CYBER MSME:

POLICY PAPER

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

With the support of the Erasmus+ Programme of the European Union.

TABLE OF CONTENTS

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

With the support of the Erasmus+ Programme of the European Union.

1. BACKGROUND AND GENERAL INTRODUCTION

We, all of the six partners involved in the Cybersecurity for micro, small and medium enterprises project, are aware of the huge economic impact of cybercrime, especially at the level of small businesses, which according to EUROPOL, provide the greatest potential profits and the lowest resistance. That's why we have directed our efforts toward developing effective tools and learning materials that can be used to bridge the skills gaps identified at the EU and national levels for micro and small enterprises on cybersecurity. Thus, the project aims at developing innovative training programs to provide new skills and competencies to entrepreneurs and staff of micro, medium, and small enterprises, as well as make it possible for young people to identify and be able to apply for jobs in the MSMEs.

The activities of the project were implemented over a period of 24 months, and they were centered around a few major objectives: developing and maintaining the Cyber-MSME OER platform, mapping the cyber threats and training needs at the level of MSMEs, defining the professional profile of the cybersecurity expert within MSMEs, developing training and operational toolkits that can be accessed in five languages, free of charge, which were to be further delivered and validated, and finally defining guidelines for the implementation of project results and its further replicability in other domains of practice that are close to the cybersecurity in MSMEs.

Thus, starting from these objectives, the partners' activities and efforts have translated into the Cyber-MSME OER platform, fully open, free, and available, a variety of knowledge in the format of training resources, courses, and materials, as well as a set of operational tools for implementing cybersecurity at the enterprise level. However, even after our work is completely done, the project still expects a series of results, such as providing learning resources to prospective users even beyond the funding timeframe, with the purpose of increasing the capacity to understand and to act in the events of a

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

With the support of the Erasmus+ Programme of the European Union.

cybersecurity threat, as well as the operational capacity to implement cybersecurity skills in a practical environment.

2. INTRODUCTION TO PROJECT OUTPUTS

First of all, we have to mention that the project outputs are designed to meet the professional needs of a cybersecurity expert and the training implementation proposed is designed to help obtaining such a status, both in an organization and for personal use, with the help of the Cyber-MSME toolkit. The profile of the cybersecurity expert consists of three different stages, as it follows:

- The entry level, consisting of cybercrime analysts, IT auditors and incident responders, who should take on courses which focus on the basics of cybersecurity, the European landscape for cybersecurity, available if the format of five courses on the platform;
- The mid-level, represented by the cybersecurity analysts, cybersecurity consultants and penetration testers, who should master knowledge and skills such as social engineering and ICT tools to prevent and recognize cyber risks, which are provided in the format of three courses and two toolkits on the platform;
- The advanced level, made of cybersecurity managers and cyber security architects, who should have the skills to deal with a cybersecurity crisis, while improving the cybersecurity management plan and implementing ethical hacking across the business.

Moving forward to the results of the project, one of its initial intellectual outputs was to map the cyber threats for micro-enterprises and SMEs, with the project targeting two specific goals from two different perspectives. Firstly, its purpose was to reach out to MSMEs who cannot afford to self-provide ICT security services, but who want to find the right tools to protect their digital information. Secondly, the project aimed at building ICT

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

With the support of the Erasmus+ Programme of the European Union.

resources and digital technologies that have achieved a high level of maturity and expertise in teaching cybersecurity issues. To achieve these two objectives, the partners carried out a comprehensive assessment of the target group and the dynamics of cyber security in its entirety and digital security in the countries involved, focusing on identifying common features and best practices for the implementation of cybersecurity technologies, as well as gaps existing in the entrepreneurship training related to the knowledge of cybersecurity and ICT.

The results of these comprehensive assessments have shown that the cyber-lag experienced by the vast majority of EU MSMEs is first and foremost an issue of cultural understanding, with SMEs failing to comply with the basics of cybersecurity. According to the results, the distribution of the cyber risks falls under the following categories:

- In the individual sector, the most popular cyber-threats are phishing, malware, information leakage, and data theft;
- At the level of multiple industries, web application attacks, phishing and malware are the biggest risks;
- The public administration confronts most frequently malware, phishing, and web-based attacks;
- In finance and banking, the biggest cyber threats are represented by web application attacks, insiders and data abuse, malware and data theft;
- The medical sector has to deal with malware, insider and data abuse, and web application attacks;
- At the level of education, the biggest cyber threats are represented by malware, ransomware, and web-based attacks;
- In the information and communication sector, as well as in the professional and digital services, web applications attacks, insider and data abuse, and malware are the major cyber threats;
- At the level of arts and entertainment, the biggest threats are represented by web application attacks, malware, and phishing;

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

With the support of the Erasmus+ Programme of the European Union.

- Last but not least, the manufacturing sector has to deal with malware, web application attacks, and insider and data abuse.

