EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY FOR SMES

Challenges and Recommendations

JUNE 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting the authors please use info@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

European Union Agency for Cybersecurity, ENISA

EDITORS

Anna Sarri, Viktor Paggio, Georgia Bafoutsou

ACKNOWLEDGEMENTS

To support the stocktaking and the initial analysis ENISA contracted Argyro Chatzopoulou, and Christos Kalloniatis via the ENISA call for expressions of interest framework.

The project team would like to express gratitude to all the people that participated in this survey. Without your participation, assistance and valuable insights, this document would not have been possible. We hope that this study will help you directly or indirectly in your endeavours.

The project team would also like to express its appreciation to everybody, who participated in the interviews, validation and final shape of this document. Thank you for your time, enthusiasm and support.

Special thanks to Brian Honan from BH Consulting that supported us in the final shaping and update of the study.

Piotr Zabrowski, CENEO
Marcel van der Kooi, COOPERATIE VALUE360 U.A.
Peter Stelzhammer, AV COMPARATIVES
Ulrich Seldeslachts, LSEC
Pauli Haikonen, SSH COMMUNICATIONS SECURITY, INC
Antonio Ramos, LEET SECURITY
Michel Dubois-Coutant, ONSEN CONSEIL & PARTICIPATION
Apostolos Rikoudis, Ampulla.gr
Sebastian Ivan, Lotus21 Investments
Paolo Campegiani, BIT4ID

Klaid Magi, CYCOS
Ramon Mörl, ITWATCH GMBH
Bernard Mallia, EQUINOX ADVISORY
Silvio Gil Martins, DETALHES PREDILECTOS GUIAS TURÍSTICOS LDA
Michal Leszek, BRAINLY
Benjamin Joly, Gabriela Gheorghe, Fabien Mathey - Cases.lu
SMILE - https://securitymadein.lu/
Magdalena Wrzosek, NASK PL
Iulian Alecu, CERT.RO
Kia Slæbæk Jensen, Danish Centre for Cyber-security
Ruiz Vázquez, Andrés Jesús, Departamento de Seguridad Nacional,inc ES
Spanish National Cybersecurity Institute - INCIBE
Eric Romang, Governmental CERT, LU
Kieran Duane, Department of Communications, Climate Action & Environment, IE

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-409-1 - DOI: 10.2824/770352

EXECUTIVE SUMMARY

The EU is the world's largest single market area and is the largest economy in the world[1]. Many may attribute that market size to large organizations and multi-national companies. While these are important contributors to the overall EU economy, the Small Medium Enterprise (SME) businesses form the backbone of the EU's economy. According to the European Commission "*Small and medium-sized enterprises (SMEs) are the backbone of the EU's economy. They represent 99% of all businesses in the EU and employ around 100 million people. They also account for more than half of Europe's GDP and play a key role in adding value in all sectors of the EU economy[2].*" They serve both as enablers for the digital transformation, and as a core element of the EU social fabric.

25M

SMEs exist in Europe. They are the backbone of EU economy.

In response to the COVID19 pandemic, ENISA analysed the ability of SMEs within the EU to cope with the cybersecurity challenges posed by the pandemic and determining good practices to address those challenges. This report provides cybersecurity advice, but also proposals for actions that Member States should consider in order to support SMEs improve their cybersecurity posture.

The COVID19 crisis showed how important the Internet and computers in general are for SMEs to maintain their business. In order to survive the pandemic and to continue in business many SMEs had to take business continuity measures such as adopting to cloud services, upgrading their internet services, improving their websites, and enabling staff to work remotely. This report highlights how many of the existing cybersecurity challenges were exasperated further by the impact of the COVID19 pandemic and are now more critical to mitigate. Our recommendations outlined in this report to enable SMEs to address these cybersecurity challenges are shaped towards this direction. The recommendations in this report was developed based on extended desktop research. This research was augmented by a two-month-long survey, where 249 European SMEs shared their feedback on their state of digital security and preparedness for crises such as COVID-19, and targeted interviews with selected participants followed. The research identified that the greatest challenges for SMEs are low awareness of the threats posed to their business by poor cybersecurity, the costs of implementing cybersecurity measures often combined with a lack of dedicated budget, the availability of ICT cybersecurity specialists, a lack of suitable guidelines aimed at the SME sector, and low management support.

In summary, SMEs within the European Union appear to understand that cybersecurity is an important issue and that they are very reliant on their ICT infrastructure.

Of the SMEs surveyed over 80% stated that cybersecurity issues would have serious negative impact on their business within a week of the issues happening, out of 57% saying they would most likely become bankrupt or go out of business. Despite this, SMEs do not seem to appreciate that cybersecurity is not something that impacts only larger organisations. Thus, SMEs need to realise the impact cybersecurity issues can have on their business. Many SMEs believe that cybersecurity controls that are included in the IT products they have purchased will

[1] https://ec.europa.eu/trade/policy/eu-position-in-world-trade/
[2] https://ec.europa.eu/growth/smes_en

suffice and that no additional security controls are necessary, unless mandated by regulations or Law.

Our recommendations towards SMEs are three-fold:

- **people,**
- **processes** and
- **technical**.

They include keeping software up to date, applying strict access control rules, making use of cloud services, having a plan for cyber-incidents and many others. For a full list of recommendations, see Chapter 5. The report also includes recommendations for national and European authorities.

The report is accompanied by a guide[3], providing SMEs with practical 12 high level steps on how to better secure SMEs' systems and their business.

[3] https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

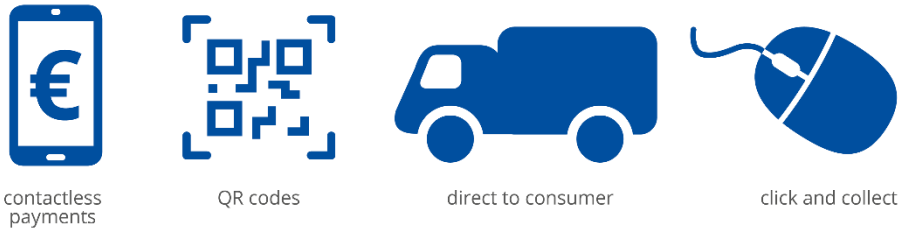
TABLE OF CONTENTS

1. INTRODUCTION

Small and medium-sized enterprises (SMEs) are the backbone of the EU's economy. They represent 99% of all businesses in the EU and employ around 100 million people[4]. There were slightly more than 25 million SMEs in the EU-28 in 2018. They also account for more than half of Europe's GDP and play a key role in adding value in all sectors of the EU economy. They serve both as enablers for the digital transformation, and as a core element of the EU social fabric.

Since the early spring of 2020, quarantine measures to prevent the spread of the COVID-19 virus were imposed on more than 3.9 billion people worldwide. This unprecedented situation affected education, work, commercial and social life.

Figure 1: New implemented technologies to avoid contact due to COVID19



Many companies urged employees to work remotely using online collaboration platforms, e-commerce, e-banking, and e-government services were enhanced, education activities shifted to e-learning and their use became part of many citizens' reality. In addition, traditional business had to implement changes to avoid contact or crowded places, and implemented technologies such as QR codes, contactless payments, and direct-to-consumer models such as home delivery, click and collect services and remote assistance via chat or phone.

The recent crisis also showed how important the digitisation of processes is for maintaining business operations. The promotion and implementation of digitisation in all sectors, not only in e-commerce, is accelerating and expanding. SMEs have to take business continuity measures, and improve online processes and related infrastructure to ensure their secure functioning. They also have the opportunity to join forces within their sectoral associations, and cooperate with partners and collaborators to guarantee the cybersecurity of their sectors.

Criminals are taking advantage of the fear and uncertainty that many citizens are experiencing because of the pandemic. We are witnesses to a marked increase in malicious emails, phishing attacks, scams and malware related to the COVID-19 crisis, In addition there is an increase in the number of cyberattacks targeting specific industries already under strain, such as hospitals, healthcare providers, and medical research facilities. Criminals are also targeting SMEs as they are aware many SMEs now have staff working remotely, have deployed systems quickly rather than securely in order to continue to serve their customers, and many do not have adequate cybersecurity defences in place.

[4] https://ec.europa.eu/growth/smes/sme-definition_en

It is important that Europe's small and medium businesses understand their cybersecurity risks, and what they can do to protect themselves, their customers and their suppliers.

Contrary to the common perception that cyber-attacks occur only against large organizations, all organizations can be similarly attacked, no matter what their size. Criminals often target SMEs for various reasons such as they offer a good value to risk ratio and as many SMEs provide services to larger organizations they can enable criminals attack those larger organizations through their supply chain.

Despite the measures an organization can implement to protect proactively itself against cyber related risks, there is no guarantee that it will not experience a cybersecurity related incident. Therefore, an SME should develop plans and capabilities to recover as quickly as possible and maintain business continuity after a cyber-related disruption.

Research and real-life practice demonstrates that organizations, who have prepared plans and capabilities to deal with a cybersecurity related incidents deal with such incidents in a much better and more efficient way than organizations that have no preparations in place. While often in reality, the impact of a cybersecurity incident never fully reflects the planning carried out, the preparations in creating those plans create a mind-set of awareness and improve team cooperation in a crisis. As an old military saying goes - plans are useless but planning is indispensable. The way that an organization will respond to a cybersecurity incident, will determine the chances of recovering from the incident successfully. In today's world, organizations will not be judged by the fact they suffered a cybersecurity breach, but they will be judged by how well they handle and respond to the breach.

While it is important for SMEs to have these preparations in place, it is important to remember that these preparations need to be adapted to the specific circumstances of each SME, such as their internal capabilities, as well as their legal, regulatory, and contractual requirements.

Effective cybersecurity provide SMEs with the confidence that allows them in an online and interconnected world to grow, innovate, and find new ways of creating value for their customers. The advice and guidance in this report provides simple measures that, if implemented, can significantly help to avoid or mitigate the impact of a cybersecurity incident affecting an SME.

The language is clear, the actions are simple, and the guidance is tailored to small and medium/sized businesses.

1.1 SCOPE / OBJECTIVES

In the current situation of the COVID19 pandemic, ENISA intends to analyse the ability of EU SMEs to cope with cybersecurity issues in a crisis by identifying cybersecurity challenges and determining good practices.

Taking note of the challenges and the good practices, this report provides cybersecurity advice for SMEs to successfully cope with cybersecurity challenges, but also proposals for actions towards Member States to support SMEs improve their cybersecurity posture.

1.2 TARGET AUDIENCE

The report intends to deliver actionable guidance to the owners and employees of SMEs. In addition, this work can be of use to other entities involved in the SME ecosystem, such as SMEs national and European associations, policy makers and implementers, SME ICT providers and others.

1.3 METHODOLOGY OVERVIEW

The methodology followed to collect and assess the information for this study included;

- conducting desktop research,
- carrying out an online survey aimed at SMEs,
- running interviews with some of the survey respondents
- interviewing industry experts.

The information derived from each stage of the process, was used to prepare and further customize the next stage.

In the end, the collected information was analysed, cross-referenced and concentrated in order to provide tangible results in line with the purpose of this study. The report was validated with the survey participants, ENISA subject matter experts, the National Cybersecurity Security Strategies Group, and the National Liaison Officers network.

For the detailed report methodology, consult Annex A.3 Methodology.

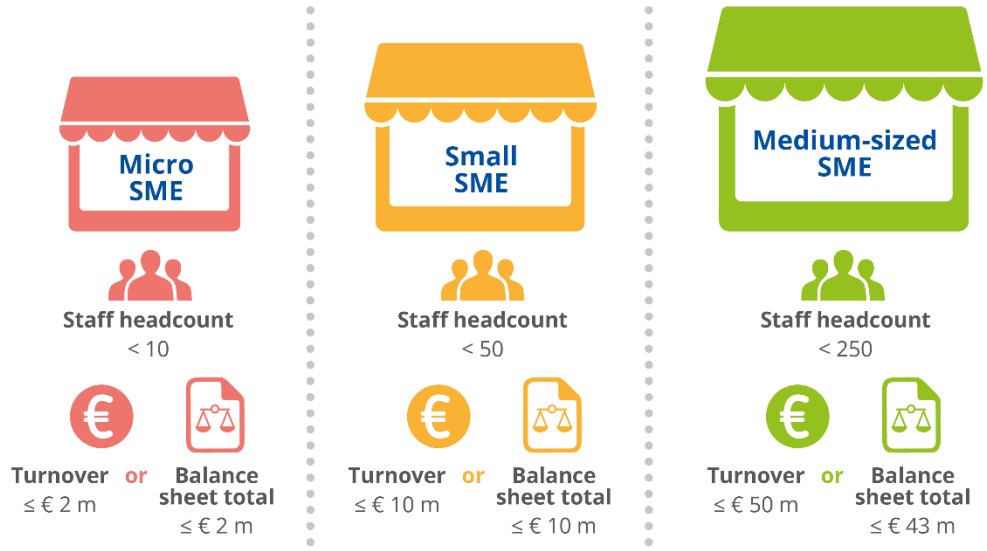
1.4 SME CHARACTERISTICS

Small and medium-sized enterprises (SMEs) represent 99% of all businesses in the EU. There were slightly more than 25 million SMEs in the EU-28 in 2018, of which 93% were micro SMEs Based on the EU definition[5]. The main factors determining whether an enterprise is an SME are staff headcount combined with either turnover or balance sheet total (Table 1).

93%

of all enterprises in Europe are micro SMEs.

Figure 2: SMEs characteristics



According to the latest (November 2019) ANNUAL REPORT ON EUROPEAN SMEs 2018/2019[6] of the European Commission micro SMEs are by far the most common type of SME, accounting for 93.0% of all enterprises and 93.2% of all SMEs in the Non-Financial Business Sector (NFBS). However, micro SMEs accounted for only 29.7% of total employment in the NFBS, while small and medium-sized SMEs accounted respectively for 20.1% and 16.8% of total NFBS employment.

For further information on SMEs and segmentation of industry, consult Annex, paragraph. A.1.

