyberattacks with 3.450 and 2.040 incidents respectively – an overall trend that was not indicative of significant improvements from the past. With COVID-19 outbreaks and the transition of economies and societies into the digital domain, cybercriminals exploited immediately the situation in their favour. An independent assessment[116] from CYNET reports that, in the period that goes from February to March 2020, Italy experienced a spike in phishing attacks (+70%), malicious log-in attempts (nearly 600 hundred), email-based attacks (nearly 9.000 thousand) – with working documents and email as favourite weapon of choice of cybercriminals.

Overall, IBM estimates that in 2020, the total cost of data breaches was nearly $4.00 Million. Out of the 17 sampled countries, Italy ranks at the 8th position with an overall total cost of $3.5 Million[117].

What exacerbates the level of exposure of Italian micro- and small/medium businesses is the fact that the national labour market suffers from a chronical shortage of ICT professionals: experts and competent in ICT and computer science able to address and tackle cyberattacks so as to better prepare MSMEs in their cyber-readiness challenges. Per se, the number of ICT professionals available for the national labour market is the lowest in Europe[118] and the challenges for MSMEs to retain ICT and cybersecurity experts is even bigger considering national labour market dynamics. Findings[119] point out that the opportunity for micro and small enterprises for gathering and retaining IT talents is threatened not only by the overall shortage of reliable profiles, but even by the fact that the vast majority of such professionals is intercepted by large enterprises (> 250 employees).

Big companies are able to provide for better social and welfare arrangements for their employees, resulting as more appealing in comparison to other kind of organisations. When supply and demand are finally matched, microbusiness and SMEs are left competing each other for the remaining part of ICT professional not employed in other industries/sectors[120].

7.5.3. The level of awareness of cyber-attacks

[116] CYNET, Recent escalations in cyberattacks in italy prove the coronavirus impact on cybersecurity – acting as a warning for cisos worldwide, 2020. Avaialble at: https://www.cynet.com/blog/recent-escalation-in-cyberattacks-in-italy-prove-the-coronavirus-impact-on-cybersecurity-acting-as-a-warning-for-cisos-worldwide/

[117] IBM Security, Cost of Data Breach Report 2020. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

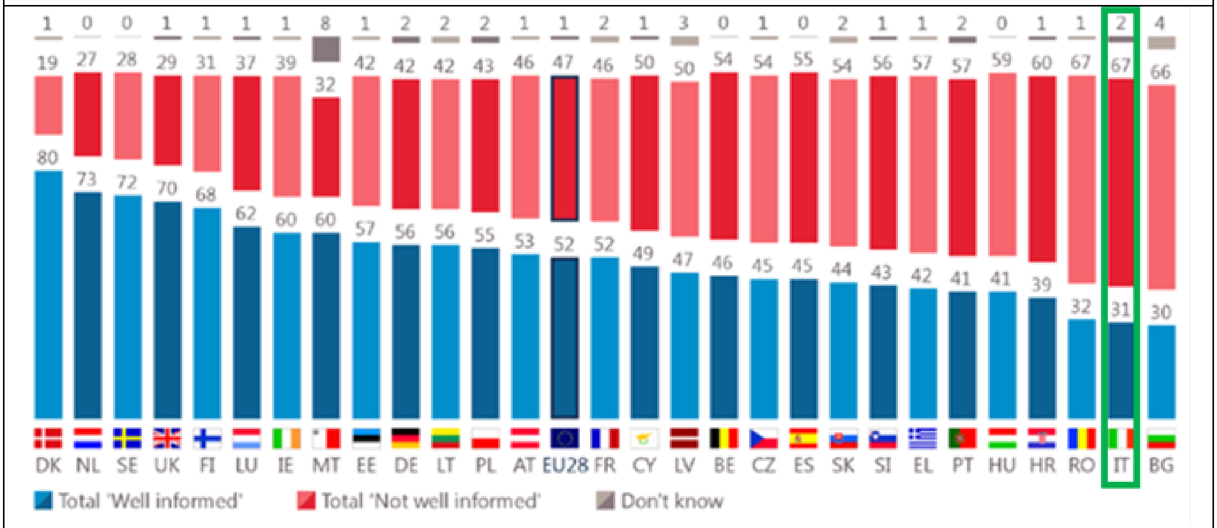
[118] Comparative data from DESI, timeframe 2018, 2019 and 2020

