Erasmus+ KA2 - KA220-HED - Cooperation partnerships in higher education
2021-1-TR01-KA220-HED-000031993

# R1/IDENTIFICATION CYBER THREATS AND SECURITY GAPS FOR NON IT ORIENTED HE COURSES

## EXECUTIVE SUMMARY REPORT

Cyber IN Practice – R1/Identification cyber threats and security gaps for non IT oriented HE courses
Executive Summary Report

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
"This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

## Project Identification

| | |
|---|---|
| Action Type | Cooperation partnerships in higher education |
| Project Agreement Number | 2021-1-TR01-KA220-HED-000031993 |
| Project Title | Cybersecurity in practice for non IT oriented HE courses |
| Beneficiary Organisation Full Legal Name (Latin characters) | MARMARA UNIVERSITY (E10205758 - Turkey) |
| Contact Person (Title, first name, last name, e-mail address) | Prof. Dr. Mert Erer, merterer@hotmail.com |
| Reporting Period (dd/mm/yyyy – dd/mm-yyyy) | 28/02/2022 – 27/02/2024 |

## Document Identification

| | |
|---|---|
| Document Title | R1 Executive Summary Report |
| Circulation to | All Partners |
| Prepared by | MU |
| Document Reference | |
| Document History | Version 1, 17.02.2023 – Team MU |

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
"This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

# Introduction

The following report was prepared as a part of Erasmus Strategic Partnership in Higher Education named "Cybersecurity in practice for non IT oriented HE courses". In this document, the first result of the project, Identification cyber threats and security gaps for non IT oriented HE courses, will be summarized.

In the light of the many new concepts brought by Industry 4.0 in today's world and the digitalized world, human beings are developing new needs and demands against the changing world dynamics. Although the new concepts that have entered our lives, the digitalization of many processes in both economic and cultural terms allows both the margin of error to be reduced and the time and manpower to be saved. On the other side of the coin, however, it is undeniable that all these processes bring with them new risks and threats. In today's world, these risks and threats appear under the title of "cyber". Against all these risks and threats, it becomes a natural condition of life for people to have cyber security awareness. In this context, the creation of cyber security perception and awareness in universities, which are the center of cultural interaction and scientific reality in society and where, in the words of German scientist Karl Jaspers, students and academics pursue the truth together, is seen as very important in a social sense.

The untimely and unexpected entry of the Covid 19 pandemic into human life has deeply affected universities and educational processes, as well as all areas of life. The use of education and training techniques and methods that have not been tried or used before, the use of remote methods in the flow of information and documents within the university in extracurricular processes, and keeping and storing the data provided in this way in virtual networks rather than physically, have required many processes in universities to change from

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

top to bottom. However, it has been clearly observed that these changes bring with them many threats, risks and vulnerabilities.

In order to determine what these cyber risks and threats are within universities and to create a solid basis for the creation of learning nuggets, three main steps are envisaged within Result 1. These are listed and briefly explained as follows.

- **The Desktop Analysis**: The bibliographical research and survey based country analysis in all participant (partner) countries.

- **Conducting Focus Group Analysis**: Organization of focus groups around selected non-IT disciplines. Level of competencies, ways of dealing with cyber threats during the preparation, teaching and learning processes were investigated. The focus groups conducted either face-to-face or virtually for deeper and narrower information of the exact skills and competencies as well as common challenges and most importantly - unknown/newly emerged needs of the specialists and trainers as target groups.

- **Collecting use cases in cyber threats and risk management**: Each partner country conducted a survey among main stakeholders (companies, ICT businesses, professional associations/organizations, education institutions in particular, non IT sciences) and generated a report with key findings in terms of frequency of the cyber threats in the pandemic conditions; precise requirements/practices in terms of cybersecurity.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

## Short Assessment of R1A1

According to the results of the desktop analysis conducted across countries, key conclusions have been reached that justify the main objective of the project.

