MECyS

Micro
Entreprise
Cybersecurity

Training Plan

Part of WP2

Co-funded by
the European Union

CONTENTS

MECyS is funded by the European Union.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

1. Overview

This Training Plan (TP) is one of the deliverables of WP2 “Backgrounds and Training Plan”. The general objectives of WP2 that are represented in the activities concern:

1. creation of national reports on the state of cybersecurity and data protection within vocational and business-related training,
2. conducting of literature review and focus group interviews in concern of general and target group specific learning hurdles to be integrated and published in an analysis report and disseminated to interested stakeholders,
3. creation of a report about best practice concerning teaching methods and training tools,
4. creation of a training plan reflecting and enhancing the results of the three points mentioned above,
5. creation of a staff training workshop, where the training plan with its systematic background will be discussed, finalized and disseminated into the further staff of the partners or associate stakeholders, so that the pilot workshops (WP3) can be conducted efficiently.
6. conducting of evaluation processes and creation of a report.

This document stands for point 4 from the list above. The purpose of the Training Plan is to provide a general overview of how the learning process can be organized and how it can be enhanced in the future. This document touches on the segmentation of potential learners and describes overall goals, training program requirements and learning journeys for each segment. Thus, it especially reflects the results of the first staff training workshop that focused on discussions about learner segmentation, learning journeys and learning tools.

This Training Plan is to be understood as a work-in-progress document. It further represents the overall training structure that provides a framework for creating the national training prototypes as a next step. Each partner will adjust the Training Plan for their specific target groups and given country-specific conditions such as Vocational Education and Training offerings. The national reports on the state of cybersecurity and data protection within vocational and business-related trainings (point 1) will be thus reflected in the country-specific training prototypes.

The contents of Training Plan reflects the results of a project workshop dedicated to WP2 held in June 2023 in Paris.

2. Learner segmentation

During the workshop dedicated to WP2, suggestion was made to divide possible training participants into three groups based on their needs and level of knowledge in cybersecurity and assign them following levels of difficulty of training program:

- Beginner level
- Intermediate level
- Advanced level

Each group will have an individual, target-group adjusted learner journey which allows each individual to receive appropriate guidance and relevant content.

These three levels are accumulative, i.e. competences of level are covered also in level 2 etc. Once a level is finished, the learner has acquired the necessary competences to start the next level. Learners can start on level 2 or 3 if they already have the required competences for the respective level.

To make this segmentation less strict, more intuitively understandable and user friendly, it was decided to assign an animal to each difficulty level according to its movement speed.

2.1. BEGINNER LEVEL: TURTLE

The turtle pathway provides a slower and steady pace. During the learning process on this level, learners will dive into the fundamentals of cybersecurity, acquiring a solid understanding of the principles of protecting and defending systems and data. In general, the focus will be on the basics of computer security.

For better understanding of what is meant by "principles" and "basics", here are some potential questions and tasks that may be provided during the learning process:

- What is a computer virus and how does it spread?
- Name three examples of phishing attacks and how can you protect yourself against them.
- Briefly explain what a firewall is and how it contributes to network security. 3 answers possible, for example.
- What are some basic measures that can be taken to protect a password?

2.2. INTERMEDIATE LEVEL: MOUSE

The mouse pathway is supposed to be the best fit for learners who are looking for a balanced approach to cybersecurity learning. This pathway offers a combination of theory and practice to help master the essential skills required to protect systems and data against common threats.

Sample questions and tasks that may be provided during Mouse pathway:

- What are the common vulnerabilities associated with web applications and how can they be mitigated?
- Explain the concept of a security assessment and its importance in risk management.
- How can organizations effectively respond to and recover from a cybersecurity incident?

2.3. ADVANCED LEVEL: HARE

The hare pathway is for individuals who want to take over responsibility for cybersecurity within their MSE, or who in general want dive deeper into the field. This pathway is designed for learners who are eager to acquire advanced knowledge and skills in a shorter timeframe.

Sample questions for this level may sound like this:

- What are the key differences between white hat, black hat, and grey hat hackers?
- What the concept of zero-day vulnerability is? How it can be mitigated?
- How can a security professional conduct a thorough network penetration test?
- What is the role of threat intelligence in proactive cybersecurity measures?
- What are the challenges and considerations of securing cloud-based infrastructure?

3. Training goals

General training goal is to close knowledge gaps in cyber security and data privacy field and provide practical implementation of this knowledge. At the same time, this general goal is extended below for each learner group depending on the individual's understanding of the field of cyber security, as well as needs, tasks and responsibilities in MSE.