[119] ISTAT, Le imprese usano il web ma solo le grandi integrano tecnologie più avanzate, 2020. Available at: https://www.istat.it/it/archivio/251968#:~:text=Le%20imprese%20usano%20il%20web,nel%20Mezzogiorno%2087%2C1%25).&text=Stat%20all'interno%20del%20tema%20imprese. AssinteL – Associazioni Italiana Imprese ICT (National Association of ICT enterprises), Il mercato ICT e l'evoluzione digitale in Italia: Orientamenti della domanda, valori di spesa, scenari globali, 2019. Available at:
https://d110erj175o600.cloudfront.net/wp-content/uploads/2018/10/Definitivo_Assintel_Report_2019_QR_bassarisoluzione.pdf

[120] GCSEC (Global Cyber Security Center), The Italian Cyber Security Skills Shortage in the International Context (De Zan), Oxford Press, 2019. Available at: https://gcsec.org/wp-content/uploads/2019/05/casoIta-ebookENG.PDF

By looking at the last available data published by Eurobarometer[121], the 47% of Europeans "are not informed" on cybersecurity and risks of data breaches[122]. Italy ranks at the very bottom with a concerning 67% claiming their ignorance on the topic (Exhibit 1):

Exhibit 1: Distribution of perception per country (%)



Source: Eurobarometer, 2020

Data from the National Association for Cybersecurity (CLUSIT) highlight that only 8% of MSMEs are "safely" aware of the threats posed by the online domain, entrusting IT-priorities to qualified employees with consistent training backgrounds[123].

For the general population of micro and small entrepreneurs, latest data[124] confirm that a small 18% of MSMEs prove to be technologically mature, meaning in possess of privacy management systems and experienced IT technicians. For the remaining sample, what emerges is a concerning cultural detachment from cyber-priorities, let alone a strategic field to intervene for business competitiveness[125].

Even more concerning is the fact that an astonishing 52% of targets has no cybersecurity policy whatsoever and manifest no real intention to integrate key IT figures. Due to cultural biases and/or budget constraints, MSMEs tempt to lean on outdated praxis and technologies with low consideration

[121] Source: Special Eurobarometer 499. Note: Fieldwork October 2019, updated January 2020 (N=27.609). Available at: https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[122] Of those, the 30% claim of being "not very well" informed and the remaining 17% claim of being "not at all" informed.

[123] CLUSIT, Rapporto CLUSIT 2019. Available at: https://web.uniroma1.it/infosapienza/sites/default/files/RapportoClusit2019.pdf

[124] Bada, Maria & Nurse, Jason. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security. 10.1108/ICS-07-2018-0080. Available at: https://www.researchgate.net/publication/333709101_Developing_cybersecurity_education_and_awareness_programmes_for_small-_and_medium-sized_enterprises_SMEs

[125] Osservatorio Information Security & Privacy del Politecnico di Milano (2019)

of their actual effectiveness. As a further result, the role of CISO remains far from being established as part of the company organisation chart[126].

The lack of a perception of urgency results in excluding the development and implementation of more sophisticated models for digital businesses. More in general, by looking at aggregate expenditure indicators, investments in IT and cybersecurity reflect a discontinuous focus, a phenomenon that is indicative of a reactive approach, aimed at responding to regulatory stimuli rather than serious intentions of innovating[127].

A relevant indicator is represented by the level of investments in IT and cybersecurity infrastructures normally made by private organisations. Unlike other types of investments, cybersecurity does not generate profits per se, its benefits are rather represented by the opportunity to do not incur in further costs; the fact that these costs are not tangible in the "here and now" weaken the perception of urgency upon the related dimension[128].

Survey data[129] published by the Bank of Italy clarifies the phenomenon from a quantitative perspective (Table 3).

