Cybersecurity for SMEs Challenges and Recommendations

# Abstract

The European Agency for Cybersecurity, ENISA is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Small and Medium Enterprises (SMEs) constitute a significant portion of the European Union's (EU) economy, comprising 99% of all businesses and playing a pivotal role in employment and GDP. However, the COVID-19 pandemic underscored the cybersecurity challenges facing SMEs, prompting ENISA to analyse their resilience and provide recommendations for improvement. This research, based on extensive desktop research, surveys involving 249 European SMEs, and targeted interviews, identified key challenges including low awareness of cybersecurity threats, budget constraints, and a lack of specialised expertise and guidance. Despite recognising the critical importance of cybersecurity, many SMEs remain vulnerable, with over 80% acknowledging potential devastating impacts within a week of a cybersecurity incident. This paper presents recommendations categorised into three pillars: people, processes, and technical measures, encompassing strategies such as software updates, access controls, cloud services adoption, and incident response planning. Additionally, guidance is provided to national and European authorities for supporting SMEs in enhancing their cybersecurity posture. Accompanying the report is a practical guide outlining 12 high-level steps for SMEs to bolster their cybersecurity defences, emphasising the urgent need for proactive measures to mitigate cyber threats and safeguard business continuity.

Keywords: Cybersecurity, SMEs, Developing Economies

# Table of Contents

[Abstract 1](#_Toc162814169)

[Table of Contents 1](#_Toc162814170)

[List of Abbreviations and Acronyms 2](#_Toc162814171)

[Introduction 2](#_Toc162814172)

[Literature Review 3](#_Toc162814173)

[Methodology 3](#_Toc162814174)

[Discussion/ Recommendations 4](#_Toc162814175)

[Conclusion 6](#_Toc162814176)

[References 6](#_Toc162814178)

# List of Abbreviations and Acronyms

* SMEs – Small and Medium-sized Enterprises
* EU – European Union
* ENSIA – European Union Agency for Cybersecurity

# Introduction

Small and medium-sized enterprises (SMEs) are crucial to the EU's economy, representing 99% of businesses, employing around 100 million people, and contributing significantly to GDP. The COVID-19 pandemic prompted a shift to remote work and digital solutions, accelerating digitisation across sectors. However, this also increased cyber threats, particularly targeting SMEs with inadequate cybersecurity defences. It's crucial for SMEs to understand and mitigate these risks, develop plans for cybersecurity incidents, and adapt measures to their specific circumstances. Effective cybersecurity not only protects businesses but also fosters growth and innovation. The report provides simple, yet impactful guidance tailored to SMEs to prevent or minimize the impact of cybersecurity incidents.

ENISA aims to assess EU SMEs' ability to handle cybersecurity challenges during the COVID-19 pandemic and provide guidance and recommendations. The report targets SME owners, employees, and other stakeholders in the SME ecosystem. Methodology involved desktop research, online surveys, interviews with SMEs and experts, and validation with relevant stakeholders. SMEs represent 99% of EU businesses, with over 25 million in the EU-28 in 2018, predominantly micro-SMEs. The report highlights the characteristics of SMEs and their significance in the European economy.

# Literature Review

# After reviewing the literature, various challenges encountered by SMEs are identified, along with significant cybersecurity incidents. Following the identification of these challenges and incidents, recommendations are initially tailored to address specific issues, then expanded to encompass national-level strategies. **The most prevalent challenges faced by SMEs included:** Low cybersecurity awareness. Inadequate protection for critical and sensitive information. Budgetary issues. Lack of ICT cybersecurity expertise and personnel. Lack of suitable guidelines. Shadow IT/Personal devices (SMEs allowing staff to use personal devices to access company data). Moving online. Low management support. **The most common cybersecurity incidents faced by SMEs included:** IT service provider company ransomwared. Stolen laptop. Email account hijacked to facilitate fraud. Ransomwared PC and server. CEO fraud.

# Methodology

The methodology followed to collect and assess the information in 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.

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

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 online survey structure was separated into five parts:

* Information regarding the participating organisation.
* The role of ICT.
* Security measures implemented.
* Cybersecurity incidents, challenges and proposals.
* Further involvement.

Following the publication of the survey, regular checkpoints were established to monitor progress. Upon reaching the three-quarter checkpoint, initial analysis was conducted, leading to the identification of cybersecurity challenges and recommendations based on responses from small businesses. To validate these findings, structured interviews were organized with volunteers from the survey, selected based on industry, country, and SME type. A customized questionnaire was utilized during the interviews, covering areas such as changes in cybersecurity posture due to the pandemic, challenges faced by SMEs in cybersecurity, recommendations for government entities, and practical measures applicable to SMEs. Results from the interviews were collected, analysed, and correlated with data from desktop research and the online survey.