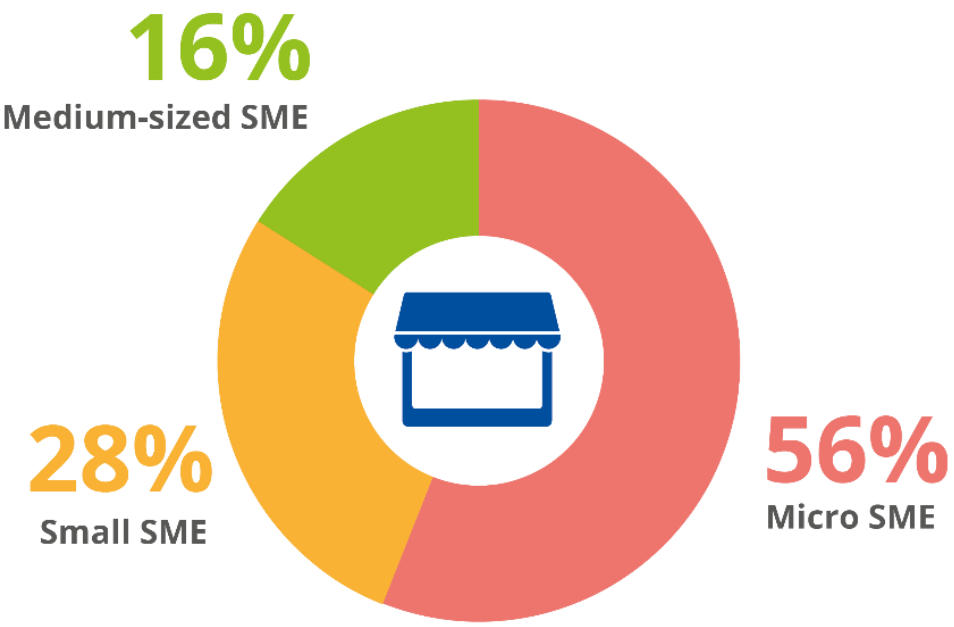
[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361&locale=en
[6] file:///C:/Users/bafouge/AppData/Local/Temp/SME%20Annual%20report%202018-2019.pdf

2. KEY SURVEY FINDINGS

2.1 SURVEY DEMOGRAPHICS

In total, 249 SMEs from 25 European Member States of the European participated in our online survey, with the following characteristics:

Figure 3: Types of SMEs that answered the survey



The participants belonged to all sectors of the economy from accommodation to manufacturing (for industry sections see Annex, Table A.1.).

More than 30% of the participants use ICT as a primary or secondary activity within their business and more than 20% of the participants carried out professional, scientific and technical activities as a primary or secondary activity.

The countries involved were Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, and Sweden.

2.2 SURVEY CONCLUSIONS

From the participants' responses some general conclusions can be drawn, regarding the role of ICT and the cybersecurity posture of SMEs:

1. **There is an increasing dependency on computers and the internet for all types of SMEs.**

Figure 4: Increased dependency on information services

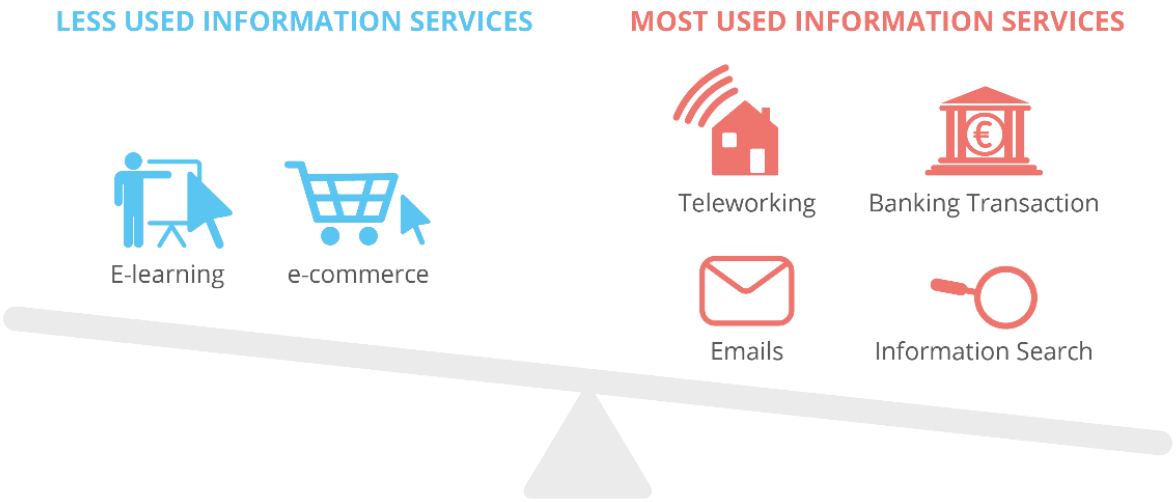
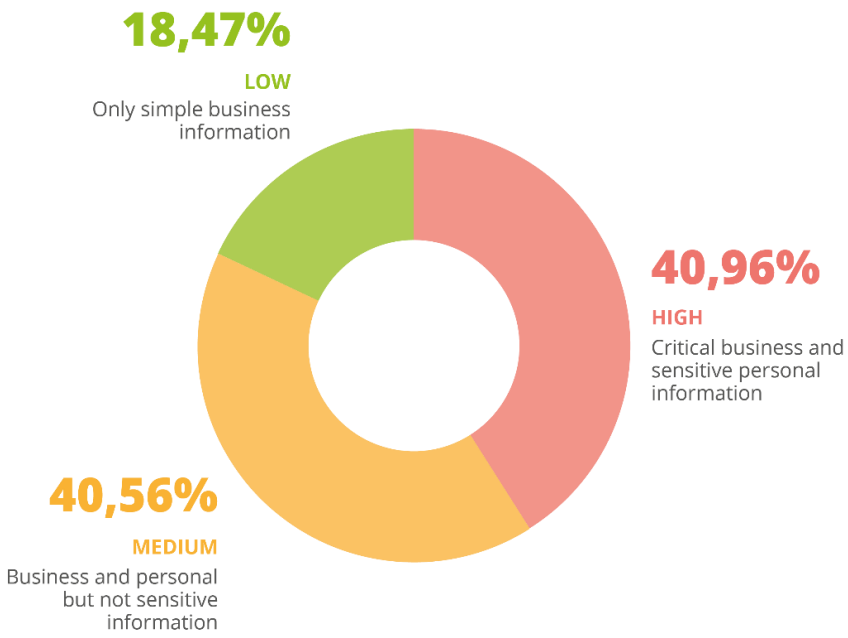


Figure 5: Cybersecurity a key concern for the majority of businesses

2. **The majority of SMEs (>80%) process critical information, making cybersecurity a key concern.**
The term critical information as defined in the survey refers to information that if it is stolen or lost, the organization would face serious legal repercussions and the owners of the personal information could encounter significant or even irreversible consequences (e.g. misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, inability to work, long-term psychological or physical ailments,).

Figure 6: Criticality and sensitivity of processed information as perceived by SMEs



3. **The majority of SMEs use some basic security controls** such as endpoint antivirus protection, backups, firewalls and perform systematic software updates. At the same time fewer SMEs perform security awareness trainings of staff and utilise logging and alerting systems.

Figure 7: Technological and Organizational Controls used by SMEs

4. **SMEs utilise the cloud for various information services and remote access tools of various types, functionalities and security levels.**

5. **25 % of participants who used some type of remote access before the COVID-19 pandemic, during the pandemic resorted to cloud services that allow, as a minimum, access to and processing of e-mails, file processing and communication**

Figure 8: Use of Cloud

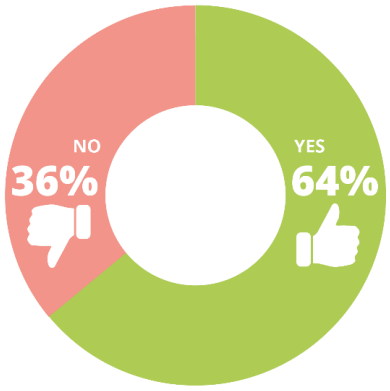
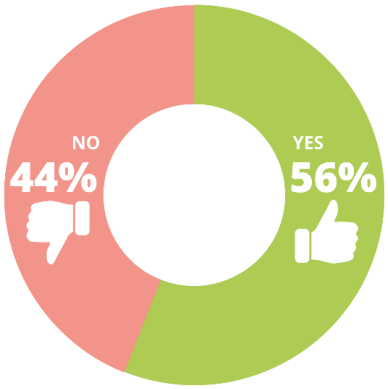


Figure 9: Use of Remote Access



6. **Phishing, Malware and web-based attacks are the most common causes of security incidents experienced by the survey participants.**

Figure 10: Distribution of Cybersecurity Incidents based on their origin

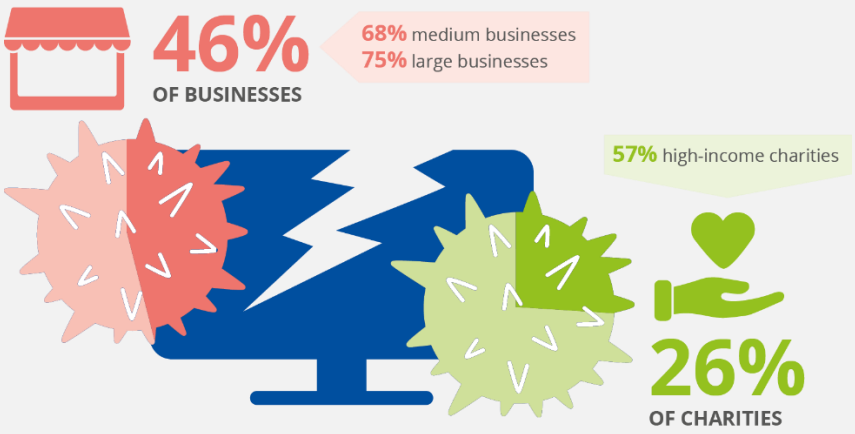
The survey showed that 45% of SMEs who responded to the survey implemented new technologies in response to the pandemic. The majority of these initiatives were to facilitate remote working for staff such as remote access or moving to the cloud. However, many of these SMEs (over 90%) did not implement any new security measures, or any additional security measures, to ensure the security of these solutions. It is also notable that while 36% of the total respondents reported that they had experienced an incident within the last 5 years, 8% of the same respondents suffered a cybersecurity incident since the start of the COVID-19 crisis; which, in terms of time, indicates a large increase of incidents during the short time frame since the start of the COVID-19 period and when the survey was conducted.

In summary, SMEs appear to implement some of the basic cybersecurity measures only as part of their overall IT implementation. However, it appears that unless cybersecurity controls are included as part of an IT solution, many SMEs do not realize the potential resultant risks posed to their business.

3. CHALLENGES

Contrary to a concept that cyber-attacks occur only to large organizations, all enterprises can be attacked regardless of their size and stored information.

Figure 11: Cybersecurity breaches and attacks in the last 12 months



Based on **UK Cybersecurity Breaches Survey**[7] "almost half of businesses (46%) and a quarter of charities (26%) report having cybersecurity breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (68%), large businesses (75%) and high-income charities (57%)".

Our findings indicate that the challenges faced by SMEs regarding their cybersecurity preparedness are many and of different nature. **The common underlying issue to all appears to be management awareness and commitment**, which in turn drives budget, allocation of resources and effective implementation of the cybersecurity practices. Seven categories of major challenges for SMEs have been identified:

- low cybersecurity awareness of the personnel,
- inadequate protection of critical and sensitive information,
- lack of budget,
- lack of ICT cybersecurity specialists,
- lack of suitable cybersecurity guidelines specific to SMEs,
- shadow IT, i.e. shift of work in ICT environment out of SME's control,
- low management support.

Sixteen SMEs from 14 different countries (Austria, Estonia, Germany, Finland, France, Greece, Ireland, Italy, Malta, Netherlands, Poland, Portugal, Romania, Spain), were selected to participate in semi-structured qualitative interviews through purposive sampling. The following

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf

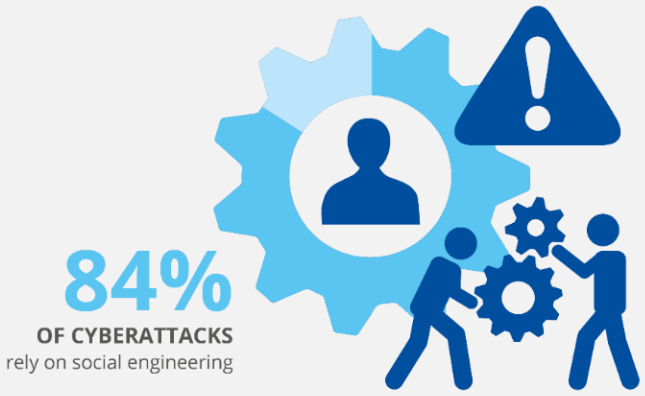
subsections summarize the cybersecurity landscape from SMEs perspective, indicating, after the data thematic analysis, their own perceptions regarding the main challenges.

3.1 LOW CYBERSECURITY AWARENESS

Because cybersecurity is a complex issue connected with technical solutions and measures, it is often perceived that it only concerns IT related people. This, though, is not the case. Cybersecurity should be part of the culture of the organization. Each person should have at least basic awareness regarding cybersecurity and how their attitude can affect the cybersecurity posture of the entire organization.

What is really needed is a transition from initial awareness to internal cybersecurity culture. For example workers should know and understand how spear phishing and other social engineering attacks work, rules of using their own devices to access company ICT environment, and other basic cybersecurity precaution measures.

Figure 12: Top cyber-threat



According to the **ENISA Threat Landscape 2020**[8], 84% of cyberattacks rely on social engineering. Furthermore, the number of phishing victims in the EU continues to grow with malicious actors using the COVID-19 theme to lure them in. COVID-19-themed attacks include messages carrying malicious file attachments and messages containing malicious links that redirect users to phishing sites or malware downloads.

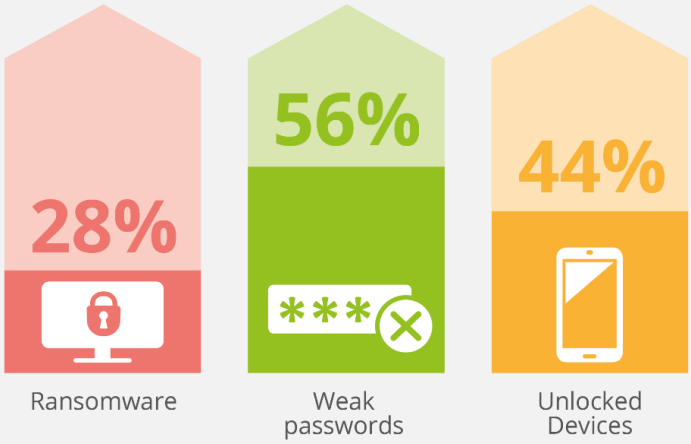
3.2 INADEQUATE PROTECTION FOR CRITICAL AND SENSITIVE INFORMATION

SMEs handle a variety of information: personnel records, customer information, details about production, procurement details, financial data, policies, procedures, and other. Each of them has a different value to the organization and laws, regulations or agreements that may mandate their protection.

