TRAININGS AND SKILLS: ENISA EXPERIENCE

Dr. Fabio Di Franco
Capacity Building Unit - ENISA

25 | 03 | 2021
Cybersecurity skills gap and shortage

What skills do students acquire?

How many students graduate yearly?

Skills Acquired

Students Graduated

Skills Needed

Unfilled Positions

How large is the skills shortage?

Which skills are needed?

Understand the cybersecurity skills gaps in the Europe.
AN EUROPEAN CYBERSECURITY SKILLS FRAMEWORK IS ON THE WAY

- Promote harmonization in the ecosystem of cybersecurity education, training, and workforce development
- Develop of a common European language in the cybersecurity skills and competencies context.
CYBERSECURITY HIGHER EDUCATION DATABASE

Crowd-sourced database of cybersecurity related education programmes: it is the largest cybersecurity point of reference for citizens looking to upskill their knowledge in the cybersecurity field.

120+ cybersecurity programmes

Collaboration with the pilots of CCCN is on-going.
ENISA EXPERIENCE IN TRAININGS
FACTORS TO CONSIDER

Knowledge
- Areas to cover
- Specialized, sector-specific
- Level of depth to cover
- Technical, Operational vs Tactical

Skills
- Skills in demand
- Exercises structure to put in practice knowledge
- Type of activities

Target audience
- Number of participants
- Background knowledge
- Prerequisite

Resources
- Trainers
- LMS Platform
- CyberRange
- Budget

Course Length (hours/days)
- Overall duration
- Lectures duration
- Exercises duration
- Working hours

Other Factors
- F2F vs remotely

Fabio Di Franco - CyberWiser
A PLAN FOR TRAININGS

**Level 1**
- **Self paced e-learning**
  - Support large numbers of participants
  - Interactive, Story-based
  - Build initial knowledge
  - Assessment questionnaires which might bring of a **certification of skills (L1)**

**Level 2**
- **(Flipped) Classroom**
  - Supports a medium numbers of participants
  - More in depth presentations and Q&A
  - Build advanced knowledge & basic skills

**Level 3**
- **Cooperative Table-Top Exercises**
  - Support very small numbers of participants (breakout sessions)
  - Build more advanced skills applied to real job tasks (case studies)

**Audience (N. of trainees)**
- Level 2 and Level 3 might be combined
**Flexibility**
Trainees have the ability to effectively use their time (use the elearning at their own pace in order to gain enough knowledge).

**Engagement**
Strong connections between pre-class preparation and in-class sessions ensure that trainees are engaged in both the material and the discussions. They are given more time to discuss and question aspects of the lecture. They become active participants instead of passive listeners.

**Peer-Learning and Collaboration**
Collaboration among team members and across teams allow knowledge transfer between learners. Activities are be trainees-led, and the teacher’s role will be the one of a facilitator.
Paul’s Success

2. Learn about Information Security
Information Security Definitions and Terms, Best Practices, and Legal and Regulatory requirements.

4. Understand the Security Organization
Get to know the Organizational Structure, Roles and Responsibilities and the Organization’s RASCI model.

6. Conduct Risk Assessment
Interview key personnel to identify assets, existing security controls, threats, vulnerabilities and the associated risks.

8. Review Organizational Controls
Revise security policies and deploy a targeted awareness program.

10. IT Security Risk Management Methodology - ITSRM
Conduct Risk Assessment based on EU ITSRM Methodology.

1. Understand the Organization
Colleagues with key roles and responsibilities.

3. Experience a security incident
Follow the established incident handling procedure starting from reporting to incident analysis and communication.

5. Introduction to Risk Management
Learn about the Organization’s Risk Management process (assets identification, threats and vulnerabilities assessment, risk treatment).

7. Risk Treatment
Make a decision about risk treatment and establish an action plan for risk reduction.

9. Review Technical Controls
Audit technical controls and enhance protection with additional technical measures.
What should I do with the USB stick...

Story Overview

The following day Paul arrives at the Ministry’s Car Park. He finds a USB stick close to the place he parked his car. He must decide what to do with the USB stick.
Question:
What should Paul do with the USB Stick?

a. Leave there
b. Try to find the USB Owner (plug it in PC at work/home)
c. Dispose it at rubbish
d. Report to Reception Desk
Question:
What should Paul do with the USB Stick?

a. Leave there
b. Try to find the USB Owner (plug it in PC at work/home)
c. Dispose it at rubbish

✓ d. Report to Reception Desk
Hi Olivia!
I would like to report that I found this USB stick at the Ministry’s Parking.
Ok Paul!
I suppose you know that a found USB stick could imply a security incident.

Therefore, we must follow the Incident Handling Procedure and complete the Incident Report Form.
He found a USB Stick at Ministry's Parking in the morning and he reported it at Reception Desk.
He found a USB Stick at Ministry’s Parking in the morning and he reported it at Reception Desk.
Hi Mr. Frank!

This morning, a colleague of ours, Mr. Paul Muller, found this device at the Ministry’s Car Park.

Thank you, Olivia!
Our Security Team will analyze the device.

Hi Mr. Frank!
This morning, a colleague of ours, Mr. Paul Muller, found this device at the Ministry’s Car Park.

Story Overview

Olivia contacts the Security Team and delivers the USB Stick to Mr. Frank, who is responsible of evaluating the potential security incident.
Analysis of the USB Stick

The Ministry’s Information Security Team analyses the USB & identifies the malware.

The type of malware is Ransomware, which could cause damage to the Ministry if an employee plugged it into a PC…
Modern Attack Example - Ransomware

Advanced Evasion Techniques

1. Research Target Infrastructure/ Employees
2. Targeted Deployment / Initial Intrusion
3. Outbound Connection
4. Expand Access / Strengthen Foothold
5. Encrypt Data
6. Blackmail / Ransom

INTEGRATED

SUPPORTING

RESEARCH

EXAMPLE

ENISA e-learning

Self paced e-learning
Dear all,

This morning, a colleague of ours found a USB Stick at the Ministry’s Car Park and he reported it to the Reception Desk.

Following our Incident Handling Procedure, the Ministry’s Information Security Team analyzed the device and identified that it included a Ransomware.

Please, be vigilant in order to handle similar incidents accordingly.

Yours sincerely,

Frank Martin
Head of Security Team
Question:

A USB stick might contain a virus and therefore running an updated antivirus program eliminates the risk of being infected.

Choose whether the statement is true or false:

- True
- False
Question:

A USB stick might contain a virus and therefore running an updated antivirus program eliminates the risk of being infected.

Choose whether the statement is true or false:

- True
- False
COOPERATIVE TABLE-TOP EXERCISES

Split participants into teams

Exercise

Present results and discuss on the solutions
Each team

- A trainer act as a facilitator
- Participants collaborate to complete the exercise
  - Discuss the exercise
  - Share screen and fill in their report/results
  - Search through the provided documents

COOPERATIVE TABLE-TOP EXERCISES
THANK YOU FOR YOUR ATTENTION 😊

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi
Attiki, Greece

+30 28 14 40 9711
Fabio.DiFranco@enisa.europa.eu
www.enisa.europa.eu