Annals of
Reviews and Research

Review Article
Volume 9 Issue 5 - August 2023
DOI: 10.19080/ARR.2023.09.555774

Ann Rev Resear

Improving Cybersecurity Awareness and Basics in Vocational Education and Training

Gabriel Vladut[1]* and Ileana Hamburg[2]

SC IPA SA, CIFATT Craiova, Romania

Westfälische Hochschule Gelsenkirchen, Germany

Submission: August 20, 2023; **Published:** August 29, 2023

*Corresponding author: Gabriel Vladut, SC IPA SA, CIFATT Craiova, Romania. Email id: office@ipacv.ro

Abstract

Vocational Education and Training (VET) are oriented to achieving skills and teaching of knowledge related to a specific occupation or vocation in which learner will participate. It is done at an educational institution, as part of secondary or tertiary education, or within initial training during employment, (as a combination of formal education and workplace learning). Digital transformation has introduced new business opportunities for companies, but at the same time also new risks. Cybersecurity is a big concern for companies, especially for small and medium-sized enterprises (SMEs) that are much more vulnerable, first of all from their organization, not having an internal IT department that also deals with security, on the other hand part of the lack of necessary skills, their staff and management not being used to face cyber risks and giving us attention to this sector. It is essential that SME management understands the need to put in place appropriate IT security policies and provide adequate staff training. It is known that technology as well as cyberattacks evolve rapidly more than people and organizations were aware of. Therefore also, within VET it is necessary that educators/trainers and students are equipped with cybersecurity awareness and have some cybersecurity basic knowledge about reasons why cyberattacks happen and tools to act against them. Results show that the education sector is leading when it comes to suffering cyberattacks (July 2022 to August 2022). It means that the education sector of a country needs more protection and knowledge in this context. This article is based on the experience of the authors within the Erasmus+ project "InCyT - Interdisciplinary Cyber Training."

Keywords: Cybersecurity; Formation; Industry 4.0; Entrepreneurship; Engineering education

Abbreviations: VET: Vocational Education and Training; SMEs: Small and medium-sized enterprises; DDoS: Distributed Denial of Service

Introduction

Access to the internet is continuing to expand, along with its use for a wider variety of purposes. There are estimates that close to 4.7 billion people are active users of the internet – close to 60% of the world's population (Johnson, 2021). However, many users have limited knowledge or awareness of the risks of being online and have never been involved in educational or training programs on cybersecurity (Aiken, 2019). Initiatives to improve cybersecurity education, awareness and remediation of threats, and training to mitigate these harms are of importance at the national level.

Some of the most common cybersecurity threats in education are:

Phishing attack is cheap and easy to steal information i.e., by clicking on the wrong link. Spear-phishing attacks are tailored to a specific individual or group. These attacks can appear as be sent from a staff member. Therefore, VET institutions need to organize special training aimed to raise awareness for such cyber threats, Malware can infect computers, servers, and other devices, lead to lose sensitive information of students and staff or causing damage to the network. This is not something to be neglected. Distributed Denial of Service (DDoS) attacks are a type of cyber-attack that overwhelms a server or a website with continuous garbage traffic. It is possible that students and staff cannot have access to online learning materials and online services. An individual within the VET institution is usually posing insider Threats. It includes downloading any software without authenticating.

Students (learners) without cybersecurity aware and basic cybersecurity can be a weak link in the education industry. Apart from cyber threats, there are also physical threats that students need to be aware of. Additionally, to knowing of such treats, there are some other relevant laws and regulations, and VET institutions must comply with these laws and regulations to ensure that all the requirements from a cybersecurity are fellfield. The project InCyT developed a Cybersecurity framework that provides a mechanism for vocational and educational training (VET) and SME business to describe the competencies and skills that students, educators, employees, managers are required to have in order to prevent cyberattacks. Taking into account the advantages of interdisciplinary training and mentoring programs, particularly in the area of cybersecurity, the team project developed, and tested digitally supported interdisciplinary training programs and a collaborative e-learning platform. Short studies done by the project partners in their seven European countries show that cybersecurity is rarely a topic in teacher training and in the classroom teaching and learning within VET. Knowing some technical and security risks of using computers and learning suitable avoidance strategies are an important aspect of dealing competently with digital media, so the issue of data and devices in VET protection should plays a central role also in VET [1-5].

