CYBER MSME:

GUIDELINES

FOR THE IMPLEMENTATION OF PROJECT RESULTS

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. GENERAL INTRODUCTION

Cyber MSME (Cybersecurity for Micro, Small & Medium Enterprises) is an international project co-founded by the Erasmus+ programme of the European Union and delivered by a consortium of six partners from five different countries, who came together to respond to a variety of challenges that micro, small and medium enterprises have to deal with in their professional journey. The project addresses organizational needs, such as bridging the skills gaps identified at EU and national levels for micro and small businesses on cybersecurity while contributing to the competitiveness of EU micro and small businesses by providing more relevant and high-quality training programs.

Over the course of the project duration, the six partners worked together to develop the Cyber-MSME toolkit, a set of training materials addressing various topics designed for entry-level, mid-level, and advanced cybersecurity professionals who want to master the skills and knowledge they need to perform their tasks and to respond to the challenges in the cybersecurity field. The six partners have developed five toolkits and eleven courses, prepared to cover the gaps emerging from literature and covering topics such as enhancing the network security with a few basic steps, improving the cybersecurity management plan, recognizing credible URLs, essential router security tips and inventory list, each of the toolkits being enhanced by a series of courses addressing similar topics.

The toolkits include guidelines, case studies, checklists, and a rich set of resources, all of them providing free and ready-to-use learning tools for all the organizations and professionals interested in understanding, anticipating, managing, and containing cybersecurity threats while enhancing operational ability to implement cybersecurity in micro, small and medium enterprises. This target audience comprises the entrepreneurship support ecosystem and digital, ICT-related ecosystems that include stakeholders such as entrepreneurship promotion agencies, public actors,

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

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

business associations, education institutions, IT consultants, universities, research centers, etc.

Considerable efforts have been invested in the development of the Cyber-MSME toolkit in order for it to act as an asset tool for all the current and future economic entities that do not want to sacrifice the strategic advantage of digital security. Moreover, to make sure that the learning resources actually fit the needs of the target audience and are developed in line with their learning demands, a real-world validation of training materials has been conducted, with all partners deploying the pilot training to at least 150 learners representing the target groups. This provided the consortium with meaningful feedback on various aspects of the training, such as usability, adequacy to their needs and preferences, means of implementation and content, and responses which proved significant for the validation purposes of the training materials.

The collected experiences constitute the pillars of this document, the guidelines promoting the project's scalability, its transferability and replicability of its results in other domains of practice that are similar to cybersecurity. This report will consider all the key recommendations, takeaways and lessons learned extrapolated from the implementation of the project on how to fully take advantage of the training materials and effectively apply the knowledge afterward.

This report aims to provide prospective users with some practical, experience-based insights gathered from the piloting and implementation of the developed toolkits. It covers a variety of recommendations on how to communicate with the participants, how to maintain active participation during the delivery of the training programs, how to rely on the cyber OER platform as a valuable resource during the implementation of the learning programs, as well as some insights from the trainers in terms of the most suitable approaches for the delivery of the training and for collaborating with the learners. While providing the starting point and our insights and experience-based opinions on implementing the Cyber-MSME toolkit, these guidelines do not act as definite rules for the implementation of the Cyber-MSME trainings. On the contrary, prospective users are highly encouraged to experiment and to use their own

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

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

input in the delivery of the trainings, further growing and contributing to the development of valuable knowledge and skills in the cybersecurity field, enriching our work and efforts in this field.

2. LEARNING OUTCOMES

The Cyber toolkits and trainings are learning outcomes-based and aligned with EQF 3-5, as it follows:

- Knowledge of facts, principles, processes and general concepts in the field of cybersecurity, with a range of cognitive and practical skills required to accomplish tasks and solve problems by selecting and applying basic methods, tools, materials and information;
- Factual and theoretical knowledge in broad contexts within the cybersecurity field, with a range of cognitive and practical skills required to generate solutions to specific problems in the field of cybersecurity;
- Comprehensive, specialized, factual and theoretical knowledge within the field of cybersecurity and an awareness of the boundaries of that knowledge, with a comprehensive range of cognitive and practical skills required to develop creative solutions to abstract problems.

