
Project no: 2020-1-LT01-KA203-078070

# IO1 A2: Results "Analysis of Existing Cybersecurity training programmes"

REPORT

2021

# Partnership


Vilnius University, Lithuania

Website: http://www.vu.lt

University of Tartu

Website: https://www.ut.ee/et


MECB - Macdac Engineering Consultancy Bureau LTD , Malta

Website: http://www.mecb.com.mt/eu


Altacom SIA, Latvia

Website: https://www.altacom.eu/


DOREA Educational Institute, Cyprus

Website: https://dorea.org/


ECDL- Information Technologies Institute, Lithuania

Website: http://www.ecdl.lt/

Funded by the Erasmus+ Programme of the European Union


(Project N°.: 2020-1-LT01-KA203-078070)

# Table of Contents



# List of Tables




Funded by the Erasmus+ Programme of the European Union




(Project N°.: 2020-1-LT01-KA203-078070)

# List of abbreviations

| | |
|---|---|
| **CCS** | Cyprus computer society |
| **CERT.LV** | Latvian Computer Emergency Response Team |
| **CSSS** | Cybersecurity skills shortage |
| **ESCO** | European Cybersecurity Organisation |
| **ENISA** | European Union Agency for Cybersecurity |
| **EU** | European union |
| **HITSA** | Information Technology Foundation for Education |
| **ISACA** | Information Systems Audit and Control Association (ISACA) |
| **ISC2** | International Information System Security Certification Consortium |
| **NCSC** | National Cybersecurity Centre at the Ministry of National Defence (the Republic of Lithuania) |
| **NCSS** | National cybersecurity strategies |
| **OCECPR** | Office of Commissioner of Electronic Communication & Postal Regulation (the Republic of Cyprus) |
| **RIA** | Information System Authority (the Republic of Estonia) |
| **SMEs** | Small and medium enterprises |

Funded by the Erasmus+ Programme of the European Union


(Project N°.: 2020-1-LT01-KA203-078070)

# 1. INTRODUCTION

## 1.1. Cybersecurity skills shortage (CSSS) and reasons behind it

Based on the annual global study from Enterprise Strategy Group and the Information Systems Security Association[1] conducted in 2019, the cybersecurity skills shortage has impacted 74 % of organisations globally. The main consequences of this shortage indicated in the report are increased workload on existing staff, inability to utilise some security technologies, and recruitment and training junior personnel instead of hiring more experienced professionals. The most critical skills shortages are cloud computing security (33%), application security (32%), and security analysis and investigations (30%).

Furthermore, according to research carried out by the Information Systems Audit and Control Association (ISACA)[2] in 2019, 57% of organisations had unfilled cybersecurity vacancies. The time needed to fill in these positions usually was three months, as indicated by more than 60 % of respondents who to part in the research. Most of the unfilled job positions are in individual contributor (both technical and non-technical cybersecurity) and cybersecurity manager positions. The demand for job positions in the individual contributor (technical cybersecurity) area is expected to grow in the upcoming years. In contrast, the demand for other jobs is expected to stay the same or increase slightly.

One of the main reasons indicated by respondents why the positions remain unfilled is the lack of qualified applicants. Almost one-third of organisations claimed that around 75% of candidates did not possess the right qualifications for the job. The most significant skills gaps indicated by respondents were lack of soft skills, IT knowledge, insufficient business insight, cybersecurity technical experience and practical experience.

According to ENISA[3], consultations with the Member States had identified a cybersecurity awareness and skills gap in the population as being among the key obstacles to building secure cyberspace. *"Notwithstanding the availability of almost 600 academic institutions and training centres offering cybersecurity programmes across Europe, the cybersecurity skills gap across all sectors remains a significant challenge"*(ENISA, 2019, p. 10).

In 2020, the estimated global shortage of cybersecurity workforce was around 3.12 million professionals[4]. In contrast, in Europe alone, the cybersecurity workforce gap is estimated to be 350 000 workers by 2022. The number has doubled from what was estimated in 2018[5].