Moving to the level of awareness of cyber-attacks, the results show the following:

- When it comes to malware, phishing, web-based attacks, web application attacks, and spam, the level of awareness is very low;
- For denial of service, identity theft, data breaches, insider threats and botnets, the level of awareness is low;
- For physical manipulation, damage, theft, loss, ransomware, cyber espionage, and crypto-jacking, the level of awareness is medium.

Moreover, each of the partners conducted a comprehensive assessment of the cyber needs at the level of Europe and their countries, and the results showed the following:

- In Europe, the results of the project suggest that the topic of cyber-readiness seems particularly urgent for micro and small medium enterprises established in Southern/Balkan regions and operating in non-ICT dominant sectors. Thus, Cyber-MSME partners suggest that policymakers should focus on making cybersecurity investments affordable for EU SMEs, taking measures to reduce the complexity of security so that this fits into work processes without major disruption, as well as Envisaging measures to favor the participation of women and minority groups in STEM.
- In Poland, a lack of awareness and preparedness of cyber security risks can be observed among companies, with only 8% of companies sufficiently prepared, which is an alarmingly small percentage. The Poland partner identified a few

Co-funded by the Erasmus+ Programme of the European Union
With the support of the Erasmus+ Programme of the European Union.

aspects that can be improved at the level of MSMEs, i.e. offering more training to employees and business relations, introducing better measurement of the financial issues related to cyber-threats, sharing information about cyber-risks among companies, paying attention to securing electronic devices other than computers and including small, micro and medium-sized enterprises in the activities falling under the Cybersecurity Strategy of the Republic of Poland.

- In Romania, a major need for cybersecurity knowledge has been noticed, as the country is currently facing threats to its critical infrastructure, originating from cyberspace and caused by an increasing interdependence between cyberinfrastructure and infrastructure such as that belonging to banking, transport, energy, and national defense sectors. The results of the research stated that Romania needs to update the regulatory framework, adopt security assessment methods, and improve the legislative framework for vocational training, research, and development programs and startups.
- In Spain, cyber attacks cause significant damages, some of them with irrecoverable results, showing a constant increase in cybercrimes. A few recommendations based on the cybersecurity situation in Spain are the following: not neglecting cybersecurity when teleworking, paying attention to data hosted in the cloud, providing active security software and solutions, paying attention to emails, and improving the training of the entire workforce.
- In Italy, findings show that micro and small-medium enterprises (henceforth MSMEs) are mostly unaware of cybersecurity and the impacts of cyber threats on their businesses. According to their findings, there are two aspects that need to be considered, i.e. the automation of the various IT processes and the training of personnel capable of managing and guaranteeing constant protection of organizational digital systems.

As mentioned before, mapping the cyber-threats for micro, small and medium enterprises in the EU was one of the intellectual outputs of the project, which highly

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

With the support of the Erasmus+ Programme of the European Union.

informed the content of IO3, meaning the development of the Cyber-MSME toolkit in five languages. Mapping the cyber-threats translated into a clear overview of the type of audience represented by the micro, small and medium-sized enterprises, as well as the skills gaps which should be filled in order to increase cybersecurity awareness. These results represented the basis for the development of innovative tools and training developed in the next stage of the project, centered around enhancing digital literacy among established economic operators.

3. MAIN TAKEAWAYS

The work of the partners within this project led to a series of takeaways that should be considered when thinking about preparing individuals and organizations for dealing with cybersecurity challenges. We'll further elaborate some of them, as perceived through the results of the project.

1. Cyber security, cyber readiness, and cyber resilience represent without a doubt a top priority for EU businesses and private sector in general, with organizations becoming more and more aware of the importance of investing in tools and strategies aimed at increasing resilience and responsiveness to possible cyber threats. However, even if an interest is shown into this field and despite the numerous initiatives implemented at EU level to increase awareness toward this topic, the vast majority of MSMEs still experience issues in responding to cybersecurity threats, which is first and foremost an issue of culture and cultural understanding, according to our research. To put it differently, the business culture at the level of MSMEs often neglects cybersecurity, especially when it comes to the human aspect of cybersecurity and the human behaviors aligned with it, which calls for a better understanding of the human aspects of cybersecurity.

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

With the support of the Erasmus+ Programme of the European Union.