However, the Cyber-MSME toolkits and training are centered around a series of specific learning outcomes for each of the modules, and we will only mention a few of them in this guideline to have a clear overview of the objectives of these training materials. At the end of the modules, the learners will be able to:

- Identify cyber crisis and potential risks in your organization;
- Avoid common cyber mistakes, while improving your cyber crisis management plan;

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

With the support of the Erasmus+ Programme of the European Union.
This document and its contents reflect 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.

- Define and recognize human centered design;
- Define and create a bug bounty program;
- Recognize and distinguish the most commonly used social engineering techniques;
- Understand vulnerability scanning, system hacking and malicious programs;
- Get familiar with the EntreComp Framework and how it can be of relevance for cyber security and IT proficiency;
- Familiarize with the DigComp Framework – the official EU framework for the education and training of digital skills;
- Know what to do before, during and after a cyber attack;
- Use the most relevant tools to identify and react to cyber attacks.

All of these learning outcomes are discussed within the training materials, each of them covering a specific topic, such as the European landscape for cybersecurity, EntreComp for cyber-risk readiness, social engineering, ICT tools to prevent and recognize cyber risk in a digital world, crisis management, etc. As mentioned above, all of these modules, with their specific learning outcomes can be accessed anytime and free of charge on the OER platform.

3. THE PROFESSIONAL PROFILE OF MSME CYBER SECURITY EXPERT

Before giving an overview of the preparation of the piloting programme, we will define the professional profile of MSME Cyber Security expert and the career path aligned to with, which is essential for knowing how to further conduct training implementation in an organization to obtain such a status.

The Cybersecurity expert should master a series of knowledge areas, such as:

- How to meet the requirements of safety standards in the European Union;
- Cyber threats and weakest points in security management plan;

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

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

- Useful tools in organizing a safe work environment;
- Specialized terminology needed to understand a cybersecurity environment;
- How to react to and recover after attacks;
- How to achieve the next level of cybersecurity knowledge.

Moreover, besides mastering certain knowledge, a cybersecurity able should be able to do the following:

- Create and implement safety procedures;
- Work in a secure internet environment;
- Use tools and systems to avoid cyber threats;
- Create safe working conditions at a low cost;
- Implement crisis management and disaster recovery plan;
- Develop a company and its employee's skills sharing his/her knowledge.

Undoubtedly, all of these skills and knowledge are not achieved instantaneously, but they require certain levels of expertise, to which the Cyber-MSME toolkits provide relevant learning materials. The first level, meaning the entry level cybersecurity expert is represented by the cyber crime analysts, the IT auditors and the incident responders, professionals in the field who should take courses such as “the European Digital Competence Framework: DigComp 2.1.” and “the European landscape for cybersecurity: policies, strategies and support resources". Both of these courses provide an overview on institutional setting of relevance and supporting network, as well as establish a common reference model for what the European Commission envisions as the key competences and skills in the domain of IT literacy and digital proficiency, essential knowledge for any entry level cyber security specialist who want to achieve the basics in the cybersecurity field.

The mid-level of cybersecurity expert is represented by cyber security analysts, cybersecurity consultants and penetration testers, who already master the fundamentals of cyber security and want to better understand security to keep cyber threats away for

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

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

the organization the are working for, as well as be able to use ICT tools to prevent cyber risks in the digital world. For these objectives, the Cyber-MSME project developed two toolkits and three recommended courses which can be used in each organization.