Table 3: Percentage of firms by level of investment (€) in cybersecurity

N. of employees	No costs	< 10.000	10.000 – 49.999	50.000 – 199.999	> 200.000	Do not know / no answer
20-49	19.8	57.0	12.0	0.8	0.1	10.3
50-199	12.8	45.7	26.3	3.5	0.8	10.8
200-499	9.9	29.5	34.4	11.1	2.6	12.6
500+	7.8	13.1	28.5	18.3	15.1	17.3

Source: Bank of Italy

More in detail, according to recent estimates[130], the expenses in cybersecurity infrastructures and technologies range from 3.500€ for small and medium enterprises at low digital intensity to nearly 19.000€ for large firms operating in the ICT sector.

Findings from the Bank of Italy[131] indicates that there is a direct correlation between investment in IT security, dimension of the firm and the actual level of exposure to cyber risks. Although it is true that MSMEs are statistically less exposed to cyber threats, such perception of immunity lowers the level of alert to a point where micro and small enterprises do not engage in any real cyber strategy for their digital readiness, remaining concerningly unprepared in case of a real cyber-attack. To the general

[126] *Idem*

[127] *Idem*

[128] Privacy Shield Framework, Italy Country Commercial Guide – Cybersecurity, 2018. Available at: https://www.privacyshield.gov/article?id=Italy-Cybersecurity

[129] Banca D'Italia, Cyber attacks: preliminary evidence from the Bank of Italy's business surveys (Biancotti C.), 2016. Available at: https://www.bancaditalia.it/pubblicazioni/qef/2017-0373/index.html?com.dotmarketing.htmlpage.language=1

[130] Il Sole24h, Cybersecurity, spesa media delle imprese ferma a 4.500 euro, 2018. Available at: https://www.ilsole24ore.com/art/cybersecurity-spesa-media--imprese-ferma-4500-euro-AE1HHXxE

[131] Banca D'Italia, The price of cyber (in)security: evidence from the Italian private sector (Biancotti C.), 2017. Available at: https://www.bancaditalia.it/pubblicazioni/qef/2017-0407/QEF_407.pdf

population of micro and small entrepreneurs, cybersecurity is conceived as an organisational priority as long as it concerns big and large companies, but not themselves.

7.5.4. Preparedness

Latest findings from ISTAT[132] highlight that the number of MSMEs failing to comply with the very basics of cybersecurity is still very high (Table 4):

Table 4: Cyber preparedness of Italian firms	
1. Percentage of firms that use at least three cybersecurity measures[133]	
N. of employees	%
10 – 49	68%
50 – 99	85,1%
100 – 249	87,1%
> 250	90,8%
2. Percentage of firms that keep track of log files to evaluate the cybersecurity incident	
N. of employees	%
10 – 49	37,7%
50 – 99	57,1%
100 – 249	66,2%
> 250	74,4%
3. Percentage of firms with consolidated monitoring procedures of cyber risks	
N. of employees	%
10 – 49	30,7%
50 – 99	51,8%
100 – 249	61,4%
> 250	71,3%
4. Percentage of firms with routine ICT test	
N. of employees	%
10 – 49	30.6%
50 – 99	49,1%
100 – 249	58,4%
> 250	72,4%
5. Percentage of firms insured against cyber attacks	
N. of employees	%
10 – 49	11,7%
50 – 99	19,2%
100 – 249	23,9%
> 250	31,3%

If robust cybersecurity systems are not perceived as an internal need, meaning a function that should be valorised and nurtured with coherent internal resources (financial, human, technological, etc.), the normal tendency is to outsource IT services (including cybersecurity) to external providers. Throughout