Especially after 2010, steps have been taken in all partner countries to integrate digitalization, but there are many gaps and weaknesses in the cyber security procedures that digitalization will bring, both within the public and universities. All countries, with a special emphasis on Eastern European countries, should continuously review and develop new strategies, procedures and measures to meet the new demands for high quality digital education. It is evident that these steps are just beginning to be taken on a national basis, but there is still a long way to go.

Although the situation in higher education is the centerpiece of the project, the current situation in secondary education is addressed in this section of the study, as it will allow the structure and development of the education system in the partner countries to be revealed.

Particularly in recent years, it has been observed in all partner countries that information technology courses have started to be included in secondary education curricula, but it is reported that educational steps in the field of cyber security remain insufficient. In this context, even though such courses are included in the curricula, it is seen that there are question marks and gaps in the teaching of the courses, the knowledge and competence of the lecturers in the field, and the evaluation of the learning outcomes of the student body taking the course. It is also crucial that such innovative courses and subjects with digitalization at their core are taught with new techniques blended with modern methods, rather than classical learning techniques.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

It should be noted that these curricula are still under development in schools. Therefore, it is important to complete a certain time cycle in order to achieve full efficiency. It is an indisputable fact that the processes in universities can be carried out more efficiently if students equipped in the field of information technologies and cyber security are trained in secondary education.

There are many different departments, programs and specializations within universities in partner countries, such as information technologies, systems engineering, software engineering, cyber security, etc. These departments and programs are inherently centered on digital processes. But apart from that, when non-IT programs are examined with reference to the subject of the project, it is noticeable that there are innovative paths to be taken within the courses. In this context, the digital awareness and knowledge of university lecturers, as well as whether universities have a student-oriented approach in this field, are among the most important topics.

Today, it is a fact that almost all of the young generation are "online users". However, it is doubtful whether they have a proactive attitude towards the risks and threats brought by the digital world they are in, and whether they have an awareness that will protect them in this area. In this context, the widespread use of digitalization not only among the younger generation but also among all people will allow the flow of information between students and lecturers to be established on a more solid and modern basis.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

# Short Assessment of R1A2

Following the bibliographic analysis in partner countries obtained in R1A1, focus group studies were conducted across universities in partner countries. The aim of these studies was to reveal the cyber awareness, cyber security knowledge levels and cyber behaviors of students, academics and administrative staff, as well as to examine the activities and trainings carried out by universities on cyber security. As a result of all these, the aim is to reveal the cyber threats, risks and gaps that exist in higher education.

This study is considered very important as it will provide the necessary infrastructure for the "learning nuggets" to be created in R2, which are the backbone of the project.

In total, 131 students, academics and administrative staff from non-IT departments participated in the focus group discussions, which lasted between 70 and 90 minutes and were conducted physically at the University of Opole, Building of the Faculty of Economics, Marmara University Business School, Muğla Sıtkı Koçman University Business School, as well as virtually through online meetings and e-surveys. All of the studies were conducted in October 2022 and included participants from different fields such as business, economics, biology, political science and psychology.

A total of 12 questions were asked in the interviews and these questions are listed below:

| | |
|---|---|
| 1 | Could you please introduce yourselves briefly? |
| 2 | Have you taken part in a study on a similar topic before? What are your expectations about the session we will hold? |

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
"This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

| | |
|---|---|
| 3 | How would you describe cyber security? Can you list at least 3 cyber threats? |
| 4 | What do you think should be considered when choosing a password? |
| 5 | Do you follow the links from the e-mails for “lottery win” or “changes in bank account”? How often do you make online transactions or orders? Do you feel safe when you make transactions or share private information? |
| 6 | On which platforms are you active in social media? How often do you use them? What kind of information do you share on social media? |
| 7 | Do you use antivirus application on your devices?<br>if yes, Would you define which? Do you have other security measures on your devices? How often do you update them?<br>if no, What kind of security measures do you have on your devices? |
| 8 | How important do you consider staying informed about cyber security? How do you keep yourself up-dated on cyber security related issues from professional and individual point of view? |
| 9 | What do you think is the role of the HEI top management in minimizing the cyber threats in the learning environment of HEI? Are you aware if your HEI developed a measurement tool about cyber security awareness both for academic staff and students? |
| 10 | Do you feel your private data is secure when you use the learning environment at your HEI? What is the reason behind your answer? |