2. The level of preparedness for cybersecurity is hugely different for large companies, in comparison to micro, small and medium enterprises, with research suggesting that cybersecurity is mainly considered a priority for large corporations or the IT sector, which appear more likely to have a formally defined cybersecurity policy. Thus, even if large companies are more exposed to cybercriminal activities, they have the resources to respond to threats, in comparison to the MSMEs, who lack both the resources and the professionals. This problem is highly related to the lack of properly trained people at the level of MSMEs, with small businesses finding it challenging to retain IT talents, computer science literates or simply employees who have the adequate knowledge and skills to to understand cybersecurity, and the threats and risks associated with it. The findings show that the opportunities for micro and small enterprises to gather and retain IT talents is not only threatened by the overall shortage of reliable profiles, but also by the fact that the vast majority of such professionals are intercepted by large organizations. Thus, this is both a problem related to economical factors and to an incapacity to properly train employees to be aware of the cybersecurity risks.
3. There are huge disparities among countries in terms of the cybersecurity preparedness, which are particularly evident between Northern territories, which are more prone to embrace digital paradigms and to respond to cybersecurity matters, and Mediterranean/Balkan territories, which are a bit slower in recepting opportunities for IT innovation. Moreover, according to a study conducted by the European Economic and Social Committee in 2018, while Estonia and France represent excellence in cybersecurity in Europe and worldwide, countries such as Slovenia or Slovakia still show a general lack of preparation on the subject, representing a vulnerable point within the European cybersecurity panorama. This context calls for stronger ecosystems, with SMEs connected and embedded in regional or sectoral support structure, as well as a structured skills development, from vision to plan.

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

With the support of the Erasmus+ Programme of the European Union.

4. Related to the previous aspect, at the level of Europe there are also huge disparities in terms of overall digital literacy, which highlights the huge role of vocational education and training as an agent of change among individuals and organizations. This calls for an improvement at the level of the legislative framework for vocational training, research and development programs, with a bigger focus on effectively training people and preparing them to respond to cybersecurity matters.
5. The first step that should be taken is to change perceptions when it comes to cybersecurity preparedness. This does not only involve complex computer science systems, but rather small actions that put together can make a difference in the event of a cybersecurity threat. For example, a few practices can be implemented among employees, i.e. frequently changing passwords, two-step verification for corporate emails, having up-to-date backups, paying attention to all the communication channels that can represent the main entrypoint for ransomware, and last but not least teaching people how to recognize malicious attacks before they cause irreparable damage.

4. CONCRETE INPUTS TO POLICY DIALOGUE

There are multiple actions that policy makers should focus on to tackle challenges and exploit opportunities that we recognized and identified during the implementation of the project, which can enhance the resilience and overall competitiveness of MSMEs that are not cyber-ready yet. We'll list a few of them here, as a point of reference.

- Cybersecurity is a huge aspect nowadays, as mentioned above, and the cyber readiness cycle should happen at the level of all the MSMEs who are not yet ready to respond to cyber security challenges, which means that the level of cyber resilience should increase in all relevant sectors, both public and private. Thus, reactiveness should be turned into awareness, with a better understanding of the

Co-funded by the Erasmus+ Programme of the European Union
With the support of the Erasmus+ Programme of the European Union.

most common, dangerous and disruptive cyber-attacks coming from the cyber-space. Then, awareness should move one step forward, to strengthen cyber resilience, which involves a better exploitation of best practices developed internally, as well as case studies and resources from outside. Then, resilience should turn into responsiveness, which calls for better cyber solutions that uphold security and privacy of organizations and people, as well as better training and educational programs tailored to MSMEs' specific needs.

- The cyber-secured enterprises have a significantly bigger economic and business potential, due to a variety of aspects: they prevent both financial frauds and sensitive data losses, which further improve their customers' confidence and loyalty, leading to both brand trust and cost savings and value at the level of the enterprise.
- There are a few key players for EU cybersecurity, whose main goal is to promote an EU-ecosystem devoted to fostering research and awareness in the domain of cybersecurity. For example, one of the top stakeholders is the European Cybersecurity Organization, a partner of both the European Commission and ENISA, and it assists EU bodies and agencies in developing new policies and recommendations that find application at national level. Another key player is the European Union Agency for Cybersecurity, which is tasked with the important responsibility to foster an EU-wide culture of IT security, digital proficiency, cyber-resilience and cyber-readiness. The identification of this stakeholders and key players is an important step to be made at the level of any MSMEs, to make sure that they have the right and adequate support in the cybersecurity endeavors.
- The training and education ecosystem has a huge role to play in giving MSMEs access to digital education, further preparing them for the cybersecurity challenges. Thus, adequate learning experiences and resources should enable MSMEs to equip themselves with a cyber-resilience mindset, with the right tools and resources to recognize cyber attacks and to either prevent them or to be able to respond to them. Conclusively, education in the field of cybersecurity must be a

Co-funded by the Erasmus+ Programme of the European Union
With the support of the Erasmus+ Programme of the European Union.

priority, as a trained workforce is essential to achieving the overall cybersecurity objectives.

5. SOME FINAL NOTES

As the project is coming to an end, we developed two different deliverables to promote the scalability of the project, its transferability and replicability of its results in other domains of practice, as well as an overview of the partners' insights on the field of cybersecurity and their recommendations they wish to share with policy makers and anyone who is willing to use the toolkits and courses. This document is one part of these deliverables, and the other document is represented by the Guidelines, where we consider all those key recommendations, takeaways, lessons learnt extrapolated from project's implementation on how to fully implement the learning materials.

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

With the support of the Erasmus+ Programme of the European Union.