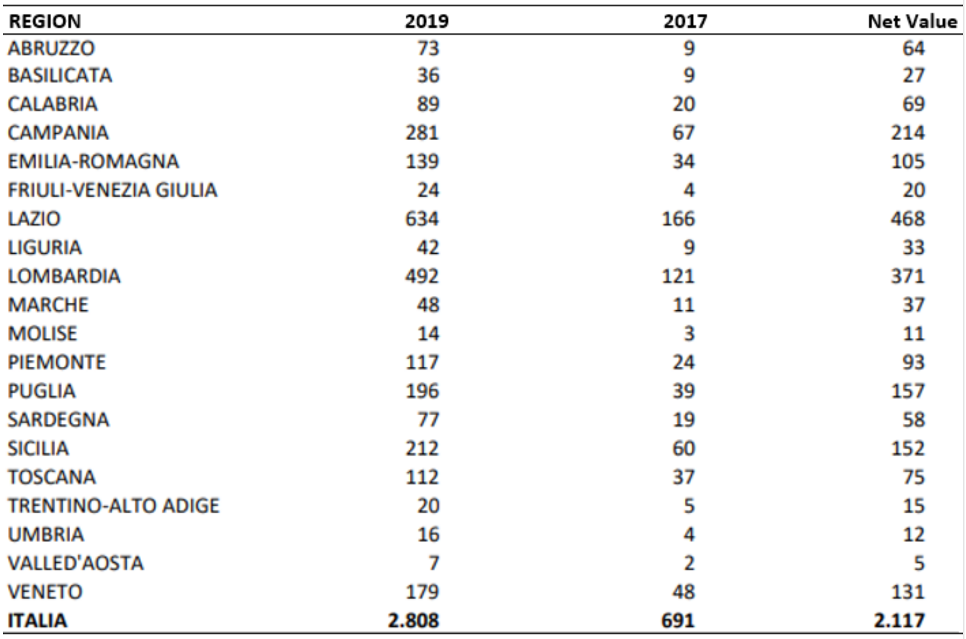
[132] ISTAT, RILEVAZIONE SULLE TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE NELLE IMPRESE (ICT), 2020. Available at: https://www.istat.it/it/archivio/177105

[133] a) complex password; b) software updates; c) backup of IT devices

the years, such trend affirmed the topic of cybersecurity more as a “business opportunity”, than an “opportunity for businesses”[134].

By looking at the latest annual censuses, the whole market of IT and cybersecurity grown exponentially both in terms of revenues and numbers of providers[135] (Exhibit 2), in most cases micro and SMEs themselves.

Exhibit 2: Regional census of private IT and cybersecurity providers (2019 vs 2017)



REGION	2019	2017	Net Value
ABRUZZO	73	9	64
BASILICATA	36	9	27
CALABRIA	89	20	69
CAMPANIA	281	67	214
EMILIA-ROMAGNA	139	34	105
FRIULI-VENEZIA GIULIA	24	4	20
LAZIO	634	166	468
LIGURIA	42	9	33
LOMBARDIA	492	121	371
MARCHE	48	11	37
MOLISE	14	3	11
PIEMONTE	117	24	93
PUGLIA	196	39	157
SARDEGNA	77	19	58
SICILIA	212	60	152
TOSCANA	112	37	75
TRENTINO-ALTO ADIGE	20	5	15
UMBRIA	16	4	12
VALLED'AOSTA	7	2	5
VENETO	179	48	131
ITALIA	**2.808**	**691**	**2.117**

Source: Unioncamere & Infocamere

Over a three-year timespan, the number of IT and cybersecurity providers has more than quadrupled. Even Southern regions (Abruzzi, Basilicata, Campania, Sicily, etc.), historically labelled as “digital tardive” compared to Northern regions[136], have shown some surprising surging trends.

But the fact that a larger number of private providers is operating in the market does not consequently represent an opportunity for MSMEs. There is no evidence that MSMEs are relying on the most efficient and effective solution by outsourcing IT and cybersecurity services to external providers. In fact, results from the aforementioned article suggest quite the opposite. For all MSMEs deciding to outsource IT and security services, the decision is certainly convenient only when looking at short-terms periods. The economic benefits are compensated by the widening of an overall gap that prevents them from embracing a more comprehensive digitalisation process[137] - a renewal that Italian MSMEs desperately need to compete in international markets[138].

[134] Unioncamere & Infocamere, Crescono gli specialisti “anti-hacker”, 2017. Available at: https://www.unioncamere.gov.it/P42A3505C160S123/cyber-security--crescono-gli--specialisti--anti-hacker.htm

[135] Unioncamere & Infocamere, Cybersecurity: crescono le imprese ‘specialiste’ anti-hacker, 2019. Available at: https://www.unioncamere.gov.it/P42A4234C160S123/cybersecurity--crescono-le-imprese--specialiste--anti-hacker.htm

[136] Politecnico di Milano, osservatorio.net digital innovation, Il Posizionamento dell’Italia e delle sue Regioni sul Desi 2020, December 2020