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

MARMARA UNIVERSITY · MUĞLA · TRAINING 2000 ITALY · БИТ · EduVibes · University of Applied Sciences and Arts of Southern Switzerland SUPSI

| | |
|---|---|
| 11 | Is there any programme/short informative course which has been created to further educate the academic staff and students, in order to reduce their chance of falling victim to cyber attacks in the learning environment in the HEI? What actions does your university take to raise awareness of cyber security in courses or extracurriculars? |
| 12 | Are there any other points that you would like to add regarding the topic? |

The results obtained in the studies are generally close to each other.  It has been observed that the participants have some basic knowledge and understanding of cyber security, but their level of awareness is not always at satisfactory levels.

Interviews with students show that different results have been reported regarding the cyber awareness and knowledge levels of students studying in non-IT departments in Turkey, Bulgaria, Italy, Poland and Switzerland. In this context, students are interested and active users of digital tools (internet, social media, etc.) and are familiar with the basic concepts. However, it is difficult to say that they always show sufficient caution against the risks and threats brought by digitalisation.

Although students do not know the technical names of cyber attacks and categories, they are able to describe the attack methods in general. They are able to give a general description of cyber security and fulfil the primary requirements against the main threats. Although they avoid very simple preferences when choosing passwords, they can sometimes reuse the same password on different platforms or record it in writing. They say that they can recognise phishing attacks, which are quite common today, and usually delete these e-mails

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

immediately. However, it is also seen that their awareness of effective attacks is not at a deep level.

Students state that they use online shopping options, which is a reality today; however, they add that they do not feel very safe when sharing their personal data in this process.

The results obtained in Switzerland show that students' cyber security awareness and knowledge levels are at a higher level compared to other countries. This situation plays a decisive role in the comparison with other partner countries, because in other countries, cyber security is not on the agenda of universities, while students do not have detailed information about what kind of activities are carried out in this field in their higher education institutions. In Turkey, Bulgaria and Poland, students have general knowledge, whereas in Italy, awareness is assessed as low.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

## Short Assessment of R1A3

In R1A1, as a result of the findings obtained in the bibliographic analysis carried out under the title of cybersecurity in higher education in partner countries, focus group studies were carried out with the participation of students, academics and administrative staff within universities in R1A2 to identify cyber threats and risks in higher education. Afterwards, use cases regarding cyber threats and attacks observed by professionals during the pandemic process were collected within the framework of R1A3. In this context, the cyber risks and threats encountered and the measures and precautions taken against these threats were detailed. The cases were collected through face-to-face interviews, e-surveys and online meetings.

In addition to demographic questions, these cases sought answers to four main questions.

| | |
|---|---|
| 1 | During the pandemic, how often have you encountered individual & organizational cyber risks and threats in your digital business processes? |
| 2 | What are the individual & organizational cyber risks and threats you have encountered in digital business processes under pandemic conditions? |
| 3 | What precautions have been taken against the individual and organizational cyber risks and threats you have explained in the previous two questions? |
| 4 | Which other measures do you think are necessary if you think the measures taken are not sufficient? |

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

During the pandemic period, changing business processes with the transition to remote working, which people were not used to until that day, brought along many new cyber threats, attacks and vulnerabilities. When the collected use cases are analyzed, it is seen that phishing, ransomware, spam, social engineering and service attack are the most important ones.

According to the sectors, the probability of success of these attacks and the reactions to the attacks may vary. However, the situation may be different in sectors such as e-commerce and manufacturing, which do not have one-to-one experience and relationship with IT issues.