Not having a specific backup up policy, an endpoint antimalware solution implemented on all types of devices and kept up-to-date, using obsolete or just unpatched software that does not auto update, could seriously jeopardize the company's critical and sensitive information, making the SME an easy target for cyberattacks like ransomware or other.

[8] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

Figure 13: Cybersecurity Threat Landscape



Based on ENISA's Threat Landscape reports of 2020, Ransomware was the second most common threat, and was related to one-third (28%) of security incidents.

In addition, according to the ENISA Threat Landscape Report 2018, weak or reused passwords (56 %) and unlocked devices (44 %) are two of the biggest weaknesses within organisations.

3.3 BUDGETARY ISSUES

Cybersecurity preparedness efforts entail investments from various aspects: such as awareness training, implementation of cybersecurity controls, engaging external experts, and specialized training for staff members dedicated to information security. Dedicated cybersecurity solutions, as advanced firewalls or security information and event management systems (SIEM), are also large investments.

While many SMEs have engaged with the cloud under subscription model, due to their size many SMEs often do not qualify for special offers and have to deal with fixed cybersecurity SLA contract clauses, unable to reach the SLA flexibility dedicated to large organizations. Advanced solutions offering great variety of abilities and possible customizations useful for more cybersecurity-mature organizations, are often not used by SMEs due to SMEs not being aware of understanding the solutions offered. In many cases, the cybersecurity features are often part of high-level subscription plans which may not be suitable to an SME.

This trend is evident from our study, which highlighted that while many SMEs engaged with new solutions in reaction to the COVID19 pandemic many of them did not invest in any additional security controls

While not specific to the cybersecurity challenges posed by the COVID19 pandemic, it is evident that many SMEs view cybersecurity as a cost rather than as an investment in their business. This is in spite of how many SMEs admitted that a major cybersecurity incident resulting in their ICT systems being unavailable would have a major negative impact on their business. It is therefore critical that SMEs understand better the risks to their business posed by cybersecurity issues and subsequently allocate appropriate budgets to invest in the required controls to protect their business.

Figure 14: Cybersecurity VS Costs

In our study, the interviewees noted that implementation cost is a major challenge. They indicated that *"the VPNs are costly and cumbersome", "the antivirus and other software security measures are expensive"* and *"security comes on an additional cost"*.

3.4 LACK OF ICT CYBERSECURITY EXPERTISE & PERSONNEL

Cybersecurity is a specialized topic, requiring specialized knowledge, however it is quite common within an SME that individuals multitask and may have multiple roles assigned to them. As a result, an employee within a SME may be responsible for cybersecurity, as well as for other processes.

While there are several cybersecurity related standards that SMEs could implement to improve their cybersecurity readiness, such as the ISO 27001:2013 Information Security Standard[9] and the Federal Office for Information Security (BSI) IT-Grundschutz[10], the implementation of these standards can be a time-consuming process.

Compounding the challenges in this area is that many cybersecurity solutions require specialized IT knowledge to implement and manage them properly. All of these issues combined make managing cybersecurity within a SME a big challenge.

As an SME's business grows and changes, the technology they employ will change and the cyber threat landscape will constantly alter, which requires SMEs to ensure their efforts to manage cybersecurity should be continuous and consistent. If the company does not directly employ a person with specialized ICT knowledge (typical for non-technical SMEs), there is need to invest in external expert assistance.

Cybersecurity vendors should also be required to ensure their products are secure by default and that managing these products should be relatively straightforward for non-technical people.

Simple to follow standards and guidelines aimed specifically at the SME sector should be developed within each Member State, such as the Cyber Essentials scheme[11] within the UK and the "12 Steps to Cybersecurity Guide"[12] published by the Irish Government.

[9] https://www.iso.org/isoiec-27001-information-security.html
[10] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
[1111] https://www.ncsc.gov.uk/cyberessentials/overview
[12] https://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf

The interview participants highlighted this challenge by saying that *"dealing with security threats is hard for non-IT related SMEs"*, and that *"there is a shortage of skills in the population regarding cybersecurity"*.

In addition, they mentioned that "*usually SMEs do not have a CISO"*. This is further substantiated by the results of the online survey where only 28% of the participants (almost half of them in the ICT industry) declared that they have assigned the role of the Information Security Officer to someone within their organization.

3.5 LACK OF SUITABLE GUIDELINES

Another challenge for SMEs is the availability and suitability of guidelines in the form of standards, whitepapers or other. There are existing documents[13], however most of them, either provide generic information, such as *"implement backup",* or address larger organizations with an existing cybersecurity framework where more specialization is possible, for example *"appoint an information security officer and make sure that segregation of duties is applied"*.

In addition, some of the well-known standards e.g. ISO 27001:2013[14] describe an approach for the design, implementation, operation, control and improvement of an Information Security Management System, which for many SMEs require external expert assistance to understand and implement.

While several EU bodies and Member States have issued guidelines in relation to cybersecurity the respondents highlight that many were not aware these were available, that some of them were outdated, and that a lot of the material is written to highlight the theory behind cybersecurity without providing practical guidelines.
The following table outlines some guidelines that are available both at the EU level and at the national level. However, there is a lack of consistency on these guidelines across all Member States and not all Member States provide guidelines in their own national language(s)

[13] https://ccb.belgium.be/en/document/guide-sme
[14] https://www.iso.org/standard/54534.html

Table 1: Available guidelines at EU and National level

Level	Organization	Guideline
European	ENISA	Tips for Cybersecurity when buying online[15]
		Information Security and Privacy Standards for SMEs[16]
	Europol	Safe Teleworking Tips and Advice[17]
	CyberWatching.EU	Cybersecurity Self-Assessment for SMEs[18]
Belgium	Cybersecurity Coalition	Cybersecurity Guide for SME[19]
	Centre for Cybersecurity Belgium	Cybersecurity Guide for SME[20]
Finland	Finnish Transport and Communications Agency National Cybersecurity Centre	Information security under exceptional circumstances - Instructions for organizations and companies[21].
France	Agence nationale de la sécurité des systemes d'information - ANSSI	La cybersécurité pour les tpe/pme en douze questions[22]
		Plateforme d'assistance et Prevention du risque numérique[23]
	Cybermalveillance	Les 10 mesures essentielles pour assurer votre sécurité numérique - Assistance aux victimes de cybermalveillance[24]
		Kit de sensibilisation aux risques numériques[25]
	BPI France	Cybersécurité : un guide pratique à destination des dirigeants de TPE, PME et ETI[26]
	Commission Nationale de l'Informatique et des Libertés (CNIL)	Les technologies pour protéger son patrimoine informationnel, protéger les personnes concernées des atteintes à leurs données[27]
Germany	BSI	"IT-Grundschutz-Kompendium" (Edition 2021)[28]
		"IT-Sicherheit im Home-Office unter besonderer Berücksichtigung der COVID-19 Situation" (April 2021)[29]
		"Home-Office? – Aber sicher!" (last update April 2021)[30]
Ireland	Data Protection Commission	Protecting Personal Data When Working Remotely[31]
		Guidance for Controllers on Data Security[32]

[15] *https://www.enisa.europa.eu/news/enisa-news/tips-for-cybersecurity-when-buying-and-selling-online*
[16] *https://www.enisa.europa.eu/publications/standardisation-for-smes*
[17] *https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safe-teleworking-tips-and-advice*
[18] *https://cyberwatching.eu/cybersecurity-best-practices-smes-assessment*
[19] *https://www.cybersecuritycoalition.be/resource/cyber-security-guide-sme/*
[20] *https://ccb.belgium.be/en/document/guide-sme*
[21] *https://www.kyberturvallisuuskeskus.fi/en/poikkeusolojen-tietoturva-ohjeita-organisaatioille*
[22] *https://www.ssi.gouv.fr/particulier/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/*
[23] *https://www.cybermalveillance.gouv.fr/*
[24] *https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique*
[25] *Kit-complet-de-sensibilisation.pdf*
[26] *https://www.bpifrance.fr/A-la-une/Dossiers/Cybersecurite-comment-se-proteger/Cybersecurite-un-guide-pratique-a-destination-des-dirigeants-52295*
[27] *https://www.cnil.fr/fr/cybersecurite*
[28] *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition202*
[29] *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office*
[30] *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/homeoffice.html*
[31] *https://www.dataprotection.ie/en/dpc-guidance/blogs/protecting-personal-data-when-working-remotely*
[32] *https://www.dataprotection.ie/en/dpc-guidance/guidance-controllers-data-security*

Level	Organization	Guideline
	National Cybersecurity Centre	12 Steps to Cybersecurity[33] Working from Home Security Advice[34]
Italy	Computer Security Incident Response Team – Italia Garante per la protezione dei dati personali (GPDP)	Lavoro da remoto - Vademecum delle policy di sicurezza per le organizzazioni35 Cybersecurity Guides[36]
Latvia	Computer Emergency Response Team (CERT.LV) Data Valsts Inspekcija	Technology Checklist for Businesses[37] What safety precautions should be followed when working remotely?[38]
Luxembourg	CASES[39]. Fit4Cybersecurity[40]	Cyberworld Awareness and Security Enhancement Services A free online survey to measure maturity in information security
Netherlands	DTC – Digital Trust Centre National Cybersecurity Centre Autoriteit Persoonsgegevens	Information and Advisories[41] Risicoklassenindeling Digitale Veiligheid[42] Factsheet Your remote work systems have become essential[43] Factsheet 5 recommendations for safe purchasing of cloud services[44] Factsheet Your home working facilities are now indispensable[45] Veilig thuiswerken tijdens corona[46]
Norway	Nasjonal sikkerhetsmyndighet (NSM)	Basic principles of ICT security 2.0[47]
Romania	CERT-RO	Cybersecurity Guide[48]
Serbia	National CERT of the Republic of Serbia	Protection of Small and Medium Enterprises Against Cyber Attacks49
Slovakia	SK CERT	Podnikatelia a organizácie[50]
Slovenia	SI-CERT National Cyber Security Response Center Informacijski Pooblaščenec	Protect Your Business[51] Guidelines on the use of private devices for business purposes[52]
Spain	Agencia Española de Protección de Datos (AEPD)	Recommendations to protect personal data in situations of mobility and telecommuting[53]

[33] *https://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf*
[34] *https://www.ncsc.gov.ie/pdfs/WFH-Advisory.pdf*
[35] *https://csirt.gov.it/contenuti/lavoro-da-remoto-vademecum-delle-policy-di-sicurezza-per-le-organizzazioni*
[36] *https://www.garanteprivacy.it/temi/cybersecurity*
[37] *https://www.esidross.lv/wp-content/uploads/2017/03/STC_Technology_Checklist_For_Businesses.pdf*
[38] *https://www.dvi.gov.lv/lv/covid-19*
[39] *https://trustbox.cases.lu.*
[40] *https://startup.cases.lu*
[41] *Informatie & advies | Digital Trust Center (Min. van EZK)*
[42] *https://www.digitaltrustcenter.nl/risicoklasse*
[43] *https://english.ncsc.nl/publications/factsheets/2020/april/16/your-remote-work-systems-have-become-essential*
[44] *https://www.ncsc.nl/documenten/publicaties/2020/oktober/29/factsheet-5-adviezen-voor-veilige-inkoop-van-clouddiensten*
[45] *https://www.ncsc.nl/documenten/publicaties/2020/april/1/factsheet-uw-thuiswerkfaciliteiten-zijn-nu-onmisbaar*
[46] *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/veilig-thuiswerken-tijdens-corona*
[47] *https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/>*
[48] *https://www.cert.ro/vezi/document/ghid-securitate-cibernetica-2021*
[49] *https://www.cert.rs/en/publikacije.html*
[50] *https://www.sk-cert.sk/en/tips-and-tricks/business-organizations/index.html*
[51] *https://www.varninainternetu.si/za-podjetja/*
[52] *Guidelines on the use of private devices for business purposes (BYOD)*
[53] *https://www.aepd.es/en/documento/nota-tecnica-proteger-datos-teletrabajo-en.pdf*

It should be noted that the above is not an exhaustive list and highlights some of the material available across EU bodies and Member States.

The participants confirmed that this is a major issue. They noted that *"a generic certification scheme does not help"*, and that the *"guidelines from governments and policy makers are too abstract"*.

Towards this, *"missing guidelines about applying security and privacy legislation"* was another perception according to the respondents. Additionally, an interesting statement concerned that "*each enterprise has different context and needs, generic guidelines should be extracted in the sense that the companies will be able to apply them"*.

3.6 SHADOW IT/PERSONAL DEVICES

Many SMEs have allowed their staff to use their own personal devices to access company data. This was a common practice before the COVID19 pandemic but was accelerated even more as a result of the pandemic. In response to the demand for remote working when the COVID19 pandemic struck, many SMEs did not have the budget, resources, or indeed the time to purchase and configure corporate devices for each of their remote workers. As a result, many SMEs allowed their staff to use their own personal devices such as computers, tablets, and smartphones to access company systems and data.

In addition, to staff using their own personal devices for business purposes they are also accessing the internet, and therefore corporate systems and data, from their own home networks. In many cases, these home networks are using consumer grade technology for items such as broadband connectivity and wireless networks, which may not be as secure as the business level technology employed by the SME in its own network. Compounding the use of these potentially less secure home networks is the issue that these home networks are also shared with others within the house. The devices others in the household use could pose an additional security threat to the SME's systems as they may not be configured in a secure manner. In effect, the COVID19 Pandemic has extended the SME's network perimeter from the locations associated with the SME's business premises, to the homes of all its employees.

The use of personal devices is not the only concern with remote working, the use of personal cloud services poses another risk that SME's need to be aware of. Staff, in an effort to be productive and to enable sharing of company data, may use their own personal cloud services for email or for sharing files. This is further exasperated if the SME does not have the facilities set up to enable remote workers to collaborate effectively. Many SMEs may have employed a Virtual Private Network (VPN) to allow remote access to its network and data, however these VPNs may not be suitable or designed to support all of the SME's staff access remotely. This can then result in staff becoming frustrated with the technology in place and in an effort to get their work done may employ their own personal cloud and email services.

3.7 MOVING ONLINE

Many SMEs surveyed had a relatively small online presence prior to the COVID19 Pandemic. This typically consisted of a website providing details about their business. Many SMEs did not use the Internet for online selling or direct engagement with their clients. However, with the various lockdowns introduced by many Member States to counter the spread of COVID19 and the resulting hesitancy of consumers to shop and engage in a face to face setting, many SMEs faced the challenge on how to continue providing services to their clients without interacting with them physically. This drove a large number of SMEs to convert all or parts of their business to be delivered over the Internet. Businesses such as shops, restaurants, and craft businesses rushed to set up an online presence from which they could promote and sell their products.