[137] CISCO, Proteggere il Presente e il Futuro: 20 considerazioni sulla cybersecurity per il 2020. Available at: https://www.CISCO.com/c/dam/global/it_it/pdf/IT-CISO-Benchmark-Report-2020.pdf

[138] EIDES 2020

What critics are observing is a “Market for Lemon effect”[139]. In most cases, the buyers of IT and cybersecurity services (i.e. the MSME) are not fully conscious of their specific needs and what might be truly suitable for their organisation. On the other hand, sellers (i.e. IT and cyber providers) are perfectly aware to negotiate from an advantageous position and leverage on buyers’ ignorance to nudge them for certain types of IT solutions that are less labour demanding and more profitable. In other words, buyers are in this uncomfortable position in which they pay more for something that might not necessarily fits their necessities.

This strange scenario could be avoided if a larger number of MSMEs start to approach to cybersecurity as many others are already doing (or planning to do in the near future): the first safety net against the threats coming from the cyberspace is represented by a full understanding of cyber-related activities as an integral dimension of the digitalisation process.

For instance, micro and small organisations are eager to compete in global digital markets, and more in general, to expand their network of suppliers/distributors so to get a better entry point to strategic segment of industries[140]. When it comes to best practices applied by thriving MSMEs, part of their e-commerce strategy is not only represented by the re-design of their supply chaing, sales/distribution funnels, but firstly and foremost by in-depth preliminary considerations that make of cloud technologies and cybersecurity the *sine qua non* condition for competitiveness, efficiency and profitability[141].

In other words, topics, actions and tasks pertaining to cybersecurity are not isolated from the grand scheme of businesses but become an essential set of a much more comprehensive decision-making process[142].

On a second note, this embodiment-effect of cybersecurity into broader organisational plans extends the roles and coverage of Risk Management as a whole: from secondary and support activity to multidimensional and trans-functional priority[143].

Cyber-resilient organisation understood that Risk Management should be reconceived form a rigid business function to a holistic mindset that applies upon each task carried out by the personnel[144]. Its role has been elevated from a monitoring process to a driver for excellence: Risk Management is called

[139] In reference to the well-know 1970 paper by economist George Akerlof describing how the quality of good traded in a market is greatly influenced by pre-existing information asymmetries between sellers and buyers.

[140] Unioncamere, Cybersecurity ed e-commerce le materie più “gettonate” tra le PMI italiane, 2019. Available at: https://www.unioncamere.gov.it/P42A4354C160S123/digitalizzazione--1-impresa-su-3-punta-sulla-formazione-4-0-per-competere.htm

[141] Unionecamere, Covid: crescono le imprese del commercio che vendono online +3.600 in 7 mesi, 2020. Available at: https://www.unioncamere.gov.it/P42A4646C160S123/covid--crescono-le-imprese-del-commercio-che-vendono-online---3-600-in-7-mesi.htm#:~:text=Sono%20state%20pi%C3%B9%20di%203.600,contro%2027.007%20ad%20ottobre%202020).

[142] Research Center of Cyber Intelligence and Information Security Sapienza Università di Roma, 2016. Italian Cybersecurity Report – Controlli Essenziali di Cybersecurity. Available at: https://www.uniroma1.it/sites/default/files/allegati_news/Segnalazioni%20dei%20media_23.pdf

[143] Potomac Institute for Policy Studies, ITALY: CYBER READINESS AT A GLANCE, 2016. Available at: https://www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf

[144] Politecnico di Milano, osservatorio.net digital innovation, Cyber Risk, assicurare è meglio che curare: come gestire il rischio informatico, 2020. Available at: https://blog.osservatori.net/it_it/cyber-risk-assicurazione-gestione

to comply with a broader spectrum of actions that overcome the traditional evaluation and assessment dimensions and reframe it as a key function for value generation[145].

More than about technologies and infrastructures, cyber-readiness for MSEMs is an issue of new managerial practices that exploit new routines of internal quality assurance such as:

- Stress Tests
- Red Teams preparedness
- Risk Simulations
- Crisis Scenario Making

7.5.5. Best practices

AgID (the Agency for the Digitalisation of Italy) is in charge of guiding this process through the coordination of activities that are part of the "Strategy for Technological Innovation and the Digitisation of the Country 2025". This document aims at the creation of a digital, innovative, inclusive and sustainable society, supporting the activities of businesses and citizens. The implementation of better IT infrastructures, the creation of skills and awareness on digital issues will give major boost to the digital transformation of the private sector[146].