*Reasons behind cybersecurity skills shortage (CSSS)*

ENISA, in their "Cybersecurity skills development in the EU" report, has indicated four leading causes that might contribute to the cybersecurity skills shortage. Two of them are focused on workplace issues, while the remaining two are associated with issues in the education and training system. To be specific:

1. *The cybersecurity job market is relatively immature and dynamic*, resulting in job specifications being highly dependent on the organisation's size and sector. For example,

[1] Jon Oltsik (2019): The Life and Times of Cybersecurity Professionals 2018, URL https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/surveys/esg-issa-2018-survey-results.pdf (accessed 09/03/2021)
[2] ISACA (2020): State of Cybersecurity 2020 Part 1: Global Update on Workforce Efforts and Resources, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf (accessed 09/03/2021)
[3] ENISA (2019): Cybersecurity skills development in the EU, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf (accessed 09/03/2021)
[4] (ISC)² (2019): (ISC)² Study Reveals the Cybersecurity Workforce Has Grown to 3.5 Million Professionals Globally, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study-Reveals-the-Cybersecurity-Workforce-Has-Grown-Globally (accessed 09/03/2021)
[5] (ISC)² (2019): Cybersecurity workforce study, URL https://www.isc2.org/Research/Workforce-Study (accessed 09/03/2021)

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

SMEs that are not specialised in the cybersecurity sector tend to hire generalist IT staff who have some knowledge of cybersecurity. In contrast, larger SMEs and those specialising in cybersecurity have staff focused on specific cybersecurity areas.

2. *Employers are not offering the right training level*, which prevents both the creation of a sustained workforce pipeline and current employees' professional development. This creates obstacles for cybersecurity professionals with a more general background to further develop the necessary professional skills.
3. *Academia is failing to produce candidates with the proper knowledge and skills.* Students also lack hands-on experience, resulting in a skills mismatch between the industry's needs and the skills students possess.
4. *There is a slow responsiveness of cybersecurity curricula comparing to the developments of the field.* Due to the bureaucracy involved, so far, cybersecurity curricula have struggled to keep up with emerging threats and news skills needed to deal with those threats.

## 1.2. Digital and cybersecurity education policy in the EU

In 2013, the European Commission published its first cybersecurity strategy, highlighting awareness-raising and skills development as key strategic objectives.

*"In 2017, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy stated again that there is a strong education dimension to cybersecurity and that effective cybersecurity relies heavily on the skills of the people concerned. They recommended that together with the Member States, the EU should enhance cybersecurity education and skills by building on the work of the Digital Skills and Jobs Coalition and establishing European cybersecurity industrial, technology and research competence centre and network of national cybersecurity coordination centres".* (ENISA, 2019, p.23)

In 2019, four projects— CONCORDIA, ECHO, SPARTA and CyberSec4Europe[6] — were launched under the Horizon 2020 programme aiming to develop a common European Cybersecurity Competence Network and European Cybersecurity Research & Innovation Roadmap.

In 2020, the European Commission proposed the Digital Europe Programme[7], the EU's programme to accelerate the digital transformation of Europe. The programme is expected to allocate 580 million euros to develop advanced digital skills by supporting the design and delivery of specialised programmes and traineeships for future experts in key capacity areas such as AI, cybersecurity, quantum, etc.

In March 2021, The European Council adopted new conclusions on EU cybersecurity strategy[8]. The conclusions recognise the shortage of digital and cybersecurity skills in the workforce and emphasise the need to meet the market demand through the further development of educational and training programmes.

[6] European Commission (2019): Four EU pilot projects launched to prepare the European Cybersecurity Competence Network, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network (accessed 10/03/2021)

[7] European Commission (2020): Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027 (accessed 10/03/2021)

[8] Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy (accessed 24/03/2021)

## 1.3. National cybersecurity strategies (NCSS)

Since 2017, all EU Member States have developed and published their national cybersecurity strategies (NCSS).

*Cyprus*

The Republic of Cyprus is aware of the importance of cyber education to guarantee National cyberspace protection. One of the existing cybersecurity strategy's main goals is to promote cybersecurity and raise awareness in its public (citizens, workforce, and youth) and build a cooperative atmosphere for implementing the strategy.

The Cybersecurity Strategy of the Republic of Cyprus was introduced in 2012[9]. The Cypriot national strategy aims to develop technical training in the cyberspace security area and teach how to protect oneself and deal with urgent situations. One of the goals is to build a specialised workforce capable of handling a real cyberattack. For that, exercises were to be held to observe the workforce's coping response in a simulated realistic crisis. The implementation of the strategy should result in the enforcement of cyber specialised job descriptions and certifications.

The strategy is comprised of 17 specific actions. These actions include the identification of available appropriate personnel training programmes and certifications in the field of cyber and digital security.