Figure 15: Increase selling online

In Ireland, the annual report from the national registry for .ie domain names, showed a 25% increase in the number of SMEs selling their products online of via an online store. In addition, the same report highlights that 55% of Irish SMEs have invested in their online presence since the beginning of the pandemic, up from just 21% in 2020.[54]

However, in the rush to get online and enable their businesses to survive many SMEs have not invested either time or money in ensuring these online services are secure. Features such as Multi-Factor Authentication to access sensitive systems such as email, ensuring websites are regularly patched, and other security configurations were not configured by default. As a result, many SMEs are now at risk of these services becoming compromised.

3.8 LOW MANAGEMENT SUPPORT

A key success factor for any business initiative within a company, no matter its size, is having senior management support for that initiative. It is well known that without management support any initiative will flounder and eventually fail. This is particularly true with cybersecurity as it can be very hard to convince management to invest time, resources and money into something that is hard to demonstrate brings direct value to the business. While in larger organizations senior management can rely on their own cybersecurity experts or bring that expertise into the organization using consultants, many SMEs do not have this luxury. Instead, senior management within an SME often rely on their own knowledge of issues or what they learn from their peer networks. As such, there is low awareness amongst SMEs that they face many cybersecurity threats with many of them thinking they “are too small for criminals to want to hack them.”

Contrary to a concept that cyber-attacks occur only to large organizations, all enterprises can be similarly attacked, regardless of their size and stored information. SMEs are an interesting target for cyber-attacks, because criminals may consider them to be easy targets due to SMEs not having robust cybersecurity measures in place. In addition, as many SMEs provide services to larger organizations an SME could be of interest to cybercriminals as a way to attack the supply chain of this larger organization.

Management leadership and support can be demonstrated by providing specific objectives regarding cybersecurity, provision of resources (human or others), the support for cybersecurity policies, procedures and controls, and the establishment of risk appetite in relation to cybersecurity – level of risk that an organization is ready to accept, before action is deemed necessary to reduce, avoid or share (transfer) it.

[54] *https://www.weare.ie/tipping-point/*

Figure 16: Increased management responsibility

The importance of management leadership is highlighted also by the SMEs as "*it is the task of the manager to continue to motivate and monitor the people. The manager should make the employee understand what the value of security is and to make sure that they continue to uphold the measures.*"

4. CYBERSECURITY INCIDENTS

Many SMEs falsely think that because of their small size they are of no interest to cybercriminals. There is an assumption that cybercriminals prefer to target larger organizations as those organizations have items that are of more interest to criminals, such as large amounts of financial details belonging to customers or sensitive and valuable intellectual property. However, criminals do not target only large organizations and will attack any company no matter its size. They often prefer to attack smaller firms as there is a higher likelihood of these companies not having sophisticated cybersecurity measures in place and therefore easier for criminals to compromise.

The following are real life incidents that occurred against SMEs within the EU since the start of the pandemic and highlight that criminals have no hesitation in taking advantage of poor cybersecurity no matter how big or small the organization is.

Note to preserve the anonymity of the victims we have removed as much identifying information as possible.

4.1 IT SERVICE PROVIDER COMPANY RANSOMWARED

- Company Type : IT Software Service Provider
- Company Size : < 50 employees
- Breach Type : Ransomware attack

An IT service company provides updates of its software to its clients using 15 servers hosted in a datacenter. Normally access to these servers was only allowed from the company's own office network, where its development team was based. As a result, of the pandemic all of the company's staff were moved to working from home. To facilitate remote working for its developers the company enabled the developers to access the 15 servers in its datacenter via the Microsoft Remote Desktop Protocol (RDP). However, the company did not secure their RDP connections and criminals were able to breach their systems resulting in 14 of the 15 servers becoming victims of a ransomware attack. The company was lucky that the remaining server, which had not yet been encrypted stored the backups of all the other servers, so they were able to quickly restore services and then secured their RDP connections.

Lessons learnt:

- If using RDP for remote access ensure it is secured[55]
- Backups are an effective method to recover from a ransomware attack. Ensure that you carry out regular backups and that they are stored offline so that criminals cannot encrypt the backups.
- Provide security awareness training to staff on selecting secure passwords

[55] *https://www.microsoft.com/security/blog/2020/04/16/security-guidance-remote-desktop-adoption/*

4.2 STOLEN LAPTOP

- Company Type : Legal Firm
- Company Size : <25 employees
- Breach Type : Laptop stolen containing sensitive client data

A legal firm in response to the pandemic allowed its staff to work from home. However, not all staff had company issued laptops and would use traditional desktop computers when in the company's office. To facilitate working from home the legal firm allowed staff to use their own personal laptops. One member of staff was the victim of a burglary in their own, which resulted in their personal laptop being stolen. The member of staff had been using this laptop for working remotely and had copied all the clients' information and emails onto the hard drive of their laptop. The laptop was not encrypted therefore the data held on it is easily accessible to anyone who gets access to the laptop

Lessons Learnt

- Restrict staff to accessing only data they need access to in order to do their job
- Ensure all portable devices are encrypted
- Provide security awareness to staff on the risks of portable devices and how to protect them

4.3 EMAIL ACCOUNT HIJACKED TO FACILITATE FRAUD

- Company Type : Marketing and branding company
- Company Size : <25 employees
- Breach Type : Email account hijacked

A marketing and branding company moved their email system to a cloud based solution to facilitate their staff to work remotely during the pandemic. One member of staff fell victim to a phishing attack, which pretended to be from the email provider looking for account verification details. Once the member of the staff entered their details, the criminals took over their email account. The criminals then sent emails from that hijacked account to clients of the marketing and branding company. These emails were a mixture of phishing emails and invoice redirection fraud emails. The invoice redirection fraud emails were sent to some clients telling them the banking details for the marketing and branding company had changed and that all future payments for invoices should be sent to that new bank account (which was controlled by the criminals). The phishing emails targeted clients of the marketing and branding company and contained a link purporting to be a link to an outstanding invoice. When a client clicked on the link it would ask the client for their user details and password.

The attack was detected by one of the marketing and branding firm's customers, when a member of that company's staff clicked on the link within the phishing email and noticed the site was a phishing site. The firm that notified the marketing and branding firm of the attack subsequently cancelled all future business to the value of €200,000 to €300,000 annually over concerns about cybersecurity.

Lessons Learnt

- Enable Multi-Factor Authentication on hosted platforms
- Provide security awareness training to staff to enable them identify phishing emails
- Implement strong password policies for hosted platforms

4.4 RANSOMWARED PC & SERVER

- Company Type : Leisure/Sports Club
- Company Size : <75 employees
- Breach Type : Ransomware Attack

A leisure/sports club closed its onsite business at the start of the pandemic but allowed staff to work remotely. To facilitate remote working the IT provider for the club installed remote desktop sharing software on each of the employee's company PC. This allowed each member of staff to remotely connect to their office PC from home and work on their office PC as if they were physically at the PC.

One member of staff received an email with an attachment in the email. The subject line was "Is this your photo?" Upon opening the attachment, the ransomware installed on the computer encrypting all files on that computer and on the file shares, it was accessing from the company's file server. This resulted in all the shared data in the company becoming encrypted.

The IT company were able to retrieve their data by using the Europol CyberCrime Centre's (EC3) NoMoreRansom website[56] which provided them with the keys to decrypt the data.

Further investigations revealed that the PC that became infected did not have an up to date anti-virus software installed, nor was the latest software patches and updates applied. This was due to no-one being in the office to check and ensure the patches and updates had been applied.

Lessons Learnt

- Ensure all software on all PCs is patched and up to date.
- Ensure anti-virus software on all PCs is up to date
- Implement spam and virus filtering on incoming emails to block emails detected to contain malicious content
- Have secure, reliable, and up to date backups stored offline
- Provide security awareness training to staff to enable them identify malicious emails
- Implement tools to alert if software is not patched and updated on PCs
- Implement tools to alert if anti-virus software is not up to date
- Ensure alerting mechanisms are in place to warn of ongoing attacks, such as a computer virus infection

4.5 CEO FRAUD

- Company Type : Technology Company
- Company Size : <75 employees
- Breach Type : CEO Fraud

A technology company that specializes in website development became the victim of CEO fraud resulting from a member of staff acting upon a fraudulent email they thought came from their CEO. The company have moved all staff to remote working but as their email server was still on their premises with poor broadband connectivity, staff were also using their own personal email accounts to communicate with each other. A member of the finance team received what they

[56] *https://www.nomoreransom.org/*

thought was an email from the CEO asking for urgent payment to be made to a new supplier in order to meet a project deadline. The email was not from the CEO but was crafted to look like it came from them. The member of staff only discovered the issue the next day when talking to the CEO by phone and informed them the payment had been made.

Lessons Learnt

- Ensure all staff, especially those in privileged role such as finance, follow written processes and procedures.
- Ensure management will not discipline staff for when they do follow proper processes and procedures
- Provide company systems for staff to communicate securely

5. RECOMMENDATIONS

Our survey demonstrated that many SMEs had already some common cybersecurity measures before the COVID19 Pandemic struck. However, the majority of these controls were basic technical controls, such as firewalls and anti-virus software, and were the responsibility of the IT person.

There are several publications issued by member states and other countries such as the United Kingdom, Australia, and the United States that offer guidelines and recommendations to SMEs on how to improve their cybersecurity.

Cybersecurity does not necessarily have to be costly for SMEs to implement and maintain. Several measures can be implemented, without the company having to invest a large amount. Many of these measures are focused primarily on ensuring roles, responsibilities are assigned to the appropriate personnel, and that staff are aware of cybersecurity risks and how to identify and protect against them. Many of the technical cybersecurity measures are also relatively cost effective to implement and need not be necessarily overly sophisticated or complex.

The core cybersecurity fundamentals outlined in the above publications, and identified from our survey and research, can be summarized in the following areas:

Figure 17: Core cybersecurity fundamental areas

As in any other areas of business, a checklist is an excellent method to ensure you are covering the key areas in addressing the business issues and risks raised by cybersecurity. An incomplete or negative response to any of the following items means that area of risk needs to be addressed.

Table 2: Core cybersecurity fundamentals

People

Check Item	Description	Answer
Responsibility	Does a director, or equivalent, have responsibility for cybersecurity?	
Employee Buy-in	Have all members of staff given written acknowledgement that they have read, understood and accepted the information security policy?	
Employee awareness	Do all users on your computer systems receive regular training on their security responsibilities on how to identify and deal with various security threats? Ensure that staff are aware of, and can verify, all contact points and communication channels	
Cybersecurity Training	Do staff members with specific security responsibilities receive proper and regular training to support their role?	
Cybersecurity Policies	Have you a documented security policy, with associated operating procedures, signed off and fully supported by senior management?	
Third Party Management	Does senior management authorise third party access to confidential and/or commercially sensitive information pending completion of appropriate confidentiality forms?	

Process

Check Item	Description	Answer
Audits	Are critical systems, such as firewalls and routers regularly tested for vulnerabilities? Are computers checked to ensure no copies of illegal software are present?	
Incident Planning and response	Are documented and frequently tested plans in place, with clearly defined roles and responsibilities, to ensure the company can respond to any security breaches such as a virus attack, fraud or natural disasters such as fire?	
Passwords	Are all default passwords on all systems reset from the default vendor installed passwords? Are users forced to use complex and hard to guess passwords?	
Software patches	Is there a mechanism to ensure that critical security patches are deployed to systems in a timely and audited fashion?	
Data Protection	Are systems and databases that store personal data secured properly to ensure compliance with regulatory and legal requirements such as the EU GDPR and the Data Protection Act?	

Technology

Check Item	Description	Answer
Network Security	Are external connections, such as to the Internet, authorised by senior management, properly documented and secured using Firewalls?	
Anti-Virus	Are all computer systems protected with the most up to date anti-virus software? Are users educated on how to identify and deal with suspect emails or files that may contain computer viruses?	
Encryption	Do all devices storing data have full disk encryption enforced? Do you user Virtual Private Networks (VPNS) when communicating over the Internet on public networks?	
Security Monitoring	Are the log files of important security devices actively monitored to detect potential security breaches?	
Physical security	Are critical IT resources, such as file servers, secured in a secured area that is protected from unauthorised access? Are home office measures in place ensuring secured areas comparable to the office (closed doors when leaving the workplace, no third party access to information via windows or else)?	
Secure Backups	A good backup may save your business from a ransomware attack. Do you regularly backup critical data and systems to secure offline storage? Do you regularly test restoring from your backups to verify you can fully recover your data and systems?	

5.1 PEOPLE RECOMMENDATIONS

5.1.1 Responsibility

Cybersecurity is clearly a key element in the ongoing success of any SME, in particular during the COVID19 pandemic, and it is only appropriate that responsibility for this critical function is assigned to someone within the organization. This role needs not necessarily be a new job posting as the responsibilities for cybersecurity could be integrated with the responsibilities of an existing role. However, it is vital that if integrating these responsibilities with another role that the appropriate resources, training and time are given to the person responsible for cybersecurity. Alternatively, this role could be outsourced to a third party provider specializing in the area of cybersecurity.

The role of cybersecurity point of contact (or manager, depending on your SME's naming conventions) will:

- act as a cybersecurity go-to contact, both internally and externally,
- implement management directions into real life practice,
- measure and report the SME's performance against the declared security objectives,
- monitor the SME for further security gaps and proactively provide executive staff with proposals for improvement.

In addition, if the SME has no data protection officer (DPO), he or she will also usually act as contact for privacy issues.

5.1.1.1 Management Commitment

Another critical success factor in effective cybersecurity is the commitment and the leadership exhibited by management. Without effective support from management, many initiatives within a business will fail. This applies to all aspects of the business but in particular to cybersecurity.

Cybersecurity demands resources such as time from personnel, the purchasing of cybersecurity software, services, and hardware, training for staff, and the development of effective policies. Management need to ensure those resources are available in a timely manner to ensure all cyber related threats and risks to the business are appropriately managed.

Management should actively support cybersecurity efforts by giving them priority as far as allocation of resources and budget is concerned. A key way to demonstrate leadership in this area is for management to be very visible in their own participation in security awareness training, ensuring that they comply with the company's own cybersecurity policies, and that they actively encourage staff to participate in trainings, support the decisions, policies and procedures and provide a vision regarding cybersecurity.

Finally, management within SMEs should ensure that cybersecurity is a standing item on the agenda for company management meetings; this is to guarantee that cybersecurity is regularly discussed at the highest level within the company and is not something that is thought of only when there is a problem.