Overall, the mentioned training goals represent exemplary goals that were discussed during the workshop and enriched by cybersecurity experts and respective training experts in the consortium. A further differentiation with regard to the country-specific target groups will be made for the national adaptions of the Training Plan.

3.1. BEGINNER LEVEL (TURTLE) GOALS

- Learn basic security measures to stay safe online, such as using strong passwords and regularly updating software and antivirus programs.
- Familiarize yourself with most common types of cyberattacks, such as phishing and malware, and learn how to detect and prevent them.

3.2. INTERMEDIATE LEVEL (MOUSE) GOALS

- Learn the basics of network security and how to protect a home or small-scale network.
- Understand the risks associated with mobile device usage and learn how to protect personal information stored on them.
- Gain knowledge of best practices for safe internet browsing, including using encrypted connections and verifying the authenticity of websites.

3.3. ADVANCED LEVEL (HARE) GOALS

- Acquire knowledge about the fundamentals of computer security and how to protect against basic threats, such as password theft.
- Understand the risks associated with online information sharing and learn how to protect privacy on social networks and other platforms.
- Learn the basics of data security and how to back up important files and protect them against loss or unauthorized access.

4. Content requirements

4.1. MOSCOW METHOD

To prioritize topics, features and requirements of training program for each of three learner groups according to goals listed in section 3, MoSCoW[1] method was utilized. This method involves defining four categories:

1. **Must-Have**: These are the essential topics, features or requirements that must be implemented. Without these, the solution would lack core functionality or fail to meet critical needs.
2. **Should-Have**: These topics, features or requirements are highly desirable and important for the solution, but not crucial for immediate implementation. They contribute to the solution's value, usability, or effectiveness and should be included if possible.
3. **Could-Have**: These topics, features or requirements are considered nice to have or optional. They provide additional benefits or enhancements but can be deprioritized if resources or time constraints arise.
4. **Won't-Have**: These are topics, features or requirements that are explicitly stated as not being included in the current scope or iteration of the solution. They may be deferred to future iterations or considered outside the project's current scope.

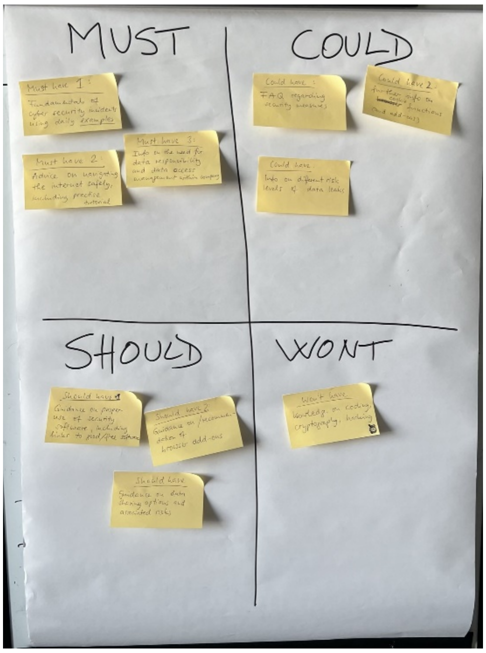
MUST
Must have 1: Fundamentals of cyber security incidents using daily examples
Must have 2: Advice on navigating the internet safely, including practise tutorial
Must have 3: Info on the need for data responsibility and data access management within company
COULD
Could have: FAQ regarding security measures
Could have 2: further info on cookie functions and add-ons
Could have: Info on different risk levels of data leaks
SHOULD
Should have 1 Guidance on proper use of security software, including links to good/free software
Should have 2: Guidance on/recommendation of browser add-ons
Should have Guidance on data sharing options and associated risks
WONT
Won't have Knowledge on coding, cryptography, hacking

Figure 1 MoSCoW board presented during the workshop

4.2. BEGINNER LEVEL (TURTLE) REQUIREMENTS

Must have:

- Fundamentals of cyber security incidents using daily examples.
- Advice on navigating the internet safely, including practical tutorial.
- Info on the need for data responsibility and data access management within the company.

[1] Early Prioritisation of Goals | SpringerLink

Should have:

- Guidance on proper use of security software in combination with a short list of good or free software.
- Guidance on browser add-ons.
- Guidance on data sharing options and associated risks.

Could have:

- FAQ regarding security measures.
- Information about different risk levels of data leaks.
- Further information on browser cookies functionality and other web browser features.

Won't have:

- Knowledge on coding, cryptography and hacking attacks.