In 2018, AgID, recognising the growing attention paid to cybersecurity by private companies and signed a memorandum of understanding with Confindustria (the General Confederation of Italian Industry). The protocol intends to plan a programme of initiatives and encourage the adoption of best practices aimed at training public administrations and private companies on cybersecurity.
Through the network of Confindustria's Digital Innovation Hubs, the aim is to spread general awareness on cybersecurity issues across Italy, ensuring the creation of training opportunities and a greater synergy between the public and private sectors[147].

In addition, several Italian regulatory interventions align with the cybersecurity needs identified at European level. Decree - Law No. 105 of 2019 (which transposes Directive (EU) 2016/1148 of 6 July 2016, the so-called NIS Directive - "Network and Information Security") was adopted with the specific aim of ensuring a secure information system of public administrations, as well as national, public and private entities. Thanks to the creation of a national cyber security perimeter and the provision of procedures and methods to ensure the required security standards, the aim is to minimise the risks associated with cybercrime[148].

In this context, CINI (the National Inter-University Consortium for Information Technology), active since 1989 under the supervision of the Italian Ministry for University and Research, has worked over the years to create training sessions on cyber risk management, which can be used by both private

[145] AGID (Agency for National Digitalisation), Cyber Risk Management. Available at: https://www.sicurezzait.gov.it/

[146] AGID, "I servizi pubblici digitali nella Strategia per l'innovazione tecnologica e la digitalizzazione del Paese 2025", 2019. Available at: https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/capitolo-1-servizi/i-servizi-pubblici-digitali-nella-strategia-per-linnovazione-tecnologica-e-la-digitalizzazione-del-paese-2025.html

[147] AGID, "Cybersecurity: nuove sinergie pubblico-privato sulla sicurezza cibernetica", 2018. Available at: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2018/06/22/cybersecurity-nuove-sinergie-pubblico-privato-sulla-sicurezza-cibernetica

[148] Camera dei deputati, "Sicurezza cibernetica", 2021.
Available at: https://temi.camera.it/leg18/temi/sicurezza_cybernetica.html

companies (regardless of their size) and the Public Administration, to assess the level of exposure to cyber risks and prepare a response plan to possible attacks. Among the tools prepared for understanding the "cyber language" and security processes, there are two documents: the "National Framework for Cybersecurity" (2016); and the "Essential Controls of Cybersecurity" (2017).

The "National Framework for Cybersecurity"[149] was created with the aim of supporting companies in need to develop cybersecurity and data protection processes. The considered areas are as follows:

- The Framework Core represents the foundation of the cybersecurity management process and consists of the main issues to be addressed for a correct management of cyber risk in a strategic manner.
- The Profile, meaning the benchmark of current cybersecurity profiles to consolidated best practices.
- The Implementation Tier provides data on the level of integration of activities related to cybersecurity within organisational dimension.

In addition to supporting organisations in developing activities that might facilitate the assessment of their cyber-matureness, the aforementioned framework prepares MSMEs to implement appropriate interventions for the development of new cyber strategies as well as the empowerment of existing plans[150].

In its "2020 Information Security & Privacy Observatory", the Politecnico of Milan (the University institute of science and technology founded in Milan) involved 180 large organisations (>249 employees) and 518 MSMEs (between 10 and 249 employees): data confirm that the digitalisation rate of a firm is significantly influenced by its size. In fact, only 73,2% of MSMEs invested in digital technology, compared to 97,1% of those with over 500 employees[151].

Results indicates a general increase in the ability of large companies to invest in cybersecurity, ensuring procedures and risk management models that are better suited to assess and monitor their cyber exposure: Larger companies tend to perceive cybersecurity with greater urgency than other organisations. Due to the lack of interna resources (first and foremost, human knowledge), MSMEs prefer to rely on external support from ICT providers[152].