5.1.2 Employee Buy-in

Just as important as having responsibility for cybersecurity assigned to an appropriate person and to have commitment from the SME's management to cybersecurity is ensuring employees buy in to having effective cybersecurity in place. It is essential that employees understand the importance that good cybersecurity is in protecting the organization, protecting the personal data entrusted by customers to that organization, and ultimately in protecting the employees' jobs.

Gaining employee buy-in for cybersecurity is critical and can only be got through effective communication on cybersecurity from management, by management openly supporting cybersecurity initiatives, appropriate trainings delivered to employees, and providing employees with clear and specific rules outlined in cybersecurity policies.

Every SME employee should have the answers to these questions:

- Am I allowed to access the company network and systems from a home computer? Can I access work email using my private smartphone? If so, what are the requirements?
- What is the process I need to follow when a supplier sends a request asking for their payment details to be changed?
- What should I do after receiving a phishing email?
- Am I allowed to use software that is not approved by my IT on my work computer?
- What is the approved method for me to share company data with others, especially those outside the company? Is there an approved file sharing platform that I can use?
- How can I access work email when accessing it over public Wi-Fi such as a hotel, airport, or indeed my home wireless network?
- How do I ensure my passwords are secure?

5.1.3 Employee Awareness

While technical controls can minimize the risks posed by various threats, the human factor is one that needs to be constantly managed. If staff are not made aware of cybersecurity threats, the reasons the SME has employed certain cybersecurity policies and controls, or how employees should react to a suspect security breach, then the risk of a security breach occurring increases significantly.

SMEs should provide regular cybersecurity awareness for employees to ensure they can recognize and appropriately deal with the various cybersecurity treats that face SMEs.

The security awareness program should be tailored for the audience and should focus on topics relevant to the audience's role. For example, the content of the training for people working in finance may be different for those working within the sales and marketing function.

Records of the training courses and those who attended should be maintained to ensure staff members have received the correct training.

Although financial and personal resources of small businesses may be limited, cybersecurity training does not necessarily mean hiring a specialized lecturer. There are great education sources on-line, and every SME will surely find one suitable to their needs. Basic tips include:

- Cover the main areas: how to recognize a phishing e-mail or an e-mail with a malicious link or attachment; why an unknown USB drive should not be plugged into any computer connected to the enterprise network; and why pirate software should not be installed.
- Do not forget to include basic physical security measures, like never leaving your laptop unattended, or locking devices when not in use.
- Consider testing your employees, and if you decide to do so, openly communicate it. After cyber awareness training, test them with a simulated phishing email of your own making. If they fail, do not *„name & shame"*, but educate further.
- Collect feedback on the training process and act accordingly, further customizing it to your needs.

The purpose of these training activities is not to make every staff member a cybersecurity expert, but rather to provide a basic understanding of the actual and practical cyber related risks, what the impact to the organization may be, and how their behavior can affect the outcome. Training should be practical and periodical, tailored to SME's special conditions and needs.

5.1.4 Cybersecurity Training

Many SMEs may have responsibility for managing and looking after their IT systems assigned to someone who may not be formally trained in cybersecurity. This may be someone internal to the SME or it could even be an outsourced IT provider, who has competence in IT but not necessarily in cybersecurity.

Staff responsible for cybersecurity who are not appropriately trained or experienced in the area may cause issues due to errors caused by lack of knowledge or experience. They may even not configure a system or device to be secured appropriately.

SMEs should ensure there is a formal cybersecurity training program, with the appropriate budgeting and resources, for those responsible for managing cybersecurity within the business.

Thus, they will have the skills and competencies required to ensure the security, availability, and ongoing operations of the IT infrastructure within the organization.

Should the SME have their IT and cybersecurity managed and supported by an external third party then the SME should engage with their provider to determine what level of competencies that provider had in cybersecurity and what plans do they have in place to ensure they have the appropriate level of competencies for cybersecurity in place.

5.1.5 Cybersecurity Policies

SMEs should set up clear and specific rules outlined in cybersecurity policies for its employees on how they are expected to behave when using the company's ICT environment, equipment, and services. These policies should also highlight the consequences an employee could face should they not adhere to the policies. The SME should ensure these policies are regularly reviewed, updated, communicated to employees, and that employees understand those policies,

Every SME employee should have the answers to these questions:

- Am I allowed to access the company network and systems from a home computer? Can I access work email using my private smartphone? If so, what are the requirements?
- What is the process I need to follow when a supplier sends a request asking for their payment details to be changed?
- What should I do after receiving a phishing email?
- Am I allowed to use software that is not approved by my IT on my work computer?
- What is the approved method for me to share company data with others, especially those outside the company? Is there an approved file sharing platform that I can use?
- How can I access work email when accessing it over public Wi-Fi such as a hotel, airport, or indeed my home wireless network?
- How do I ensure my passwords are secure?

The ideal policies should be short, succinct, with specific guidelines for employees to follow, and should be written in easy to understand language.

5.1.6 Third Party Management

Like all organizations, SMEs rely on other organizations to provide them with services. Some of these services may involve outsourcing of key business functions to a third party. Indeed, it is not uncommon for SMEs to outsource the management and support of their IT systems to another firm specializing in IT.

However, many of the arrangements in place with third parties, particularly concerning cybersecurity, are informal and may not have appropriate confidentiality clauses within the contract for service. SMEs should ensure that all vendors, particularly those with access to sensitive data and/or systems, should be actively managed to ensure they meet agreed service level commitments. Contractual agreements should regulate how the information will be accessed during the provision of said service and how will it be treated, as well as penalties, billing, guarantees and other aspects.

To ensure the security of services provided by Third Party vendors or outsourced partners, SMEs should:

- Develop a list of minimum cybersecurity requirements and obligations that vendors and suppliers must have in place in order for the SME to engage with them
- Regularly review and conduct an inventory of all its vendors and suppliers.
- Appoint someone with the responsibility to manage these relationships
- Ensure Service Level Agreements are in place with each key supplier and that these are managed and monitored on an ongoing basis.

  The above Service Level Agreements should clearly;

  - state the scope of the service being provided,
  - outline the roles and responsibilities for each party,
  - define clear lines of demarcation,
  - demonstrate the agreed cybersecurity level of the provided services,
  - detail how to report problems and associated escalation procedures,
  - include metrics by which the services are measured.
- Conduct regular reviews with suppliers, especially those managing data and/or services on behalf of the SME to ensure the security measures they implement are appropriate.
- Develop a process to manage the end of a service, either expected or unexpected, with a supplier. This process should ensure that any sensitive data that the vendor had access to are either securely destroyed or returned to the SME.
- Include a Non-Disclosure Agreement (NDA) or a confidentiality clause detailing what data is considered confidential, how long this confidentiality relationship will last, restrictions on the use of information by the service provider and the legal jurisdiction accepted.

If the external vendor provider requires access to any personal data under the care of the SME, a Data Processing Agreement should be put in place as per the requirements outlined in the EU General Data Protection Regulation (GDPR).

5.2 PROCESS RECOMMENDATIONS

5.2.1 Cybersecurity Audits

Without regular cybersecurity audits, or assessments, it is possible that issues will develop and go undetected by SMEs. Regular audits can help ensure any issues are identified and remedied before a breach. Regular cybersecurity audits also ensures an SME can have confidence that discipline and that its cybersecurity framework is being maintained. These audits can include assessments on the effectiveness of the cybersecurity policies that are in place. They can also test the technical controls to ensure the SME's firewalls, website, and other critical systems do not have any weaknesses that could allow an attacker to gain access.

Those with the appropriate knowledge, skills, and experience to conduct effective audits should carry out regular audits. These people could be internal to the SME. Ideally, they should be conducted by a party that is independent from the daily operations of the IT systems within the SME.

5.2.2 Incident Planning and Response

In today's environment, it is often not a question if a company will suffer a cybersecurity breach but more likely when will it suffer one. While in the past companies may have been judged for suffering a breach, today it is accepted that cybersecurity breaches do occur and that those organizations that suffer a breach are a victim of a crime. As such, many will not negatively judge an organization should it fall victim to a crime but they will judge the organization on how it responds to the incident.

Therefore it is important for SMEs to accept that at some stage they may suffer a cybersecurity breach and it is important to have a formalized incident response plan in place, as without such a plan the response to a cybersecurity incident will most likely be *ad hoc* and unplanned which often results in;

- Disclosure of confidential information.
- Prolonged recovery times.
- Lack of evidence for a criminal or civil case.
- Negative impact to the organisation's image.
- Potential legal and/or compliance Issues.
- Potential Legal Cases from Third Party Organisations.
- Exposure to Legal/Libel Cases from Employees/Individuals.

SMEs should develop a formal incident response plan, which contains clear guidelines, roles and responsibilities to ensure that all security incidents are in a professional and appropriate manner.

This policy should include details of how electronic evidence should be preserved, gathered and handled and each responsibilities.

Standard Operating Procedures to respond to incidents of different types should also be developed to include;

- The actions to be taken if multiple machines are infected with a computer virus.
- Under what conditions, and whose authority, network segments are shut down.
- Under what conditions, and whose authority, internet connectivity is disabled.
- How computer virus infections are identified and removed.
- Who liaises with the press, key stakeholders and public in the event of a serious incident?
- How to liaise with clients and partners, law enforcement, the Data Protection Supervisory Authority, or other regulators?

5.2.3 Passwords

One of the key layers of protection against unauthorized access to a company's data is the implementation of a suitable access control procedure. An SME should ensure its computer network could support the ability to centrally implement access control such as those provided by modern network systems like Microsoft Active Directory, or the Lightweight Directory Access Protocol (LDAP).

This will enable the SME to ensure those accessing its systems and data can be centrally managed and controlled. The ENISA Tips for secure authentication is an excellent resource that SMEs can refer to to help them address this challenge

When dealing with credentials and more specifically passwords, SMEs should ensure that employees:

- use strong passwords or passphrases which should be long, with lower-and upper-case characters, possibly also numbers and special characters.

  It is preferable that employees use a passphrase – a collection of random common words combined into a phrase that provide a very good combination of memorability and security. For example, three random words like:

  ''ogre swingy glamor''

  present a very strong password and if it can be sprinkled with uppercase characters or numbers, it's even stronger. Many national authorities, like UK National Cybersecurity Centre, also vet the passphrase approach[57].

  The French Commission Nationale de l'Informatique et des Libertés (CNIL, National Commission on Informatics and Liberty) recommends to organizations that process personal data and employ authentication based only on an identifier (e.g. username) and a password, that *"password should have a minimum of 12 characters, and .. must include upper-case letters, lower-case letters, numbers, and special characters."*[58]

  Whatever approach you choose, stay away from the obvious, like using word *"password"*, sequences of letters like *"abc"*, sequences of numbers like *"123"*, keyboard paths like *"qwerty"* on English language keyboards, and your real life data like date of birth or name of your high school. In password creation, randomness is your friend.

- do not reuse their work passwords elsewhere
- do not attach Post-it notes detailing passwords to their screens or leave passwords otherwise accessible in written form (they should be encouraged to use a password manager instead),
- We recommend the use of a dedicated password manager (usually superior in features to the browsers in-built password managers), as they help to keep strong, unique passwords.

[57] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[58] https://www.cnil.fr/sites/default/files/atoms/files/recommandation_passwords_en.pdf

- do not to share their passwords with colleagues (nor user accounts)
- **Where possible, enforce Multi-Factor Authentication.**

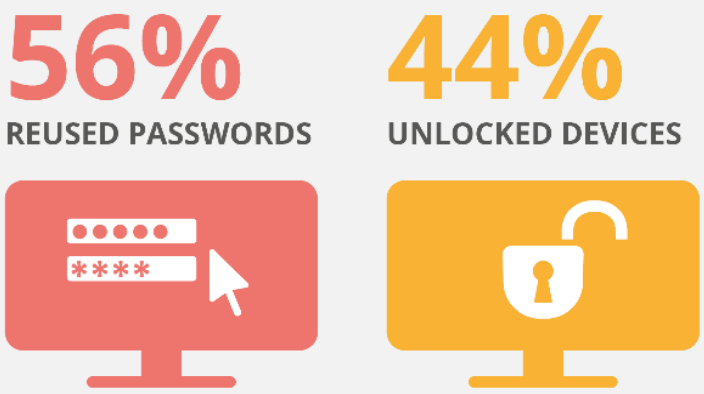
Figure 18: Multi-factor authentication technologies

Many services now provide Multi-Factor Authentication (MFA)[59], which is an additional step outside of entering a password to verify that the person trying to access the system is indeed who they claim to be. This often is done by either sending a text message to a known number for the account holder, using an app that supports authentication, or by using physical tokens, which must be present at the time of accessing the account.

Once an employee leaves that organization, the SME should also ensure that they revoke the employee's access to business systems if they leave the business.

Master passwords may be stored as part of SME's contingency planning or to provide backup if some of the administrators is unavailable. However, they need to be stored in a safe place and accessible only to authorized personnel.

Figure 19: Overview of weak password issues



According to the ENISA Threat Landscape Report 2018, weak or reused passwords (56%) and unlocked devices (44%) represent two of the highest risks.

An incident connected with the malfunction of passwords, is one experienced by Twitter. Specifically, a glitch in the password handling procedure potentially exposed all users' passwords in plain text before completing the hashing process. (ca. 330 million)[60].

[59] *https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods*
[60] *https://www.bbc.com/news/business-43995168*

5.2.4 Software Patches

Software updates fix known security vulnerabilities, and may improve the functionality and performance of your program or device. SMEs need to be prepared to upgrade their systems on a regular basis due to software and hardware becoming out of date. An SME's IT infrastructure should be treated the same way as any other business infrastructure and modernised on a regular basis;

- Update all of their software.
- Set up a systematic procedure to keep it that way.
- Turn on automatic updates whenever possible.
- Identify software and hardware that requires manual updates
- Take into account mobile and IoT devices.

SMEs should look at implementing solutions that allows them to centrally manage and control how and when software patches are applied. This will also enable the SME to have visibility as to what devices may not have been successfully patched and may need additional attention to remedy.

A well-known example of how a major security incident happened due to a vulnerability being exploited before organizations were able to patch their systems was with the "**WannaCry**"[61] **ransomware attack**. It is estimated that 230,000 organizations in 150 countries fell victim to these attacks. The estimated losses were 4-8 Billion US $[62]. WannaCry indiscriminately targeted vulnerable systems that ran specific versions of the Windows operating systems with many SMEs falling victim.