The contribution to the concept

The project goal is to train the staff of companies that do not have specific IT skills in their staff to deal with problems related to cybersecurity. The training program identifies and responds to the training needs of both managers and staff, developing two different training courses. The project started from the analysis of the state of the art in cybersecurity general education, analyzing the existing training courses in particular in the partner countries. As training courses on the subject already exist, particular attention has been paid to courses that use innovative learning methodologies. This analysis allowed implementing the first main outcome of the project: a cybersecurity competency framework: the Digital Competence Framework 2.0. Companies can adopt it to describe and improve competencies and skills in order to develop a company's cybersecurity policy, avoid cyber-attacks, and improve their VET education plans. The Digital Competence Framework 2.0 (Dig Comp 2.0) has been used to prepare employees for the digital transformation that will be pursued in InCyT. Competences: (Figure 1)

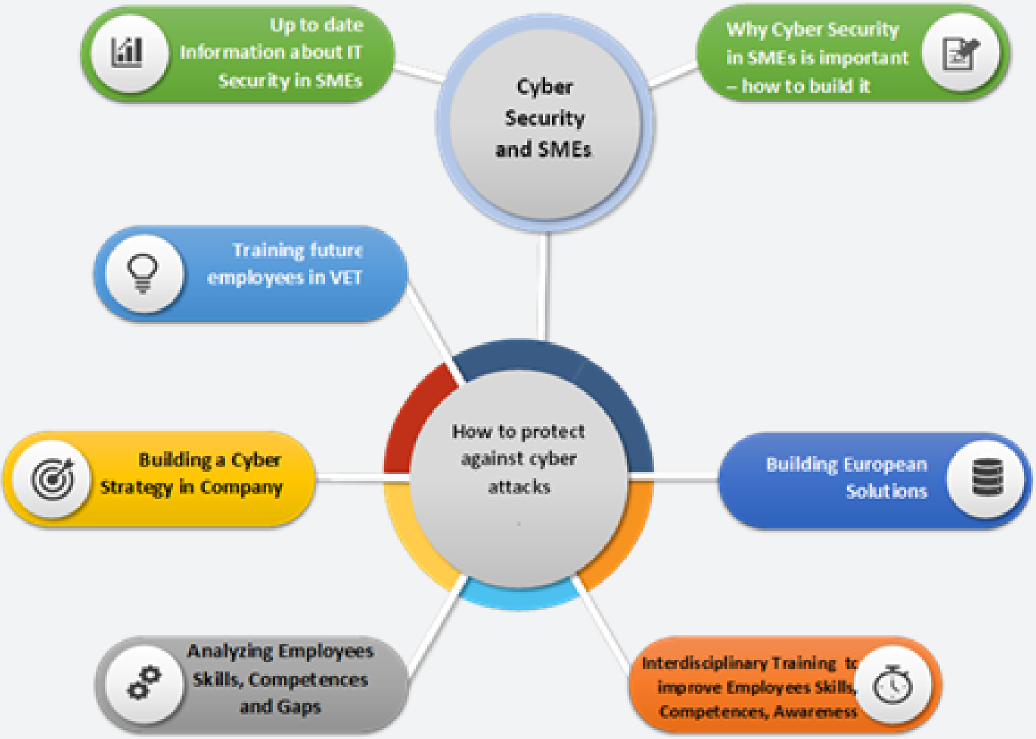

Up to date Information about IT Security in SMEs
Cyber Security and SMEs
Why Cyber Security in SMEs is important – how to build it
Training future employees in VET
How to protect against cyber attacks
Building a Cyber Strategy in Company
Building European Solutions
Analyzing Employees Skills, Competences and Gaps
Interdisciplinary Training to improve Employees Skills, Competences, Awareness

Figure 1

Collaboration and communication between educators, researchers, and people using information technologies are necessary. One problem is that companies, especially SMEs with fewer resources, need help to assess the skills and gaps of their employees, methods of assessing the existing situation, as well as using training opportunities to reskill their employees.

The project will want to implement several solutions:

i. Development of a Framework, which provides a mechanism for VET and companies to describe the competences and skills, needed in cyber security for professionals and non-professionals, to avoid cyber-attacks, as well as digital gaps and others.

ii. Taking into account the advantages of interdisciplinary training and mentoring programs, especially in the field of cyber security, the project will develop, and test supported interdisciplinary digital training programs and a collaborative e-Learning platform for SMEs.

iii. Adapt for VET.

iv. Development of a European model of transferability

v. Taking into account the advantages of interdisciplinary training and mentoring programs, especially in the field of cyber security, the project will develop, and test interdisciplinary digital training programs supported by e-mentoring for SMEs and adapt them for VET.