The Republic of Cyprus is also dedicated to establishing public-private partnerships to support higher education institutions by incorporating cybersecurity subjects and strengthening the training of professionals and academics in the cybersecurity field.

The newest version of the national cybersecurity document was developed in 2020. The strategy is currently under review and is pending final approval from the Ministry of Communication and the Council of Ministers.

Digital Security Authority (DSA)[10] is an independent governmental agency under the Commissioner of Electronic Communications and Postal Regulation supervision. It is responsible for implementing the European NIS (Network and Information Security) Directive, focusing on upgrading and maintaining high levels of cybersecurity for all of the operators of essential services and critical information infrastructures in Cyprus. The agency also aims to raise cybersecurity awareness among society and boosting Cyprus international competitiveness in general.

Another important organisation is Cyprus computer society (CCS)[11], an independent non-profit organisation founded in 1984 to develop, upgrade, and promote Cyprus's IT sector. CCS seeks to set high standards among industry professionals, recognising the impact that Information and Communication Technologies (ICT) has on employment, business, society, and citizens' quality of life. One of the annual events organised by CCS is the Cybersecurity Challenge[12]. The event aims to discover cyber talents and motivate youth to pursue a career in cybersecurity.

[9] OCECPR (2012): Cybersecurity Strategy of the Republic of Cyprus , URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus (accessed 11/03/2021)
[10] Digital Security Authority (DSA), URL https://dsa.cy/en/
[11] Cyprus computer society (CCS), URL https://ccs.org.cy/en/
[12] Cyprus cyber security challenge, URL https://ccsc.org.cy/#home

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

*Estonia*

Estonia was one of the pioneers in the publication of cybersecurity strategies and currently has its third version of a national cybersecurity document[13]. The strategy is divided into four areas: 1. Sustainable Digital Society; 2. Cybersecurity Industry, Research and Development; 3. Leading International Contributor; 4. Cyber-liberate Society.

The Estonian strategy in very inclined to enhance cyber education, and its applicability is described on the second objective of the plan. Since 2014, the country has been investing in education and deals with universities to promote cyber studies, funding projects, and supporting scholarships. The goal is to guarantee that the digital technology and cybersecurity competencies are included in live training to prepare the public for cyber understanding.

The Ministry of Education and Research oversees these educational projects and follows the Cybersecurity Strategy's established priorities to execute the lifelong learning plan and support the development of basic cyber education to all levels of graduates.

According to the strategy, the fulfilment of the strategic objectives is supported by the Information Technology Foundation for Education (HITSA), which contributes to the training of specialists in the field through coordinating both the *Targalt Internetis* ("Staying Smart Online") and the IT Academy programmes.

Another important organisation is the Information System Authority (RIA)[14] , which coordinates information systems' development and administration, organises activities related to information security, and handles security incidents. RIA has also plays a central role in cyber hygiene, prevention activity and increasing awareness in society.

*"The broad-ranging prevention and awareness campaigns will be launched to spread the word about cyber threats to different target groups, including businesses. To raise the level of cyber hygiene at government institutions, it will become obligatory for government institutions and local government employees to pass tests on knowledge of cybersecurity. Training courses and information outreach for target groups will be continued*". (The Republic of Estonia, Ministry of Economic Affairs and Communication, 2019, p. 67).

*Latvia*

In Latvia, the concern with National security is also connected with the current technological development. The first Latvia's cybersecurity strategy came into effect in 2014, with the plan's approval from 2014 until 2018. In 2019, a new cybersecurity strategy for 2019- 2022 was approved. The updated strategy aims to strengthen and improve Latvia's cybersecurity capabilities by enhancing public awareness and resilience against cyber-attacks. To achieve these objectives, the strategy proposes actions in six areas[15]:

1. enhanced cybersecurity and manageable digital security risks;
2. the resilience of ICT systems;
3. better universal access to strategic ICT systems and services;
4. public awareness, education, and research;
5. international cooperation;
6. the rule of law in cyberspace and cyber-crime prevention.

[13] Republic of Estonia, Ministry of Economic Affairs and Communication (2019): Cybersecurity Strategy, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf (accessed 10/03/2021)
[14] Information System Authority (RIA), URL https://www.ria.ee/en.html
[15] Latvian Defence Ministry (2019): Latvia approves new Cyber Security Strategy 2019-2022, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022 (accessed 11/03/2021)


Funded by the Erasmus+ Programme of the European Union

When it comes to the area of "Public Awareness, Education and Research", the strategy indicates five main tasks[16]:

- provide support for research development in the field of cybersecurity;
- raise awareness of learners and educators in information security, privacy protection and the use of reliable e-services;
- strengthen public awareness of safe internet use (develop educational and informative materials for various age groups with safety recommendations, activities using the internet, organising social campaigns). Develop and implement annual interinstitutional work and action plan for companies' information and awareness building on cybersecurity issues;
- promote awareness of safe use of ICT among the staff of local and state institutions;
- promote educational activities and competitions in the field of cybersecurity.