5.2.5 Data Protection

Under the EU General Data Protection Regulation any SMEs that process or store personal data belonging to those resident within the EU/EEA are required to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. The Irish Data Protection Commission provides a guide on the security measures expected to be in place.[63]

5.3 TECHNICAL RECOMMENDATIONS

5.3.1 Network Security

According to the results of the online survey, a firewall solution has been implemented by at least 86% of the participants even before the COVID19 crisis. This percentage appears to have risen further (90%) during the crisis.

[61] *https://www.europol.europa.eu/wannacry-ransomware*
[62] *https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cybercrime-and-exploits-attacks-on-unpatched-systems*
[63] *https://dataprotection.ie/en/dpc-guidance/guidance-controllers-data-security*

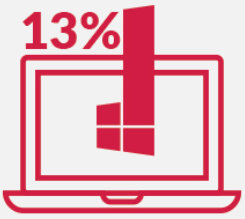
Firewalls filter and monitor the incoming and outgoing traffic on the perimeter of trusted and untrusted networks based on given rules. The effective configuration of these rules is a key success factor, and should be implemented and gradually tuned up with care. Firewalls may also provide and manage remote access to the organization by supporting Virtual Private Networks (VPNs).

When selecting a firewall an SME should also look to see, what additional security features are provided, either by default or by paying extra fees. Some of these features could include filtering email and web traffic for malicious software such as viruses, blocking access to known bad sections of the Internet, and providing alerting and monitoring to potential attacks.

Given the important role firewalls play in protecting an SME's internal network and systems, SMEs should ensure they employ the most appropriate firewall for their needs. This may require engaging with someone who has the relevant expertise that can recommend that most appropriate solution.

5.3.2 Anti-Virus

Figure 20: 13% increase since 2019 in Windows malware detections



Despite the increased awareness and implementation of anti-virus solutions, the ENISA Threat Landscape Report 2020 shows that there was a 13% increase since 2019 in Windows malware detections at business endpoints globally and that 71% of organizations experienced malware activity that spread from one employee's computer to another. The report also highlighted that malware attacks have grown in volume and in sophistication.

Anti-virus software is one of the most commonly used cybersecurity tools for endpoint protection. It protects against various kinds of malware, unauthorized malicious software designed to cause harm. Malware can gain access to important information such as bank credentials, credit card numbers or passwords. It can also take control or spy on a user's computer.

The majority (88%) of the survey participants already implemented some form of anti-virus solution even before the COVID19 pandemic, and the number appears to have further risen (>90%) during the COVID19 pandemic.

An anti-virus solution should be implemented on all types of devices and kept up-to-date in order to ensure its continuous effectiveness. This includes employees' tablets and smartphones connected to the company network, be it in SME's or their ownership. This anti-virus solution should provide the SME with the ability to manage centrally the anti-virus software installed on all devices within the organization and ensure that it is kept up to date. Should the anti-virus software on any of the devices detect a potential infection, it should also alert the appropriate personnel within the SME to deal with the situation.

5.3.3 Employ Email and Web Protection Tools

Email remains a major attack medium and a way to gain a foothold within the systems of an organization. Malicious e-mails may come in the form of e-mails with malicious attachments, e-mails containing links to malware distribution sites, phishing e-mails, or scam e-mails tricking SMEs into revealing their sensitive data or sending money.

Phishing emails can be very sophisticated, leveraging social engineering practices – creating a sense of urgency, and often mimicking phrasing, branding and logos of a well-known institution (such as a bank or a business partner) or just a colleague. Phishing or fraudulent emails target employees within an SME to trick them into giving away sensitive personal or enterprise information, such as passwords or credit card numbers. One popular form of malicious emails targeting SMEs are invoice redirect scams, where cybercriminals create a fake email to look like it comes from known supplier requesting the account payment details for the supplier be changed to one controlled by the criminals.

The fact that SME staff may have a low awareness regarding this type of malicious behavior makes them ideal candidates for criminals to exploit. In tandem with cyber awareness trainings, SMEs should implement rules that will not allow change of payment details or transfer of funds based on an email only. Such an important step should also be confirmed using a different communication channel (in person, by phone, using live videoconference etc.) to prevent cyber criminals from taking advantage.

The overwhelming amount of news coverage surrounding the novel coronavirus has also created a new danger — phishing scams looking to exploit public fears about the sometimes-deadly virus. These fraudulent emails assert to be sent from the World Health Organization or the US Centre for Disease Control or a renowned specialist offering information or help regarding COVID-19. You can find ENISA's advice that is more detailed on how to protect against phishing attacks in an article on phishing during the COVID-19 pandemic[64].

Employees at SME should also know basic web browsing security practices, like how to spot fraudulent pages and stay clear from installing suspicious browser plug-ins.

In order for organizations to be better prepared against these types of attacks, it is necessary to combine solutions that will filter out the possible spam emails, email containing link to a malicious website, emails containing a malicious attachment (i.e. containing a malware payload), or phishing attempts with relevant and practical training of the organization's staff.

5.3.4 Encryption

Encryption is information that is scrambled in such a way that only those with the appropriate access can unscramble that data to read it. Encryption therefore provides strong protection for sensitive data. Where possible SMEs should use encryption to protect data when it is being stored or being transferred over public networks such as the Internet.

Due to their portable nature, mobile devices, such as laptops and smartphones, are more likely to be lost or stolen. While the cost of the mobile device itself may not be high the value of the data held on the device could be quite high. Many modern operating systems have encryption features built into them, which SMEs should enable to ensure the data stored on mobile devices are encrypted.

For data that is transferred over public networks, such as hotel or airport Wi-Fi networks, or over the Internet, SMEs should ensure that data is encrypted, by either employing a Virtual Private Network (VPN) from a trusted provider or accessing websites over secure connections using SSL/TLS protocol.

[64] https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic

Similarly, for their own websites, especially if that site is being used to support online transactions, SMEs should ensure they are employing suitable encryption technology to protect client data as it travels between the SME's server and the clients' devices.

5.3.5 Security Monitoring

Many of the systems and devices which SMEs employ, such as servers, firewalls, and anti-virus software, can log and record system activity to support troubleshooting and maintenance. In many cases, this also includes recording any suspicious activity that could be related to a potential security breach. However, by default there is often no facility to generate alerts, which often results in breaches occurring without the victim organizations being aware.

So while SMEs may have the data to alert them to suspicious activity on their systems or breaches that data is not being actively monitored to alert the SME to these incidents. This is similar to having a burglar alarm installed on the premises but not turning it on. SMEs should investigate tools that could monitor and create alerts when suspicious activity or security breaches are occurring.

5.3.6 Physical Security

Physical security is an important aspect of an overall cybersecurity program. Sensitive data can be stored in electronic format and in physical format such as on paper. If there is no appropriate physical security to protect the data, then criminals can quickly undermine the cybersecurity controls that may be in place. It is therefore important to ensure appropriate physical controls are employed where important information resides.

A company laptop or a smartphone, for instance, should not be left unattended in the back seat of a car, and the same principle applies for information on USB drives or prints on a sheet of paper. To prevent unauthorized access, anytime a user walks away from their computer, be it on the company premises or elsewhere, they should lock it. Setting auto-lock function, using full disk encryption and if possible purchasing laptops with TPM chips are a number of measures that could reinforce physical security. Sensitive printed documents should also not be left unattended and when not in use securely stored away.

Figure 21: Result of the Hørsholm Municipality security breach

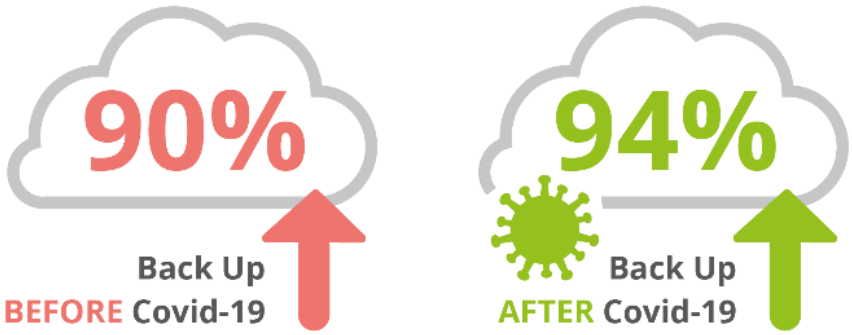
The Danish Data Protection Authority imposed a fine on the Hørsholm Municipality resulting from a security breach that happened when an employee had their municipality issued laptop stolen from their car. On the stolen laptop was personal data of approximately 1,600 employees at Hørsholm Municipality, including information of a sensitive nature and information about social security numbers.

5.3.7 Secure Backups

According to our online survey, more than 90% of the participants were already taking some kind of backup even before the COVID19 pandemic. This percentage appears to have risen further (>94%) during the COVID19 pandemic.

Irrespective of the root cause, the company should be able to recover its information within a desirable period. **To enable the recovery of the information, backups should be kept, as they are an effective way to recover for example from ransomware.** The exact technology employed (sophisticated dedicated software, simple scripts or manual backups) remains at the choice of the organization. In every case, the following rules should apply:

Figure 22: Increase of back-up policies



- backup is regular and automated whenever possible,
- backup is held separately from the SME's production environment, i.e. the network that employees directly interact with,
- backups are encrypted, especially if they are going to be moved between locations,
- the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done.

To ensure an SME has an effective backup strategy the SME should consider employing the common easy-to-remember so-called 3-2-1 rule approach to safeguard data against most failure scenarios:

Figure 23: 3-2-1 rule to safeguard data

A retention period should be set and implemented based on the specific circumstances of the organization. In other words, backup iterations should be set according to business reality of each company, so the cost of lost data in a given timespan is acceptable. Backup practices need to be tailored according to the SME infrastructure (on premise vs cloud).

In 2017, GitLab experienced an incident, and had to go offline after suffering what appears to be a major backup restoration failure after accidentally deleting production data. As mentioned in the company's blog "out of five backup/replication techniques deployed none are working reliably or set up in the first place. We ended up restoring a six-hour-old backup" [65] (This means that data created in the meantime between the last backup and the time of the incident were lost).

5.4 COVID19 SPECIFIC RECOMMENDATIONS

As stated earlier in this document, many SMEs had to react quickly to the impact of the COVID19 pandemic and the subsequent widespread lockdowns that many member states implemented to protect the lives and health of citizens. However, this quick reaction to the pandemic meant that most SMEs simply focused on keeping their business operating and took what the necessary steps to ensure staff could work remotely and in some cases, SMEs changed their business models to service their customers online rather than in traditional face-to-face situations.

With this background in mind, it is not surprising that SMEs focused primarily on ensuring their ICT environments operated in such a way to support the SMEs business goals. Cybersecurity may not have been a major factor in deciding how to meet those business goals. This focus on keeping the business running is understandable. However, in the rush to achieve this goal key cybersecurity measures may not be implemented properly or not implemented at all.

This section of the report will highlight several areas SMEs should examine to ensure the security of their data, services, and systems.

5.4.1 Review Remote Access Facilities

In response to the pandemic many SMEs installed various ways to enable staff to access remotely the SME's network. This could be installing or upgrading a Virtual Private Network (VPN) for the organization, or installing remote desktop management tools, enabling remote connecting protocols such as the Remote Desktop Protocol (RDP), or by installing other remote access technologies.

SMEs should now review any remote access facilities to ensure they are secure. The following are the key things SMEs should focus on;

- Ensure all remote access software is patched and up date.
- Implement a tool or a process to ensure that remote access software will continue to be patched and kept up to date.
- Review the remote access settings to restrict access from known or trusted locations, such as restricting remote access to staff based in certain geographical locations or accessing from certain IP addresses.
- Restrict staff accessing systems remotely to only the systems and computers they need access to.
- Enforce strong passwords for remote access and where possible enable multi-factor authentication.
- Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.

[65] https://about.gitlab.com/blog/2017/02/01/gitlab-dot-com-database-incident/

5.4.2 Engage with the Cloud

Many Cloud Service Providers (CSPs) can offer services that will enable SMEs continue to support their staff working remotely. These can range from providing email platforms, file-sharing facilities, and video conferencing, to online collaboration tools. In most cases, the CSP can secure the services being provided to the SME much more effectively and efficiently than the SME.

As mentioned earlier in the report SMEs should ensure they keep software installed on their computer systems patched and up to date. They also need to ensure their anti-virus solution is managed so that it is kept up data on all devices. Traditionally these two functions were often managed using servers and software installed on the SME's own network. However, with many staff working remotely these solutions many not be as effective.

Moving to cloud based patch management and cloud based anti-virus platforms can provide the SME with the capability to ensure that their IT infrastructure is being managed and secured.

While offering many advantages, cloud based solutions do provide some unique risks. SMEs should consider them before engaging with a CSP. ENISA have published a "Cloud Security Guide for SMEs"[66] which SMEs should refer to when migrating to the cloud.

The following are some of the key items an SME should consider before engaging with a CSP;

- Determine the physical location where the SME's data will be stored. This is important to ensure the SME does not breach any laws or regulations by storing data, especially personal data, in CSPs located outside of the EU/EEA. For example, the EU GDPR requires that personal data of residents within the EU/EEA is not stored or transmitted outside of the EU/EEA unless under very specific conditions.

- Implement Multifactor Authentication to ensure that cloud based accounts are at a lesser risk of being hijacked by criminals. Without MFA implemented on CSP based services the only protection for the accounts that access those CSP based services are the passwords people employ on their accounts. If those passwords are weak, have been reused from other websites, or the account holder falls victim to a phishing attack, then that could result in a security breach. MFA provides an additional layer of protection to help prevent this from happening.

- Many cloud services are provided with built-in security features, however these are often turned off by default. SMEs should make sure they understand what the security features are in the service they are subscribing to and enable them. If the security features at the current plan the SME is using are not adequate the CSP may offer the required features at a different plan, which the SME could subscribe to.

[66] *https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes*

5.4.3 Implement Mobile Device Management

When facilitating staff to work remotely many SMEs allowed their staff to use their own personal devices such as computers, laptops, tablet, and/or smartphones. While this may have helped ensure the SME could continue to provide services to its client, it also introduced several security concerns about the SME's data stored on those personal devices. One way for an SME to manage this risk is to employ a Mobile Device Management (MDM) solution. With a MDM solution a SME could

- Control what devices are allowed to access its systems and services.
- Ensure the device has up to date anti-virus software installed.
- Determine if the device is encrypted.
- Confirm if the device has up to date software patches installed.
- Enforce the device is protected by a PIN and/or a password.
- Remotely wipe any SME data from the device should the device owner report it lost or stolen, or if the device owner's employment was to end with the SME.