It can be observed that several competence frameworks already exist on the subject, developed both domestically and in Europe or the United States. However, these framework skills mainly refer to advanced figures in the cybersecurity sector (professionals, consultants, specialized personnel). The Competence Framework of the InCyT project, although born from an analysis of the existing ones, describes the skills that also the management and non-IT specialized staff of SMEs should have to properly deal with cyber risk [6-12].

The Platform

We have created a fully digitized Platform (from registration, course modules, mentoring, to the diploma for co-students and course participation). The object of the ICT Platform methodology is to provide a collaborative workspace to support the learning methodology and deliver the learning material / content. The ICT Platform (IO3) has the following objectives:

a) To guide SMEs through learning process about cyber-attacks and refer them to relevant material as required.

b) To provide opportunities for collaboration Communities of Practice / Discussion Forums.

c) Brainstorming tools.

d) To be a Collaborative platform to allow SMEs and education providers to connect.

e) To produce reports about learning being undertaken in SMEs.

This Platform is made available to VET / Stakeholders who wish to apply, after the end of the project, through an elaborate transferability methodology.

The structure of the ICT Platform:

i. About (Objectives, Registration, Guide, News/ Additional Information)

ii. The content of the course is presented both in the form of Manuals/ppt and video.

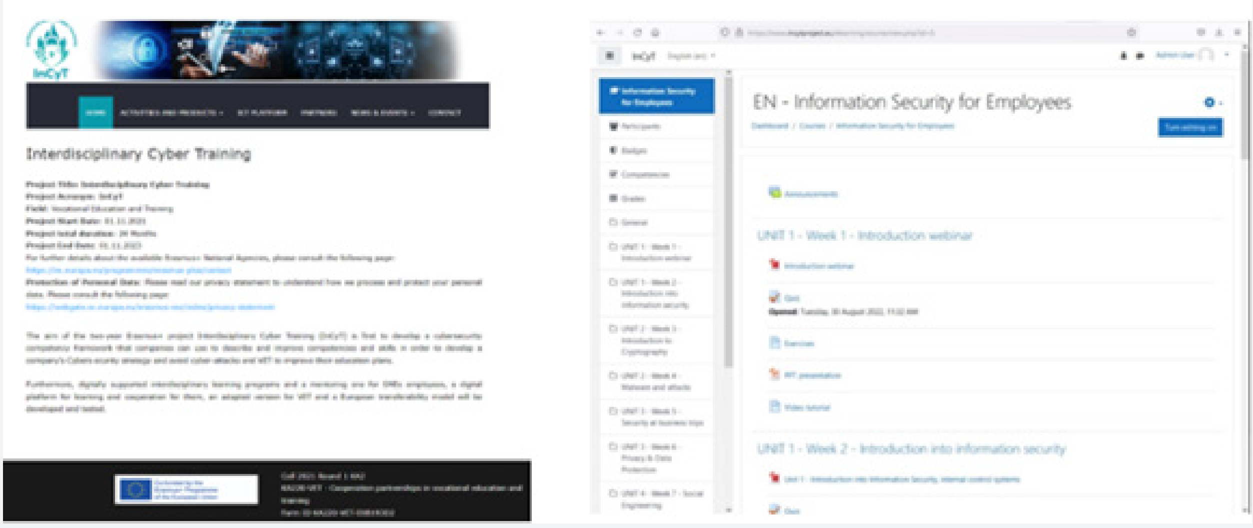
iii. Two training Modules (Employees, Managers) in seven languages: English, Turkey, Romanian, Denmark, Italian, Poland, German (including for Austria), and each module with eight training units.

iv. Bibliography

v. Quiz / Exercises for each Modules and final Exercises.

vi. Certification / Diploma

vii. Tools; FAQ (Chat – Forum, Media files, YouTube channel, Quiz, FAQ, E-Book for mentors) (Figure 2)



Interdisciplinary Cyber Training

EN - Information Security for Employees

UNIT 1 - Week 1 - Introduction webinar

UNIT 1 - Week 2 - Introduction into information security

Figure 2

How to cite this article: Gabriel V, Ileana H. Improving Cybersecurity Awareness and Basics in Vocational Education and Training. Ann Rev Resear. 2023; 9(5): 555774. DOI:10.19080/ARR.2023.09.555774