The strategy also highlights the need for better engagement from the public and private actors to strengthen cybersecurity systems' resilience and provide investments in ICT security and employees' training.

The Latvian Computer Emergency Response Team (CERT.LV) is responsible for monitoring and handling cybersecurity incidents. CERT.LV also organises educational events and training courses for the general public. Under the new strategy, CERT.LV is expected to develop resources with the public and private sectors for collecting intelligence on incidents for analysis and evaluation[17].

Another important organisation is the Latvian Safer Internet Centre. Its main tasks are to educate, inform and raise public awareness about the safer use of the internet, provide a platform for reporting illegal content and security breaches online to a hotline, and offer professional psychologist consultations via its helpline[18].

*Lithuania*

In 2018, updated the Government approved Lithuania's National Cybersecurity Strategy of the Republic of Lithuania[19].

*"The strategy's primary purpose is to provide the Lithuanian society with the opportunity to exploit the potential of information and communications technology (ICT) by identifying cyber incidents effectively, preventing their occurrence and spread, and managing consequences resulting from cyber incidents*. Resolution on the approval of the national cybersecurity strategy, 13 August 2018 No. 818

To achieve its objective, the strategy proposes five targets:

1. strengthen the cybersecurity of the country and the development of cyber defence capabilities;
2. ensure prevention and investigation of criminal offences in cyberspace;
3. promote cybersecurity culture and development of innovation;
4. strengthen close cooperation between private and public sectors;
5. enhance international cooperation and ensure the fulfilment of international obligations in the field of cybersecurity.

[16] Latvian Defence Ministry (2019): Latvia's cyber security strategy for 2019 – 2022, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf (accessed 11/03/2021)
[17] Cyber Wiser (2021): Education and training in national cybersecurity strategy, URL https://www.cyberwiser.eu/latvia-lv (accessed 11/03/2021)
[18] ENISA, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Latvia
[19] Government of the Republic Of Lithuania (2018): Resolution on the approval of the national cyber security strategy, URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

Promoting cybersecurity culture and innovation is the key target of the national strategy. The strategy proposes these actions to reach this specific target[20]:

- continuous and regularly updated training courses for private and public sector employees aimed at increasing employee awareness and building an overall cybersecurity culture;
- continuous dissemination of information on the latest cyber incidents;
- making ICT education a part of educational processes from an early age, starting from the nursery till secondary school;
- continuous teacher upskilling and training aimed to improve their qualifications in cybersecurity.

The strategy emphasises the need to develop cybersecurity skills and competences to meet market needs continuously. To achieve this goal, the strategy proposes "*creating a cybersecurity competence model and standards, developing training systems, accreditation and certification oriented towards the needs of the labour market, providing training and testing environments for cybersecurity, offering training to ICT workers, etc*." Resolution on the approval of the national cybersecurity strategy, 13 August 2018 No. 818

The strategy also highlights the need to develop innovations in the cybersecurity area. To achieve this goal, the cooperation between key public and private actors and academia is crucial.

National Cybersecurity Centre at the Ministry of National Defence (NCSC)[21] is a central Lithuanian cybersecurity institution responsible for handling cyber incidents, monitoring the implementation of cybersecurity requirements, and accrediting information resources. The NCSC also works on promoting cybersecurity awareness in society.

*Malta*

The National Digital Strategy for Malta, also known as Digital Malta,[22] was implemented in 2016. The strategy covers the need and expectations of three key national stakeholders – the public sector, the private sector and civil society to ensure cybersecurity. There are five dimensions outlined in the strategy upon which the strategy is based - Policy, Legislation, Risk Management, Culture/ Awareness and Education.

The strategy proposes four key goals:

1. combat cybercrime by identifying gaps and strengthening law enforcement agencies capability to investigate cybercrime;
2. strengthen national cyber defence by guiding and assisting public and private entities in improving their cyber defence capabilities;
3. secure cyber-space higher levels of trust by implementing awareness programmes and the delivery of trustworthy, ICT-enabled services;
4. build capacity (cybersecurity awareness and education) by identifying and developing skills and educational frameworks required.