# Discussion/ Recommendations

**Current Cybersecurity measures used by SMEs**

The literature revealed that while many SMEs had basic cybersecurity measures in place before the COVID-19 pandemic, such as firewalls and antivirus software, these were often managed by IT personnel. Various publications from member states and countries like the UK, Australia, and the US offer guidelines for improving cybersecurity in SMEs. Cost-effective measures exist for SMEs to enhance cybersecurity, focusing on assigning responsibilities appropriately, raising staff awareness of risks, and implementing relatively simple technical controls. These measures need not be overly complex or expensive to implement and maintain. ENSIA provided recommendations which should be followed by all SMEs and divided them into three categories which should be addressed. These categories are people, which are all individuals within the company, processes, which are the practices which SMEs follow, and technology, which are the types of software or hardware used by the company.

**Recommendations**

ENSIA recommended employees in SMEs mitigate risk by:

* Ensuring the director or equivalent is somewhat responsible for cybersecurity.
* All members of staff read and understand an information security policy.
* All users of computer systems in SMEs receive regular training on their security responsibilities on how to identify and deal with threats.
* Staff members with specific security responsibilities receive proper and regular training to support their role.
* Implement a documented security policy that is fully supported by senior management.
* Determine whether senior management authorise third part access to confidential or sensitive information.

ENSIA recommends SMEs implement certain processes including:

* Audits, ensuring critical systems, such as firewalls and routers are regularly tested for vulnerabilities. Computers are checked to ensure no copies of illegal software are present.
* Incident planning and response plans are frequently teste and in place, with clearly defined roles and responsibilities to ensure the company can respond to and attack.
* All default passwords on all systems reset from the default vendor installed passwords and all users are forced to use complex hard to guess passwords.
* Ensure there is a mechanism to ensure all critical security patches are deployed to systems in a timely and audited fashion.
* Ensure that all systems and databases that store personal data are secured properly to ensure compliance with regulatory and legal requirements.

ENSIA recommends SMEs have certain technologies within their companies which include:

* Network security, external connections such as to the internet are authorised by senior management and are secured using firewalls.
* All computer systems are protected with the most up to date anti-virus software and users are educated on how to deal with and identify suspect emails or files which may contain computer viruses.
* Encryption, all devices storing data have full disk encryption enforced and users use VPNs when communicating sensitive information over public networks.
* Log files of important security devices are actively monitored to detect potential security breaches.
* Physical security which involves critical IT resources such as file servers are in a secure area which is protected from unauthorised access.
* Secure backups of SMEs critical data and systems are kept in secure offline storage. These backups should be regularly tested if they are able to be restored so if a ransomware attack occurs SMEs should be confident they can restore these backups.

# Conclusion

# In summary, ENISA's investigation underscores the pressing cybersecurity dilemmas confronting SMEs within the EU, a situation that has been magnified by the onset of the COVID-19 pandemic. Despite the existence of rudimentary cybersecurity measures among many SMEs, there persists a notable gap in both awareness and specialised expertise. To address these challenges, ENISA advocates for a holistic approach, encompassing the assignment of cybersecurity responsibilities at managerial levels, comprehensive staff training initiatives, the formulation of robust security policies, and the establishment of effective incident response plans. Moreover, fostering collaboration between SMEs and governmental bodies is deemed essential to provide vital support and facilitate the exchange of knowledge. By prioritizing cybersecurity and implementing ENISA's recommendations, SMEs can not only mitigate risks but also fortify their defences, safeguard sensitive data, and ensure the seamless continuity of business operations within an increasingly digitalized landscape.

# References

ENSIA (European Union Agency for Cybersecurity) (2021) [‘Cybersecurity for SMEs’](file:///C:\Users\mferr\Downloads\ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations%20(2).pdf), European Union Agency for Cybersecurity, European Union.

Heidt M, Gerlach J, Buxmann P (2019) Investigating the security divide between SME and large companies: how SME characteristics influence organizational IT security investments. Inf Syst Front 21(6):1285–1305

Lloyd G (2020) The business benefits of cyber security for SMEs. Comput Fraud Secur 2:14–17

Mahmood A, Hamdan A, Tahoo LA, Akeel H (2023) managing small and medium enterprises (SMEs) during unexpected situations: strategies for overcoming challenges. In: Alareeni B, Hamdan A, Khamis R, Khoury RE (eds) Digitalisation: opportunities and challenges for business. ICBT 2022. Lecture notes in networks and systems, vol 620. Springer, Cham. <https://doi.org/10.1007/978-3-031-26953-0_19>

Matt DT, Vladimir M, Zsifkovits H (2021) Industry 4.0 for SMEs: challenges, opportunities, and requirements. Palgrave Macmillan.