Next Task within InCyT

The next objective of InCyT, is to ensure that the project results i.e. training and digital InCyT platform can be adapted to be used in the future also by VET organisations increasing their cybersecurity awareness of its results. One deliverable is a report that details the project process, results of the course developed, and recommendations on transferring the course and platform to VET. The methodology to be use includes a comprehensive 9-step process, starting with defining objectives and concluding with the preparation of a report summarizing findings, especially in the realm of cyber security. Tasks are outlined sequentially from surveys and interviews, examining existing programs, creating transferability recommendations, drafting the report, peer reviews, and finalizing and publishing the report. These tasks have been adapted due to movement restrictions brought about by the COVID-19 pandemic, which prompted a shift from face-to-face to online activities. Metrics for measuring success are defined for each task, ranging from conducting online surveys to publishing the final report. The document also includes various templates as annexes for tasks such as surveys, analysis, recommendations, and report content. In each partner country a Multiply event within VET will be organized with educators and students to discuss concrete measures for developing special courses in order to achieve cyber awareness and avoid cyber-attacks like the presented in this file.

Conclusions

The importance of cybersecurity in education cannot be neglected. Educators, learners use increasingly technology to support learning and daily operations, so the security of used systems and data should become a high priority. This is a complex and can be a difficult task for educators and administrators who do not have enough knowledge in cybersecurity. Many resources and results of projects are available to help to develop your knowledge and skills in this area. Suitable learning facilities for learners should be created. Sure, cybersecurity professionals can help in this context. In particular, the project will help small and medium-sized enterprises without specific IT skills to assess their level of maturity to face today's cyber-attacks, and to adopt adequate policies and train their management and staff. For schools and universities, the introduction of a framework for entrepreneurship and digitization courses will be analysed, with the adaptation of the curriculum.

The platform would be a support tool (which may require adaptations / upgrades). For VET addressed to companies, it can be used directly, without major changes. A main provider will be the Chamber of Commerce and Industry, but other VET entities that provide services for the benefit of companies (VET entities, business and technologies parks and Incubators). The topic of cybersecurity training must be correlated with fields such as entrepreneurship, company management, and digitalisation. Despite the existing challenges, the need is clear to include cyber security in VET programs in Romania, to meet the growing need for cyber security professionals and to ensure that the workforce is prepared to face digital threats. It is necessary to digitize the systems in Romania and increase the IT skills of the citizens to utilise platforms Overcoming these challenges will require collaboration between educational institutions, stakeholders from the economy, industry, and social life and policy makers to develop large-scale and standardized cybersecurity training/education pathways for VET beneficiaries.

References

1. Assante D, Fornaro C, Strzalka D, Vârtopeanu G, Vladut G, et al. (2003) Cybersecurity education for SMEs, 20th International Conference on Remote Engineering and Virtual Instrumentation.
2. OECD (2021) The Digital Transformation of SMEs.
3. InCyT Website.
4. Bada M, Nurse JR (2019) Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security.
5. European Commission (2018) Digital Education Action Plan.
6. European Commission (2018) The Digital Skills and Jobs Coalition. In: Publications Office of the European Union, Luxembourg.
7. Vlăduț G (2018) Business transformation towards digitalization and smart systems, Annals of Reviews & Research-Juniper Publishers, California, United States 4(2).
8. Bauer J (2017) Hochschule Reutlingen, Conference, Leeipzig, Digital Transformation in Central and Eastern Europe, survey of enterprises with 250+ employees in five key countries.
9. Hamburg I (2021) Approaches to support learning in today ´s workplace. In: VI International Scientific Conference Winter Session: Industry 4.0 6(4): 284-288.
10. Stefan S, Berttram P (2016) Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused.
11. Shillai P, Esteve-González, Dutton W, Creese S, Nagyfejeo B, et al. (2022) Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise, Elsevier, Computers & Security, 119: 102756.
12. O'Brian E, Hamburg I, Vladut G, Southern M (2017) Learning to solve lifelong problems: Online PBL, 4th Annual HELLIN Conference.

How to cite this article: Gabriel V, Ileana H. Improving Cybersecurity Awareness and Basics in Vocational Education and Training. Ann Rev Resear. 2023; 9(5): 555774. DOI:10.19080/ARR.2023.09.555774

DOI:10.19080/ARR.2023.09.555774