5.4.4 Conduct Appropriate Security Awareness Training

Criminals will take advantage of all situations if it results in them achieving their goals. The COVID19 pandemic is a perfect scenario for criminals to exploit as they can leverage of the fears and concerns that people have regarding the pandemic. Criminals will look to compromise accounts and systems using COVID19 themed phishing emails, or use scam emails pretending to be from couriers to spread malicious software.

In addition, many staff will now be working remotely from their own homes and may not be working from a network or device as secure as that provided within the SME's own office environment.

With this in mind, it is important for SMEs to ensure staff are regularly updated on what the latest cybersecurity themed threats are and how they should work securely while working remotely.

The Irish Data Protection Commission have issued a guide, "Protecting Personal Data When Working Remotely"[67] for companies so they can ensure personal data entrusted ot them is secured when staff are working remotely.

5.4.5 Secure Online Sites

Many SMEs moved from engaging directly with their customers in face to face to dealing with them via online. SMEs rushed to set up new websites so they could sell to their customers online. However, it is essential that SMEs ensure that their online websites are configured and maintained in a secure manner. Any personal data or financial details, such as credit card data, must be appropriately protected. This will entail running regular security tests against the websites to identify any potential security weaknesses and conducting regular reviews to ensure the site is maintained and updated properly.

[67] *https://dataprotection.ie/en/dpc-guidance/blogs/protecting-personal-data-when-working-remotely*

5.4.6 Information Sharing

An effective tool in the fight against cybercrime is the sharing of information. Many firms are afraid of publicly discussing cybersecurity issues, in particular details about breaches, as they fear negative publicity resulting from their perceived weakness in relation to cybersecurity. However, while this may be true in the past, this is no longer the case as many firms realize that they cannot deal with this issue by themselves.

The sharing of information in relation to cybercrime is key to SMEs to understand better the risks they face. Firms that hear about cybersecurity challenges, and how those challenges were overcome, from their peers will more likely take steps to secure their systems than if they were to hear similar details from industry reports or from cybersecurity surveys.

A key element in facilitating information sharing is with ISACs, as outlined in our recommendations at the EU and National level. However, until ISACs are in place SMEs can use other mechanisms to share good practices for cybersecurity, alerting others to potential attacks, or how to recover from a breach. Similar to neighborhood watch schemes in the real world, information-sharing networks in relation to cybersecurity, can quickly improve security for all. SMEs can look to existing bodies to facilitate this information sharing. Bodies such as chambers of commerce, industry representative bodies, or local business associations all provide a useful platform to facilities information sharing and education. These bodies could also engage with cybersecurity experts to address their members at meetings or conferences to ensure they are aware of the latest threats and the good practices that SMEs can employ.

5.5 MAPPING THREATS TO RECOMMENDATIONS

The survey identified the typical cybersecurity issues experienced by SMEs. These are outlined in Figure 6. The following table demonstrates how these cybersecurity issues can be managed by the above recommendations;

Table 3: Mapping threats to recommendations

Issues	Categories	Recommendations
 **Phishing**	People	Employee Buy-in Employee Awareness Cybersecurity Training Cybersecurity Policies
	Process	Incident Planning and Response Passwords (implement Multi-Factor Authentication)
	Technical	Network Security Security Monitoring
 **Web Based Attack**	People	Cybersecurity Training Cybersecurity Policies Third Party Management
	Process	Audits Incident Planning and Response Passwords Software Patches Data Protection
	Technology	Network Security Anti-Virus Security Monitoring Secure Backups
 **General Malware**	People	Employee Buy-in Employee Awareness Cybersecurity Training Cybersecurity Policies
	Process	Audits Incident Planning and Response Passwords Software Patches Data Protection
	Technology	Network Security Anti-Virus Encryption Security Monitoring Secure Backups

Issues	Categories	Recommendations
 **Malicious Insider**	People	Employee Buy-in Employee Awareness Cybersecurity Training Cybersecurity Policies
	Process	Audits Incident Planning and Response Passwords Software Patches Data Protection
	Technology	Network Security Anti-Virus Encryption Security Monitoring Physical Security Secure Backups
 **Denial of Service**	People	Cybersecurity Training Cybersecurity Policies Third Party Management
	Process	Audits Incident Planning and Response Passwords Software Patches Data Protection
	Technology	Network Security Anti-Virus Security Monitoring Secure Backups
 **Social Engineering**	People	Employee Buy-in Employee Awareness Cybersecurity Training Cybersecurity Policies
	Process	Incident Planning and Response Passwords (implement Multi-Factor Authentication)
	Technical	Network Security Security Monitoring
 **Compromised/Stolen Device**	People	Employee Buy-in Employee Awareness Cybersecurity Training Cybersecurity Policies
	Process	Audits Incident Planning and Response Passwords Data Protection
	Technology	Encryption Physical Security

6. EU AND NATIONAL LEVEL RECOMMENDATIONS

The following recommendations are directed towards Regional, National and European Authorities with the purpose of assisting SMEs in adopting cybersecurity solutions.

It is important to outline that most SMEs who participated in the survey and the interviews highlighted the lack of applicability and usefulness of the various measures, guidelines, and approaches to dealing with cybersecurity that some Member State authorities have proposed to SMEs for adoption.

This shortcoming of existing measures will hopefully be overcome, as this part of the study, provides recommendations towards policy makers of all levels of government that have been derived and validated by the affected parties (the SMEs).

6.1 PROMOTE CYBERSECURITY AT LARGE

Specific awareness raising campaigns on cybersecurity issues, which educate SMEs owners, managers, employees and shareholders, should be created by the relevant authorities and where possible in partnership with business representative organizations. Such practices will help the organizations to understand how they can protect their businesses and which resources, such a guidelines, standards, and tools they could possibly use. These campaigns should be orchestrated within Europe but adjusting its pace and content to specific regional cases.

However, experience has shown that despite regular campaigns, many SMEs do not engage in these campaigns or the campaigns do not effectively reach the target audience. As such, future campaigns need to be more focused on the SME sector as a target. It is recommended, that these campaigns should be run regularly and be customized depending on the topic being promoted at the time. It is essential that the content is aimed at the needs of the intended audiences, primarily SMEs, hence the need to partner with business representative organizations who can highlight those needs to those designing the campaigns. The campaigns should aim at helping SMEs to understand cybersecurity threats and how these threats can affect people, in both their personal and professional lives. Finally, the methods of implementation should be carefully selected, in particular as to how the campaigns are delivered to the SMEs. It may require tailored content for each business sector with the emphasis placed on the key issues affecting that business sector (for example, cybersecurity issues relating to online shopping may not be relevant to business sectors that do not use the Internet to sell their goods and services).

The effectiveness of these campaigns must be measured to ensure the key messages are being delivered and that cybersecurity within SMEs is improving. This could be achieved by conducting regular surveys similar to the one conducted to support this report, by gathering feedback from SMEs after a campaign has been completed, and by analysis reports of cybercrime incidents to law enforcement agencies, Computer Emergency Response Teams (CERTs), and Data Protection Supervisory Authorities

Note: This type of training is different from the one mentioned in section 5.1.3. The desired results after the implementation of this recommendation is the increase in the awareness regarding cybersecurity within the SME sector in general.

6.2 PROVIDE TARGETED GUIDELINES AND TEMPLATES

It has been pointed out from the contributions to the online survey and the subsequent follow up interviews that there are many generically written guides in relation to cybersecurity, such as cybersecurity standards and relevant laws and regulations, which outline what should be done. For example, the EU General Data Protection Regulation states in Article 32[68] that:

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk…".

Although the meaning of this requirement is clear, the implementation path for an SME with limited resources and knowledge on cybersecurity is anything but clear.

As most SMEs are not aware of either specific standards or methods and techniques for implementing security and privacy measures, easy to use, clear and structured implementation guidelines, plans, procedures, and exercises should be developed to assist SMEs bridge this gap.

Good practices handbooks including realistic and specific examples, simple terms and easily translatable language should be prepared. These guidelines and templates should be especially adapted to the characteristics of SMEs and should be adaptable based on the criticality of information processed by the SME, the industry and their dependence on ICT.

Public-private collaboration is proposed through collaboration with SME representative bodies, appropriate public sector organizations, and, where there is no conflict of interest, cybersecurity companies for the better definition and content of these guidelines, exercises, procedures, handbooks and standards.

6.3 CREATE SME FOCUSED CYBERSECURITY STANDARDS

A standard is a document designed to be used as a rule, guideline or definition. It is a consensus-built, repeatable way of doing something. Standards are created by bringing together all interested parties such as manufacturers, consumers and regulators of a particular material, product, process or service[69]. However, SMEs often have a minority contribution in these standardization efforts and the resulting work rarely makes specific provisions for SMEs.

There are many existing standards for cybersecurity, which are not adopted by SMEs. There are various reasons why this may be the case. Primarily due to the fact that cybersecurity standards are suitable for larger organizations and not SMEs. However, this should not

[68] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[69] https://www.cen.eu/work/ENdev/whatisEN/Pages/default.aspx

necessarily be the case. SMEs should be encouraged to adopt cybersecurity standards. Tailored guidance and implementation guides for SMEs on how to adopt these existing cybersecurity standards should be created.

In addition, it is important that good practices and guidelines are created and published for cybersecurity and that they are developed based on the needs of SMEs. Participation of SMEs in all stages of the standards' lifecycle must be ensured, from their participation in standardization committees to the final standard use and adoption. Standards focused primarily on SMEs, similar to the Cyber Essentials, should be considered.[70]

Furthermore, SMEs are reminded that adhering to cybersecurity standards, while it is a positive measure in improving the cybersecurity for the organization, it is no guarantee that systems are 100% secure. Cybersecurity standards are a means to manage the risk related to cybersecurity but do not eliminate that risk.

The Belgian guide for SMEs[71] includes basic but also advanced measures to enable SMEs to improve their cybersecurity levels, reduce cybersecurity risks, mitigate vulnerabilities and improve their resilience.

6.4 BOLSTER USE OF RISK MANAGEMENT FRAMEWORKS

Throughout this document, various risks related to cybersecurity have been presented. Each organization (small or large) has to identify, assess and evaluate these risks, decide on based on their business requirements how they will manage those risks. This process is known as Risk Management and presents a crucial decision making tool that can be fitted to every organization including SMEs.

There is a huge variety of standards, tools, methodologies and techniques that could be used to identify key cybersecurity risks. Many of these tools are outlined in the ENISA "Inventory of Risk Management/Risk Assessment Methods & Tools[72]". However, in many cases there is a lack of simplified and practical risk management solutions aimed at the SME sector.

Risk Management frameworks that are practical, easy to understand, easy to translate to business terms, easy to implement without specialized knowledge, and scalable to SMEs need to be designed and promoted. Similar to the Dutch VNO-NCW Cyber Risk guide for SMEs[73].

Promoting the use of these risk frameworks and providing instructions on how to apply them should be encouraged by Member States.

[70] https://www.ncsc.gov.uk/cyberessentials/overview
[71] https://ccb.belgium.be/en/document/guide-sme
[72] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory
[73] https://www.vno-ncw.nl/standpunten/cybersecurity

EBIOS (**E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité - Expression of Needs and Identification of Security Objectives) is a method for analysis, evaluation and action on risks relating to information systems. It generates a security policy adapted to the needs of an organization. The method was created in 1995 and is now maintained by the ANSSI, a department of the French Prime Minister.

The **IT baseline protection** (German: IT-Grundschutz)[74] approach from the German Federal Office for Information Security (BSI) is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. To reach this goal the BSI recommends "well-proven technical, organizational, personnel, and infrastructural safeguards".

MONARC (Method for Optimised Analysis of Risk CASES) of the Ministry of Economy in Luxembourg. The advantage of MONARC lies in the capitalisation of risk analysis already performed in similar business contexts: the same vulnerabilities regularly appear in many businesses, as they face the same threats and generate similar risks. Most companies have servers, printers, a fleet of smartphones, Wi-Fi antennas, etc. Therefore, the vulnerabilities and threats are the same. Thus. it is sufficient to generalise risk scenarios for these assets (also called objects) by context and/or business.

6.5 MAKE CYBERSECURITY AFFORDABLE

As mentioned in the Challenges section, cybersecurity bears a cost for organizations and in particular for SMEs who due to lack of understanding or awareness may not budget appropriately for cybersecurity solutions. These costs can relate to the purchasing of cybersecurity products, services, external consulting service, and other related costs. These costs may play the leading role in the decision whether or not to implement cybersecurity measures and to which extent.

The vast majority of the participants in this survey highlighted that they need help in this area. It is recommended, that the relevant bodies in Member States consider assisting SMEs in this area by implementing any of the following actions:

- Improving access to competent cybersecurity advice or guidelines.
- Providing funding for the strengthening of the SMEs cybersecurity posture.
- Providing tools to lower the cybersecurity solutions price per SME (using more effective procurement methods and systems, pooling demand[75], etc.)

For example many SMEs (in particular the smaller ones) use cloud services, which are managed by the provider under standard contract clauses and fixed Service Level Agreements (SLAs). Individual SMEs due to their size have no advantage or ability to negotiate suitable SLAs, something which larger organizations may be able to do so. In larger numbers, SMEs might develop customized SLAs or contract clauses to fit better their cybersecurity needs.

[74] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
[75] https://en.wikipedia.org/wiki/Pooling_(resource_management)

6.6 PROMOTE THE CREATION OF ISACS

Information Sharing and Analysis Centers (ISACs)[76] are important instruments to ensure close cooperation between public and private stakeholders within different business sectors. ISACs are non for profit organizations set up within a business sector or focusing on a common theme for various businesses to enable those businesses to share experiences regarding cybersecurity. This could be advice on best practises for those who are members of the ISAC on how to deal with cybersecurity issues, providing warnings relating to cybersecurity issues specific to the ISAC, and guidelines and best practises on how to manage cybersecurity.

Participation of SMEs in ISACs could greatly enhance the SMEs cybersecurity posture, particularly if the ISAC is aimed at the SME sector, or can facilitate the cybersecurity concerns specific to SMEs. ENISA has done substantial work on the topic of ISACs to identify the different ISAC models in Europe through the report on Cooperative Models on ISACs[77]. Moreover, ENISA recently published the ISAC in a BOX[78], an online toolkit created around a lifecycle of building, running, evaluating and developing phases and each phase includes information, activities, documents, tools for setting up and running an ISAC. There is also available from ENISA the report on “Public Private Partnerships (PPP) - Cooperative models”[79] which Member States can refer to when designing the appropriate ISACs.