The advanced cybersecurity expert is represented by the cyber security managers and cyber security architects, with a vast experience and knowledge in the information security and systems, as well as network security and cryptography, who can enhance their knowledge with the toolkits and courses offered by the Cyber-MSME project, such as “Human-centered design vs. company priorities — guidelines” and “Crisis management — they hacked me, what next?”.

All these learning resources can be used either in an organization or for individuals looking for developing new skills and knowledge in a field that is more and more present in today’s society, such as cybersecurity. For example, any person actively looking for a job should take interest in such learning resources, as they provide information and practical abilities which can prove to be an asset in their career journey.

Moreover, all these trainings should be adapted to the target audience, with a focus on the needs trainees have and on their field of expertise, and we will further introduce you to our piloting programme and the way we implemented these trainings with the target audiences.

4. PREPARATION OF THE PILOTING PROGRAMME

The preparation of the piloting programme can be divided into two levels, the preparation at the project level and at the organization level. At the project level, CTS Customized Training Solutions, one of the six partners, prepared a document specifying the schedule, tasks and means of implementing the pilot version of the training, which also included tips on how to organize the learning activities and what tools to use to collect feedback from users. This has proven to be a valuable step in the preparation of the piloting programme, as all of the partners have had access to a clear structure and operational guidance in further preparing the piloting programme at the organization level.

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

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

At the organization level, all partners defined their own schedule, format and duration of the sessions in which they would pilot the training, followed by a session of gathering feedback from the participants to evaluate their impressions, comments and suggestions on how to improve the training. At the end of the validation phase, all of the partners provided CTS Customized Training Solutions with these feedback forms to enable the development of guidance on the continued acceptance of the training.

At the organization level, the preparation of the piloting programme included a few steps, such as recruiting the participants, establishing a communication with them, choosing appropriate tools and strategies, delivering the training, and gathering feedback. At a quick overview on how the partners chose the participants and invited them to the event, we can see that they have been chosen from each partner's business clients, especially from the micro, small and medium enterprises, as well as from social media targeting. The partners provided promotional actions on social media, targeting small entrepreneurs, employees and unemployed, teachers and other VET providers who joined the events. The channels for gathering the participants were emails and social media advertising.

From a training organization perspective, the events were held in a face-to-face environment, and they followed a few steps: the trainers/teachers introduced themselves and briefly explained the project's objectives, then the trainees introduced themselves and expressed their expectations of the course. Subsequently, the teachers presented the content of the educational materials developed by the partners, as well as
the OER platform, and the trainees were encouraged to frequently ask questions to clarify any doubts they might have had or to bring their personal experiences with the cybersecurity field to the discussion. Also, the participants were encouraged to access the learning contents whenever they needed them as a valuable asset in dealing with their cyber security related challenges. As a final step, the participants were asked to provide their honest feedback on the event and on the learning materials.

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

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

5. THE CYBER OER PLATFORM AS A DIGITAL ALLY

One of the main objectives of this project was to build an internet platform as a carrier for Open Educational Resources (OER) to act as a learning environment where various knowledge is shared about the main aspects to be considered in the cybersecurity field. As the project targets micro, small and medium-sized enterprises that lack the necessary tools and resources to manage digital security risk, the OER platform is aimed at providing prospective learners with all the necessary knowledge, available in one place, will all the content completely open and available for free.

From a technical point of view, the platform has a Cyber-MSME public frontend and a private/hidden back-office section through which the content of the websites is managed through PHP development and advanced engineering technologies (Ajax, DHTML, Javascript) to create an environment characterized by usability, while simultaneously downloading and displaying content and tools in five different languages, meaning English, Romanian, Italian Polish and Spanish.

In order to ensure the platform fully meets its objectives and the needs of the prospective learners, the partners have ensured its full operability and openness, which means that no login or registration is required and all the content is available for free and accessible anytime. Moreover, the construction of the platform meets the requirements of the ICT Open Platform (ICT), which is meant to broaden the project's target group, as it serves students in vocational education and training (VET) and expands and deepens digital skills (ICT).