Based on the above, the "investments" dimension considers:

1. Training and education in ICT enable large companies to equip themselves with a cyber-resilience mindset that improves significantly their performance. control and monitoring emerge as two key-processes that distinguish the cyber-readiness of large companies form MSMEs. Small organisations are less likely to review security procedures and analyse

[149] CINI – Cyber Security National Lab and CIS - Sapienza Research Center of Cyber Intelligence and Information Security (Sapienza Università di Roma), "Framework Nazionale per la Cybersecurity e la Data Protection", 2019. Available at https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf

[150] CINI – Cyber Security National Lab, "The future of Cybersecurity in Italy: Strategic focus areas", 2018. Available at https://cybersecnatlab.it/wp-content/uploads/2020/03/White-Book-2018.pdf

[151] Giuseppe Badalucco for DMO (Data Manager Online), "Cybersecurity targata Italia, a misura di PMI?", 2019. Available at https://www.datamanager.it/2019/03/cybersecurity-targata-italia-a-misura-di-pmi/

[152] CISCO, "Piccole e forti Ecco come PMI e imprese medio-grandi possono rafforzare le proprie difese contro le minacce odierne", 2018. Available at: https://www.CISCO.com/c/dam/global/it_it/products/security/pdfs/report-speciale-sulla-cybersecurity-SMB2018.pdf?CAMPAIGN=SC-11+Network+Visibility+and+Control&COUNTRY_SITE=it&oid=wprsc017184&ccid=cc000739

cybersecurity incidents on a regular basis, let alone the implementation and validation of new incident plans, risk assessment models and cyber-breach simulations.

2. Machine learning and cloud systems allows organisations to reduce the probability of human error and make processes more effective and efficient. Moreover, these two technologies are the ones with the lowest financial commitment, if compared to other major innovation in cybersecurity. Machine learning allows the IT systems to respond automatically to violations or anomalies, speeding up the response to the attempted attack; cloud services guarantee the storage of personal data in a third-party data centres, so that data are always safeguarded even in the case of a direct attacks menacing the IT networks of the organisation.

7.5.6. Policy recommendations

The Italian government has long implemented policies and interventions in the domains of IT and cybersecurity. With the "National Plan for Cyber Protection and Cyber Security" (March 2017) Italy has stepped into a policy framework that suffered from many legislative holes. The National Plan was intended to nurture a collaborative dialogue between key public and private stakeholders for cyber protection and cybersecurity, while encouraging overall awareness about the topic[153].

On a public scale, the Plan gave great boost to cybersecurity as a top-priority within the national development framework, but its reception at private level is still facing many difficulties. The first issue is related to the lack of qualified personnel in IT security[154]: according to the prementioned report from CISCO, 24% of Italian CIFOs (chief information security officers) believe that the lack of qualified personnel in the sector have a negative impact on the activities of the IT department of companies.

In order to respond to these needs, it is essential to work on two elements: the automation of the various IT processes and the training of personnel capable of managing and guaranteeing constant protection of organisational digital systems. Italy has not yet developed effective training initiatives, capable of filling two major gaps: the absence of a sufficient number of experts operating in the field and transferring their skills; and the absence of national coordination plans between the academic world, the public and the private sectors supporting the creation of "cyber situational awareness"[155].

CISCO itself, for example, is committed in creating an investment plan ("Digitaliani" Programme, launched in 2016) to accelerate the national digitalisation process by training of qualified personnel, and that will be later reinvested into the IT sector[156]. In the aforementioned report, CISCO emphasised this general lack of awareness by correlating it with the risk associated with cybercrime activities. In fact, even the less harmful threat can become a menace if not immediately addressed by people detaining knowledge and skills to proceed so. The automation of cybersecurity-related procedures seems to be able to guarantee the right support to organisations that need to create an effective analysis and response to possible attacks. The problem is that even if the management of the digital facilities is automated, it demands anyway professional personnel that is capable to operate such systems. The area related to cybersecurity support skills is considered the most relevant by the

[153] Presidenza del Consiglio dei Ministri, "Piano nazionale per la protezione cibernetica e la sicurezza informatica", 2017. Available at: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

[154] ISTAT, Quattro imprese su dieci utilizzano una connessione fissa veloce o ultra veloce, 2019. Available at: https://www.istat.it/it/files//2019/12/Testo_integrale.pdf