[76] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[77] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models
[78] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view
[79] https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

A ANNEX: METHODOLOGY

A.1 SMES IN EU

According to the latest (November 2019) ANNUAL REPORT ON EUROPEAN SMEs 2018/2019 of the European Commission[80]:

- There were slightly more than 25 million SMEs in the EU-28 in 2018, of which 93% were micro SMEs. SMEs accounted for 99.8% of all enterprises in the EU-28 nonfinancial business sector (NFBS), generating 56.4% of NFBS value added and 66.6%of NFBS employment. Overall, the NFBS represented 54.5% of EU-28 GDP and 61.4% of total EU-28 employment.
- Micro SMEs are by far the most common type of SME, accounting for 93.0% of all enterprises and 93.2%6 of all SMEs in the NFBS. However, micro SMEs accounted for only 29.7% of total employment in the NFBS, while small and medium-sized SMEs accounted respectively for 20.1% and 16.8% of total NFBS employment.

To help in the extraction of information on cybersecurity in SMEs, a predefined set of industry sectors was utilised. The industry sectors used were derived from the Annual Report on European SMEs 2018/2019 and the NACE Rev. 2 statistical classification of economic activities in the European Community81

Table A.1: Industry sections and descriptions

Industry section	Brief Description
Accommodation and food service activities	This section includes the provision of short-stay accommodation for visitors and other travellers and the provision of complete meals and drinks fit for immediate consumption. The amount and type of supplementary services provided within this section can vary widely. This section excludes the provision of long-term accommodation as primary residences, which is classified in real estate activities. Also excluded is the preparation of food or drinks that are either not fit for immediate consumption or that are sold through independent distribution channels, i.e. through wholesale or retail trade activities. The preparation of these foods is classified in manufacturing.
Administrative and support service activities	This section includes a variety of activities that support general business operations. Examples of activities belonging to this section are: Rental and leasing activities, Employment activities, Travel agency, tour operator and other reservation service and related activities, Security and investigation activities, Services to buildings and landscape activities and Office administrative, office support and other business support activities.
Construction	This section includes general construction and specialised construction activities for buildings and civil engineering works. It includes new work, repair, additions and alterations, the erection of prefabricated buildings or structures on the site and also construction of a temporary nature. Also included is the repair of buildings and engineering works.

[80] https://ec.europa.eu/growth/smes/sme-strategy/performance-review_en#annual-report
[81] https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF

Industry section	Brief Description
Electricity, gas, steam and air conditioning supply	This section includes the activity of providing electric power, natural gas, steam, hot water and the like through a permanent infrastructure (network) of lines, mains and pipes. The dimension of the network is not decisive; also included are the distribution of electricity, gas, steam, hot water and the like in industrial parks or residential buildings. This section therefore includes the operation of electric and gas utilities, which generate, control and distribute electric power or gas. Also included is the provision of steam and air-conditioning supply.
Information and communication	This section includes the production and distribution of information and cultural products, the provision of the means to transmit or distribute these products, as well as data or communications, information technology activities and the processing of data and other information service activities.
Manufacturing	This section includes the physical or chemical transformation of materials, substances, or components into new products. The materials, substances, or components transformed are raw materials that are products of agriculture, forestry, fishing, mining or quarrying as well as products of other manufacturing activities. Substantial alteration, renovation or reconstruction of goods is generally considered to be manufacturing.
Mining and quarrying	Mining and quarrying include the extraction of minerals occurring naturally as solids (coal and ores), liquids (petroleum) or gases (natural gas). Extraction can be achieved by different methods such as underground or surface mining, well operation, seabed mining etc. This section includes supplementary activities aimed at preparing the crude materials for marketing, for example, crushing, grinding, cleaning, drying, sorting, concentrating ores, liquefaction of natural gas and agglomeration of solid fuels. These operations are often accomplished by the units that extracted the resource and/or others located nearby.
Professional, scientific and technical activities	This section includes specialised professional, scientific and technical activities. These activities require a high degree of training, and make specialised knowledge and skills available to users. Activities contained within this section are Legal and accounting activities, Activities of head offices; management consultancy activities, Architectural and engineering activities; technical testing and analysis, Scientific research and development, Advertising and market research, Other professional, scientific and technical activities.
Real estate	This section includes acting as lessors, agents and/or brokers in one or more of the following: selling or buying real estate, renting real estate, providing other real estate services such as appraising real estate or acting as real estate escrow agents. Activities in this section may be carried out on own or leased property and may be done on a fee or contract basis. Also included is the building of structures, combined with maintaining ownership or leasing of such structures.
Transportation and storage	This section includes the provision of passenger or freight transport, whether scheduled or not, by rail, pipeline, road, water or air and associated activities such as terminal and parking facilities, cargo handling, storage etc. Included in this section is the renting of transport equipment with driver or operator. Also included are postal and courier activities.
Water supply, sewerage, waste management and remediation activities	This section includes activities related to the management (including collection, treatment and disposal) of various forms of waste, such as solid or non-solid industrial or household waste, as well as contaminated sites. The output of the waste or sewage treatment process can either be disposed of or become an input into other production processes. Activities of water supply are also grouped in this section, since they are often carried out in connection with, or by units also engaged in, the treatment of sewage.
Wholesale and retail trade, repair of motor vehicles and motorcycles	This section includes wholesale and retail sale (i.e. sale without transformation) of any type of goods, and rendering services incidental to the sale of merchandise. Wholesaling and retailing are the final steps in the distribution of merchandise. Also included in this section are the repair of motor vehicles and motorcycles

A.2 METHODOLOGY

A.2.1 Phase I: Stock Taking

The first phase (Phase I), 'stock-taking', was gathering all the data that was to make up base for the study and was divided in three main activities:

- desktop research,
- online survey and
- interviews

Analysis of Phase I(a): Desktop Research

During the desktop research, more than 70 documents were analysed including high reputational publications (i.e. technical reports, good practices and standards), other technical documents, whitepapers, and reports previously published by ENISA which focused on SMEs.

Even before the pandemic crisis, there were a number of available recommendations regarding the design and implementation of cybersecurity measures in organizations – some of them focused on SMEs. During the desktop research, such publications were systematically sought, identified, and analysed.

After the review of these publications, the project team was able to identify the documents that provided insight into the challenges faced by SMEs in their cybersecurity endeavours and the associated recommendations.

The results of the desktop review were consolidated, categorized, and a table was created containing the categories of challenges and recommendations identified by each relevant document. This table is not included in this report (because of size limitations), but was used in two different ways within this study:

- The most predominant results were simplified and were used in the construction of the content of the online survey.
- The quantified information was one of the influencing factors in the selection of the recommendations presented in sections 4 and 5 of the report.

Note: The recommendations reviewed covered technical, organizational, and policy recommendations, including recommendations towards relevant national and European authorities.

Analysis of Phase I(b): Survey

An online survey was conducted in the period between July and September 2020 in which 249 SMEs participated. In order to promote the survey and make sure that there was an adequate degree of participation several different channels of communication were selected (the ENISA website, social media, direct contacts with various stakeholders in various member states, relevant European funded projects etc).

The results of the online survey are analysed in Sections 2, 3 and 4.

The online survey provided a lot of information regarding the challenges and the recommendations for cybersecurity, but in order to achieve the objectives of this study, it was critical to have access to the perceptive of the SMEs regarding their actual value and practicality.

In order to collect these opinions, the structure of the survey was as follows:

Section A – Information regarding the participating organization

Purpose: Gather general (demographic) information regarding the SME in order to make sure that they should be included in the survey (valid replies) and be able to extract some conclusions based on industry, country, size etc.

Section B - The role of ICT

Purpose: Gather information on the technology knowledge and dependence of the organization to computers and the internet as well as the perceived criticality and sensitivity of information processed by the organization. These parameters together would show the impact of a possible cybersecurity incident to the organization (in terms of operation and legal compliance). Furthermore, information derived from this study would show whether there is a difference in the cybersecurity posture of the SMEs based on the organization's dependence to computers and the internet and the criticality of the information processed.

Section C – Security measures implemented

Purpose: This section gathered information regarding the security technologies and controls implemented before and after the COVID-19 pandemic. The results to these questions would allow for conclusions regarding the security level of the SMEs before and after the COVID-19 pandemic.

The security technologies and controls examined are presented in the following Tables A.4 & A.5.

Table A.2: Security Technologies

Type	Description
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Antivirus	Antivirus is a computer program or set of programs which are designed and used to prevent detect, and remove malware.
Backup	Backup concerns the procedure of copying of software and computer data and their storage elsewhere in order for them to be used to restore the original after a data loss event.
Logging and Alerting Systems	Logs are records of events related to the state of a system. There are applications that manage these logs and provides timely alerts.
DLP	Data loss prevention software detects potential data breaches and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion and at rest.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Antivirus	Antivirus is a computer program or set of programs which are designed and used to prevent detect, and remove malware.
Backup	Backup concerns the copy of software and computer data taken and the stored procedure elsewhere in order for them to be used to restore the original after a data loss event.
Logging and Alerting Systems	Logs are records of events related to the state of a system. There are applications that manage these logs and provides timely alerts.
DLP	Data loss prevention software detects potential data breaches and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion and at rest.
Digital Signatures	A digital signature is a mathematical scheme that is used to verify the authenticity of digital messages or documents
VPN	A virtual private network (VPN) extends a private network across a public one and enables users to send and receive data, across shared or public networks as if their computing devices were directly connected to the private network.
Virtualization	In computing, virtualization refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices and computer network resources.
Encryption	Encryption is the process of encoding information, so that to become unreadable without the suitable key. Encrypted hard disks and devices are such relative examples.
Secure deletion (erasure) of information	Secure deletion refers to the action of removing information permanently, without leaving traces and without the ability of restore
IoT	The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Here, the security measures regarding the protection of IoT are implied

Table A.3: Security Controls

Type	Description
Security awareness and training to staff	Awareness and training seminars are offered to staff members on information security / cybersecurity topics.
Internal Audits	Audits on the level of information security in an organisation that are implemented systematically by the organisation.
Security Assessments	Information Technology Security Assessment is an explicit study to locate IT security vulnerabilities and risks. These studies could include Vulnerability Analysis and Penetration Tests.
ISMS	ISMS stand for an Information Security Management System. An information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process, and it gives confidence to interested parties regarding the adequate management of such risks.
Password Policy	A password policy is a set of rules, designed to enhance computer security by encouraging users to employ strong passwords and use them properly.
Removable media monitoring	Removable media is a form of computer storage that is designed to be inserted and removed from a system.
Acceptable use policy on the use of company devices and applications	An acceptable use policy (AUP), acceptable usage policy or fair use policy is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restricts the ways in which the network, website or system may be used, while it sets the guidelines for their use.
Systematic updating of software	An update is a new, improved or fixed software, which replaces older versions of the same software.
Cybersecurity Risk Assessment	A cybersecurity risk assessment is the process of identifying, analyzing and evaluating risks. It ensures that the chosen cybersecurity controls are respectively appropriate to the faced risks.
Control and Monitoring of services provided by other parties	Third-party management is the process whereby companies monitor and manage interactions with all related external parties. Third parties often have access to the organization's information or can influence the security posture of the organization.
Increased physical security controls around ICT equipment	Physical control concerns the implementation of security measures in a defined structure, used to deter or prevent unauthorized access to sensitive material. Examples of physical controls are: Motion or thermal alarm systems, Security guards, Access control systems
Cyber/Information Security Officer	An information security officer is a senior-level executive within an organization, which is responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and the adequate protection of technologies.
Asset management	Asset management process provides for the identification of the organizational IT assets, the classification and the development of the appropriate security measures.
Contracts containing security clauses	Agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier or staff member regarding both parties' obligations to fulfil relevant information security requirements.
Incident response structure	An incident response team (IRT) or emergency response team (ERT) is a group of people who prepare for and respond to any security emergency incident, such as a natural disasters or an interruption of business operations.
Business continuity and Disaster recovery plan	A business continuity plan (BCP) is a document that outlines how a business will continue operating during an unplanned disruption in service. A disaster recovery plan (DRP) is a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. A DRP is an essential part of a business continuity plan (BCP). It is applied to the aspects of an organization that depend on a functioning IT infrastructure.

Section D – Cybersecurity Incidents, challenges and proposals
Purpose: Within this section, information regarding cybersecurity incidents, challenges, and recommendations were requested. An analysis of the answers regarding a cybersecurity incident could provide conclusions regarding the rate of cybersecurity incidents in SMEs, the origin of the cybersecurity incidents, the possible correlation between the cybersecurity incidents, and the implemented measures, as well as the measures implemented after these incidents. An analysis of the challenges faced and proposals for action would provide a gravity factor, which, when correlated with the results of the desktop research, would enable a more realistic set of recommendations to be provided for SMEs.

Section E – Further involvement
Purpose: The results of the online survey and the final results of this study were planned to be further validated through various methods. In this section, the help of the participants was solicited. The information of the participants would only be used only in this part of the study for the development of recommendations for actions and in accordance to the ENISA privacy policy.

Analysis of Phase I(c): Interviews

After the publication of the survey, at specific checkpoints, the results of the online survey were monitored and when the ¾ checkpoint was reached, the first preliminary analysis was conducted. This analysis contained all information and correlations mentioned above and led to the compilation of an initial set of cybersecurity challenges and recommendations by the SMEs.

To further validate these preliminary results, structured interviews were planned and conducted. The participants in these interviews were selected from the volunteers of the online survey. The interview participants were selected based on the industry, the country, and the type of SME, they were involved in. To facilitate the interviews, a customized questionnaire was created. The questions covered all the areas mentioned in the survey and focused on

- Which were (if any) the changes regarding cybersecurity posture brought by the pandemic.
- Which are the challenges an SME is facing regarding cybersecurity.
- Which recommendations towards European / Country / Regional government could have value to the SMEs.
- Which measures affecting the SMEs themselves could be practically applicable.

The results of the interviews were collected, analysed, consolidated, and correlated with those collected through the desktop research and the online survey. The result is presented in Sections 4 and 5.

A.2.2 Phase II: Extraction of Results

The second phase (Phase II) of the study was based on the qualitative analysis of the findings and the development of recommendations in two discrete axes:

- Cybersecurity recommendations for SMEs
- Proposals for actions to Regional, National and European authorities, to support the SMEs in strengthening their Cybersecurity posture.

A.2.3 Phase III: Report Validation

The draft version of this study was shared with an extended ecosystem of stakeholders in order to validate the results. This ecosystem included representatives of the SMEs participating in both the online survey and the interviews, the ENISA National Liaison Officers network, the National Cybersecurity Strategies Group and ENISA subject matter experts. A final validation stage was carried out by conducting a validation workshop organized by ENISA.

TP-01-20-706-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Ethnikis Antistaseos 72, Agamamnonos street
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-409-1
DOI:10.2824/770352