4.3. INTERMEDIATE LEVEL (MOUSE) REQUIREMENTS

Must have:

- Knowledge on passwords
- Two-factor authentication fundamentals and implementation examples.
- Information on browser cookies functionality.
- Knowledge on GDPR
- Antivirus software basics
- Safe payment methods (i.e., single use credit cards)
- Information on most common hacking attacks (related to social engineering, not to IT)

Should have:

- Information on password managers.
- VPN basics.
- Data protection: avoiding people getting individuals' data.

Could have:

- Safe internet browsing,
- Deleting personal data: legal aspects, practical examples,
- “I’m not a robot”: human user validation fundamentals.

Won’t have:

- Basic knowledge,
- Detailed information about cyber attacks.

4.4. ADVANCED LEVEL (HARE) REQUIREMENTS

Must have:

- Cyber security in terms of needs of MSE’s.
- Cyber threat level detection, data protection assessment.
- Detailed information on possible cyber threats to individuals both on personal and company levels.
- Issue reporting: contacting governmental structures for notifying and help.
- Data backups good practices: general knowledge, backups frequency, technical nuances.

Should have:

- Infrastructure: critical elements of the system, IoT security, VPN, firewall management,
- Disaster Recovery Plan: what is it, frameworks, examples,
- Team/community management skills, dissemination,
- Data protection: avoiding people getting individuals’ data.

Could have:

- Cyber attacks detection,
- Links to external open source knowledge bases,
- “I’m not a robot”: human user validation fundamentals.

Won’t have:

- Basic knowledge,
- Coding and hacking techniques.

5. Learner journeys

To achieve the best flexibility in designing of learner journey paths, it was decided to split the learner process into 4 or 5 steps, depending on the level. Each level will refer to the requirements from section 4 and to the chosen tools represented in the Learning Tools Report. This approach was tested during the workshop and showed good results from the flexibility and usability perspective. Below there are two examples of possible learning journeys presented: one for Basic (Turtle) and Intermediate (Mouse) levels, and one for the Advanced (Hare) level.

5.1. BEGINNER & INTERMEDIATE (TURTLE & MOUSE) LEARNER JOURNEY

The learner journeys for the Basic and Intermediate levels are combined into one due to the similarity in the nature of the questions and assignments for these two levels, which differ only in depth of knowledge. This journey is designed with the help of short questions that show learner what each part of training path stands for.

1. **What?**
   This part is dedicated to the fundamentals of cybersecurity field. For "turtles" and "mouses" fundamentals of course may differ, but in general it's very important for both groups to learn or refresh knowledge about what do they deal with.
2. **How?**
   After theoretical block, learners will switch to the practical examples and learning tools that are focused mainly on skills and actions that individuals should be aware of.

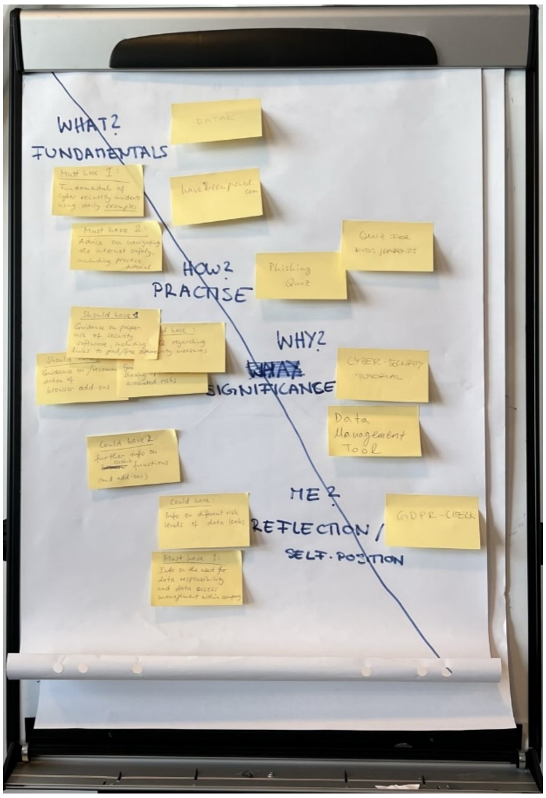
WHAT?
FUNDAMENTALS
DATAK
Must have 1: Fundamentals of cyber security incidents using daily examples
havebeenpwned.com
Must have 2: Advice on navigating the internet safely, including practise tutorial
Quiz for kids/parents
HOW?
PRACTISE
Phishing Quiz
Should have 1 Guidance on proper use of security software, including links to good/free software
Should have: Guidance on/recommendation of browser add-ons
WHY?
~~WHAT~~
SIGNIFICANCE
CYBER-SECURITY TUTORIAL
Data Management Tool
Could have 2: further info on cookie functions (and add-ons)
ME?
REFLECTION /
SELF-POSITION
Could have: Info on different risk levels of data leaks
GDPR-CHECK
Must have 3: Info on the need for data responsibility and data access management within company

Figure 2 Beginner & Intermediate (Turtle & Mouse) learner journey draft made during the workshop.

