CASE- Center for Social and Economic Research

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

Executive summary

The European Commission's SME Strategy for a Sustainable and Digital Europe recognised the vulnerability of SMEs to cyber-threats and identified cybersecurity as one of the key aspects of digital upskilling. At the global level too, cyber-threats emerge among the main short-term global risk (World Economic Forum, 2021) and become a constant threat to most of the enterprises amid the accelerated digital transformation induced by the Covid-19 crisis (OECD, 2021).

This report identifies internet-based incidents, including phishing, malware, and web-based attacks, as the **most frequent cyber-threats** relevant to the EU MSMEs. In line with ENISA (2020), other important cyber-threats also include spam, denial of service, identity theft, data breaches, insider threat, botnets, physical manipulation and damage, information leakage, cyberespionage, and cryptojacking. At the same time, while internet access and remote work arrangements might increase MSMEs' exposure to cybersecurity risks, human factor is another important source of digital vulnerability as about 84% of all cyberattacks in the EU rely on social engineering to lure people into divulging sensitive information or clicking on the link that may contain malicious files (ENISA, 2020).

The **country analyses** presented in this report further underline growing importance of cybersecurity topics at the national levels and confirms relatively low extent of knowledge on cybersecurity among the MSMEs. According to the results of the 2020 Eurobarometer, the share of respondents that reported being 'not well informed' about the risks of cybercrime stood at 67% for Romania and Italy, 55% for Spain, and 43% for Poland. Further, at the company level, only 7% of SMEs in Romania made their employees aware of their obligations in ICT security through compulsory trainings. SMEs in Spain, Poland, and Italy, in turn, performed closer and even above the EU average with 20%, 30%, and 34% figures, respectively. When the gap between the SMEs and large enterprises in considered, however, Romania and Italy have one of the smallest gaps EU-wide – only 21 pp and 23 pp, respectively. While Spain has relatively higher gap at 27%, it managed to stay below the 30 pp EU-27 average and the 35 pp gap registered in Poland.

Thus, the EU MSMEs often lag behind large enterprises in terms of **awareness** of and **preparedness** to deal with proliferating cyber-threats. More importantly, the greater and the most frequent cyber-threats are also the ones on which the level of awareness in the EU remains the lowest. The lack of awareness and commitment from management, in particular, is the common and most often cited challenge (ENISA, 2021). As a result, only 30% of the EU SMEs resort to more than basic cybersecurity measures and less than 30% of the SMEs in the EU-27 make their employees aware of their ICT security obligations through compulsory training courses – almost twice less compared to large enterprise.

Other **structural challenges** that undermine greater preparedness of the MSMEs also include low cybersecurity awareness of the personnel, inadequate protection of critical and sensitive information, lack of budget, lack of dedicated IT and cybersecurity specialists, and lack of suitable cybersecurity guidelines specific to SMEs.

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

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

A number of **EU-level initiatives**, including, among others, EU Cybersecurity Strategy, EU Agency of Cybersecurity, as well as SMESEC and Make_SME_Digital frameworks, allow to bridge the skills gaps and bolster collective resilience against cyber-threats. These are further supported by the **country-level initiatives** – e.g., Polish National Platform for Cybersecurity and PWCyber Cybersecurity Cooperation Program and Italian National Framework for Cybersecurity and National Inter-University Consortium for Information Technology (CINI) – that establish national cybersecurity frameworks and support digital skills development at the local level.

Yet, as discussed in this report and individual country profiles, a more comprehensive policy actions are needed to tackle systemic lack of cybersecurity capabilities among the EU MSMEs. These should focus on strengthening:

(i) **cyber awareness** among MSMEs by promoting better understanding of cybersecurity at large and tailoring the content and channels of the outreach campaigns to the MSMEs context and sectoral needs.

(ii) **cyber resilience** of the MSMEs by creating MSMEs focused cybersecurity standards and guidelines, promoting use of cyber risk management frameworks within MSMEs, and making cybersecurity more accessible.

(iii) **cyber responsiveness** of the MSMEs by promoting voluntary and compulsory trainings among employees and supporting development of simplified security protocols.

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

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