[155] CINI – Cyber Security National Lab, "The future of Cybersecurity in Italy: Strategic focus areas", 2018. Available at: https://cybersecnatlab.it/wp-content/uploads/2020/03/White-Book-2018.pdf

[156] CISCO, "Lo stato della sicurezza informatica in Italia", 2018. Available at: https://www.CISCO.com/c/m/it_it/campaigns/security/cyber-threats-and-protection-2018-report/index.html

responding companies: 77,2% of companies consider the ability of their staff to “protect personal data and privacy” and 75% to “protect digital devices from viruses or external attacks” to be crucial. The best defence against cyber threats therefore comes from the proper management and preparation of resources, processes and technology, but also, and above all, from developing an awareness of the issues and risks associated with digital activities.

Despite the public recognition of cybersecurity as a top priority at national level, Italian MSMEs are still lagging of a robust and reliable awareness associated to cybersecurity, cyber readiness and cyber resilience. A survey carried out by AlmavivA – leading Italian group in digital innovation – found that 84%[157] of companies in Italy are exposed to cybersecurity risks due to the use of obsolete technologies, highlighting the need to create initiatives that safeguard both organisations and national economy[158].

The investment targeted at coordinating and improving these resources (often problematic for MSMEs) represent one of the basic conditions to prevent or mitigate the effects of any cyberattack, functional to increase and update an adequate cyber situational awareness[159]. The Italian National Statistical Office (ISTAT), in a survey[160] conducted between May and October 2019 on a sample of about 280 thousand companies (of different sizes), confirms this situation. According to the report, the main challenge hindering the process of digital transformation of enterprises is the lack of suitable personnel, poorly trained in the use of modern technologies.

The analysed data suggest an increasing awareness about threats connected to cybersecurity: many MSMEs are starting to realise that they are a target for cyber criminals, and therefore need to develop security systems in the event of a possible cyberattack.

The remaining problem is that as far as MSMEs are more aware, there is not a correlated rise in the adoption of digital technologies as integral part of their businesses[161]. In other words, intentions are not followed by consistent actions. What is recommended is a so defined “staged methodological approach” aimed to nurture and increase the cultural understating of cybersecurity among MSMEs as ordinary function of their businesses and new strategic leverage for performance, competitiveness and efficacy.

Lessons extrapolate from this report highlights the following intervention areas for stakeholders and policy makers:

1. Strengthening CYBER AWARENESS among MSMEs and their staff

- Better awareness on what are the most common, dangerous and disrupting cyber-attacks coming from the cyber space

[157] The sample of the survey is represented by the top 500 SMEs: 148,000 companies with a turnover between 2 and 50 million euros and more than 10 employees.

[158] AlmavivA, “Cybersecurity: l’84% delle PMI ha una superficie di attacco scoperta”, 2020, Available at: https://www.almaviva.it/dam/jcr:08670360-264a-4c75-a8b6-6a5ff1e47f90/cs%20AV%20TM%203%2012%2020.pdf

[159] CISCO, “Piccole e forti Ecco come PMI e imprese medio-grandi possono rafforzare le proprie difese contro le minacce odierne”, 2018. Available at https://www.CISCO.com/c/dam/global/it_it/products/security/pdfs/report-speciale-sulla-cybersecurity-SMB2018.pdf?CAMPAIGN=SC-11+Network+Visibility+and+Control&COUNTRY_SITE=it&oid=wprsc017184&ccid=cc0007399

[160] ISTAT, “Digitalizzazione e tecnologia nelle imprese italiane”, 2020. Available at https://www.istat.it/it/files/2020/08/REPORT_DIGITALIZZAZIONE_CENSIMPRESE_PC.pdf

[161] Preferring to rely on external support provded by technology or consultancy companies, rather than carrying out such activities in-house.

- Better awareness on currents trend in cyber security, most reliable cyber-resilience strategy, obsolete measures to avoid
- Better awareness on Cyber Risk Management framed within traditional risk management models

2. Strengthening CYBER RESILIENCE among MSMEs and their staff

- Better exploitation and validation of best practices developed internally
- Better exploitation and validation of case studies and resources from the outside

3. Strengthening CYBER RESPONSIVENESS of MSMEs

- Better cyber solutions that uphold security and privacy of organisations and people
- Better training and educations programmes tailored on MSMEs’ specific operational context