3. **Why?**

   This part reveals the significance of the knowledge in cyber security and explains how the information from parts 1 and 2 can be applied to MSEs.

4. **Me?**

   In the end, learners will get the information why it's important to start cyber security education on individual level. In general, this part will touch reflection problems and self-positioning of individuals in MSEs.

5.2. ADVANCED (HARE) LEARNING JOURNEY

Learning journey for Hares is designed a bit differently. It is supposed that individuals in Advanced group have more connections with others inside MSE and can be responsible for team training and management.

There are five steps:

1. First, learners will go through knowledge blocks that will lead to the first risk assessment of cyber security inside MSE.
2. Depending on the results of the first assessment, learners will be offered with several various step-by-step courses that are appropriate to the MSE's level of cyber security awareness and protection.
3. Then, a middle assessment will take place. This should help learners to strengthen their blind spots and to maximize the effectiveness and applicability of their knowledge.
4. Next step would be to communicate inside the team about cyber security: it can be either an informal talk or a prepared training. Learners may be provided with a checklist or a form for the feedback that can help them to go through all the topics that are important for their MSE.

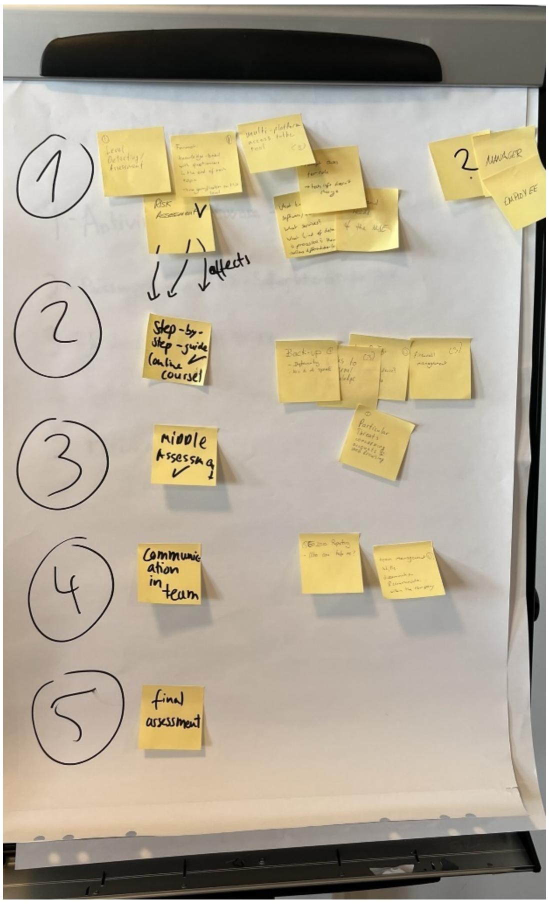
1
Level Detecting/ Assessment
Format: knowledge-based with questionnaire in the end of each topic
multi-platform access to the tool
?
MANAGER
EMPLOYEE
Risk Assessment
affects
2
Step-by-step-guide (online course)
Back-up
Firewall management
3
Middle Assessment
Particular Threats concerning accounts & web browsing
4
Communication in team
Reporting
- Who can help me?
Team management
5
final assessment

Figure 3 Advanced (Hare) learner journey draft made during the workshop.

5. In the end, after getting the results of the communication inside the team, a final assessment should be done. This assessment is the most important part of the learning process and will provide a certification (if learner shows good results) and further steps how to improve cyber security knowledge and skills if applicable.

6. Conclusion

The Training Plan is aimed to cover a diverse range of learners from MSEs in the field of cybersecurity. The use of learner segmentation and animal metaphors adds an engaging and user-friendly dimension to the plan. However, the actual success of the Training Plan will depend on the quality and relevance of the content and tools used in each learning journey, which should be carefully developed, tested, and later assessed to ensure their effectiveness.

REVISION HISTORY

Version	Date	Author	Comment
0.1	16.08.2023	Ilya Misyura	Table of contents
0.2	04.09.2023	Ilya Misyura	First draft
0.3	07.09.2023	Bettina Schneider	Review
0.4	11.09.2023	Ilya Misyura	Text and images adjustment
0.5	11.09.2023	Bettina Schneider	Review
0.6	12.09.2023	Ilya Misyura	Text adjustments
0.7	14.09.2023	Jessica Peichl	Final review

MECyS

Micro - Entreprise Cybersecurity

mecys.eu

Co-funded by
the European Union