Moving to the aspect of organizing and displaying the content on the OER platform, it serves as an eLearning platform where the training content, with all the toolkits and the courses are easily displayed by area/topic thanks to the intelligent browsing functionalities. These guidelines are also included in the platform, aimed at increasing the possibility of accepting and using the results of the projects implemented within the target groups.

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

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

One of the functionalities implemented within the platform is the backoffice, which includes the following:

- The back office users section, which allows us to add users to the platform;
- The news section, which allows us to add news and dissemination events on the public part, in each language;
- The FAQs section;
- The partners section;
- The documents section, where we can upload learning resources with the possibility to send an alert to everyone to inform that a new document has been uploaded;
- A deadline section;
- A glossary section containing terms that might be of use;
- An associates section;
- A categories section, with categories grouped in thematic areas, such as cyber crisis simulations and cyberspace readiness checklist;
- A training section, with learning materials listed in the training section, that can be ordered by reference, training title, date and language;
- A training content section, with learning resources that are easy-to-use, but concise and tailored to the training groups, based on their specific needs.

As we mentioned before, the OER platform is aimed at acting as a digital ally for all the prospective learners working in the field of VET vocational education, as well as for people learning independently on their own scope, who are encouraged to rely on it for the piloting both in digital and face to face learning settings.

From our own perspective on delivering these trainings, the OER platform proved to be a reliable ally, as the trainers presented the platform as a source of knowledge, available after the training at any time, and they showed learners how to use it for self study, to enlarge their knowledge on the cybersecurity area, and also how to access the feedback and test sections, which the learners found intuitive and engaging.

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

With the support of the Erasmus+ Programme of the European Union.
This document and its contents reflect 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.

6. TEACHERS/MENTORS NOTES

Among other objectives, these guidelines are aimed at offering an experienced-based overview of the delivery of these trainings, as well as some insights on the learners' possible reactiveness to the content of the lesson, general background knowledge of the discussed topics, most suitable means approaches for the delivery based on the given content of the lecture and other learning-to-learn experiences in general.

Based on the trainers' perspective, the knowledge of the participants attending the training was elementary, with little or no information at all about the content, but they all showed strong interest in the topics covered throughout the lesson, and said they were satisfied with the exploration of the learning resources through the OER platform. When asked about the most suitable approaches for the delivery of the training, the mentors stated that combining topics from many different courses led to the best results, and advised on using both the online piloting and the face-to-face piloting with support from the OER platform. Also, having completed testing procedures and seeing first hand what worked and what did not, the trainers were able to provide some ideas for improvement, saying that a good approach would be to include a knowledge assessment test before starting the modules, on the one hand, and to use more real life scenarios to engage the learners, on the other hand.

7. A FEW RECOMMENDATIONS

The message our trainers wish to convey to organizations that want to implement the Cyber-MSME content and tools in their professional journey is to spend some time getting to know the learning materials and finding ways to adapt them to various target audiences, based on their needs, general knowledge on the topics and professional areas. Moreover, according to trainers' notes and recommendations, the project's mapping report shows statistics and needs in each of the partners' countries, which represents a good starting point for delivering the trainings.

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

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

However, even if these guidelines, along with the trainers' feedback are a good starting point in delivering the trainings, we highly encourage all the prospective users to adapt the learning materials to the contexts in which they operate and to the individuals to which trainings are delivered. The coaches are highly advised to invest efforts in engaging the learners in the course delivery, and to build a learning environment defined by co-development and co-creation of the content, where active learning is pursued.

8. 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. These document is one part of these deliverables, and the other document is represented by the Policy Paper, which is an input to the domain of policy and (local) decision makers in the field of cyber security, cyber readiness and cyber resilience of private sector – with particular reference to micro and small medium enterprises – and more in general, approaching aspects such as SMEs competitiveness, managerial VET, business development, digitalisation of EU citizens at large.

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

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