In this context, the most important thing is to increase the awareness and knowledge of employees and internal stakeholders, which is also the subject of the project. For this purpose, it is considered very important to conduct trainings within the company on a regular basis.

In order to prevent incoming attacks, it is important to determine an effective "data protection and cyber security policy" within the company and to establish a guideline for this. Thus, after raising awareness, a documentation can be created on which procedures should be followed and what kind of escape plan should be implemented in case of a possible threat.

Not only the employees but also the shareholders and owners of the company play an important role in cyber security issues. It is very important to invest in preventive software and tools and to include items related to cyber investments in business budgets. In this context, investment budgets should be allocated for firewalls, intrusion detection, virus and malware protection softwares.

Reviewing and strengthening all passwords used both individually and organizationally is one of the simple but highly effective measures. By using complex passwords, malicious

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

algorithms should be defocused and applications that ensure password security and recording should be used. In addition, ensure that wi-fi networks are secured.

Last but not least, experience sharing events should be increased and workshops should be organized based on the incidents and thus, in addition to raising awareness, current solutions should be discussed both in the academic and corporate community.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".

“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

# Conclusion

In order to realise the project, it is very important to establish a solid infrastructure. In this context, in order to be able to provide cyber security education in non-IT HE courses within Result 2 and to prepare learning nuggets for raising awareness and perception on cyber related issues, it is vital to first identify which issues are considered as a cyber risk and threat by university students and employees.

The bibliographic study carried out in partner countries shows that, especially in recent years, cyber security as well as digitalisation-based topics are gradually finding their place in secondary education curricula. However, it is seen that these initiatives are still quite new and have problems in realising the transition from the theoretical framework to practice. It is seen that students who do not prefer technical faculties (Engineering, Information Technologies, Software Sciences, Cyber Security, etc.) and who continue their education in non-IT departments remain away from cyber-related subjects, as students specialise in the fields they want in line with their own preferences by leaving the common curriculum practice in universities. At this point, it is a vital issue to update the course curricula, course contents and education methods and to respond to the needs of the age as well as the need for people who have mastered the field to teach as teachers/lecturers.

In the second step, focus group analysis, almost all of the participants emphasized that this was the first time they had participated in a study of this type, and they were willing to continue such studies and to increase their awareness and development in cyber security.

Among the participants, especially students are seen to be very active in using social media, but they can sometimes be negligent about cyber privacy and security issues in social media.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
"This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

Although they do not fall into basic pitfalls, it is seen that there is a need to make progress in thinking one step ahead as well as some technical deficiencies.

Most of the participants stated that cyber security is not among the "priority issues" for universities, and argued that it would be beneficial for universities to focus on studies in this direction.

In the third step, the use cases collected from the partner countries were focused on the perspectives of professionals instead of the perspective of students, thus addressing the issue of what kind of cyber-attacks emerged during the pandemic period, when the popularity of digital processes increased even more, and what kind of risk management process was carried out to prevent these attacks. In this context, it has been seen that cyber-attacks have become a world reality in today's conditions and have the power to affect companies from every sector and people from every profession. It has been observed that even in units operating in the field of technology, seemingly simple attacks can have devastating effects, therefore, it has been revealed that the concept of "awareness" is not always sufficient, as well as the importance of developing an effective and proactive mindset and knowledge level.

Considering the focus group studies and the use cases collected, it seems appropriate to list the cyber risks and threats that seem reasonable to be addressed within Result 2 as follows:

- Data Breaches
- Privacy Violations
- Phishing/ Skimming Incidents
- Technology-focused Threats such as hacking, malware and spyware
- Content-related Risks (exposure to illicit or inappropriate content),
- Harassment-related Threats

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

- Risk of Exposing Information

Taking these risk and threat groups as a basis in the creation of learning nuggets was obtained within first Result. In this process, increasing cyber security knowledge in the courses, being cautious against attacks, as well as outlining how to create an effective escape plan seem to be the crucial goals of the further results.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects 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".
“This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.