The last key goal (Awareness and Education) targets academia, the public and private sector and citizens as a means to increase awareness, knowledge as well as capabilities and expertise in cybersecurity through an ongoing educational and awareness campaign, as well as rigorous and

[20] Cyber Wiser (2021): Education and training in national cybersecurity strategy (LT), URL https://www.cyberwiser.eu/lithuania-lt (accessed 11/03/2021)
[21] National Cyber Security Centre, URL https://www.nksc.lt/en/
[22] The Malta Information Technology Agency (2016): Malta Cyber Security strategy 2016, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Malta (accessed 12/03/2021)

Funded by the Erasmus+ Programme of the European Union

(Project N°.: 2020-1-LT01-KA203-078070)

continuous educational and training exercises targeting both the current workforce as well as the younger student generation. This measure thus primarily entails[23]:

- Further recognition of the need for cybersecurity skills and competencies;
- Academic and training programmes designed to consolidate cybersecurity expertise;
- Review of existing curricula that focuses on cybersecurity along with ICT and media competencies.

The strategy also aims to empower the youth through their support network, namely parents, carers, educators, and youth workers. It is foreseen that *"Digital Citizenship"* will become part of the National Education Curriculum to equip children and youths with the skills needed to use the internet while producing creative online content safely.

Digital Malta states the Government's commitment through educational institutions and industry to support the creation of specialist educational pathways, address labour market requirements, and develop the curriculum and provide technical materials. Cybersecurity related training and certification programmes should be further encouraged as an opportunity to effectively increase the security level of organisations and maintaining such an increased level of security in the long term.

Cybersecurity Malta[24] is part of Malta's National Cybersecurity Strategy, which aims to establish a governance framework, combat cybercrime, strengthen national cyber defence and provide cybersecurity awareness and education. One of the key goals of the National Cybersecurity Strategy is nation-wide cybersecurity awareness and education campaign.

Another important organisation is Malta's national Computer Security Incident Response Team (CSIRT). CSIRT Malta supports Malta's critical infrastructures organisations in protecting themselves and their data from cyber threats and incidents[25].

## 1.4. "Safeguarding Against Phishing in the Age of 4th Industrial Revolution" project

Cybersecurity becomes one of the biggest challenges[26] in the digital age because information becomes an expensive asset dealing with huge data volumes, improving communication with the digital environment. Digital devices and information systems increasingly become attractive for cyber-attacks.

Phishing is one of the biggest problems because cybercriminals use faster and innovative technological tools to carry out phishing campaigns. Therefore, human-driven phishing defence system that leverages human instinct for detection and technology to scale response should be developed and freely available for a broad audience. To create a human-driven phishing defence, education is required for the user to identify and respond to phishing attacks in the correct manner.

The international project "Safeguarding against Phishing in the age of 4 Industrial Revolution" ("CyberPhish") initiated by Vilnius University Kaunas Faculty and partners has started at the beginning of November 2020 and will last for two years.

The project's objective is to educate students of higher education institutions, educators, university staff (community members), education centres, the business sector (employers and employees) and encourage critical thinking of the target group in the cybersecurity field.

The project partners will design a curriculum, e-learning materials, a blended learning environment, knowledge and skills self-assessment and knowledge evaluation system simulations for students

[23] Cyber Wiser (2021): Education and training in national cybersecurity strategy (MT), URL https://www.cyberwiser.eu/malta-mt (accessed 12/03/2021)
[24] Cyber Security Malta, URL https://cybersecurity.gov.mt/
[25] Cyber Security Intelligence, URL https://www.cybersecurityintelligence.com/csirt-malta-2727.html (accessed 12/03/2021)
[26] European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020

and other users to prevent phishing attacks, raise competencies, which will help to focus attention to threats and take appropriate prevention measures.

The project partnership is comprised of six organisations coming from five European countries:

1. Vilnius University, Lithuania (Coordinator)
2. Information Technologies Institute, Lithuania
3. DOREA Educational Institute, Cyprus
4. University of Tartu, Estonia
5. Altacom SIA, Latvia
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

For more information about the project and project activities, please visit the project's website: https://cyberphish.eu/

Updates on the project in general and Cybersecurity in particular may also be followed on the project Facebook page at: https://www.facebook.com/eucyberphish.

Funded by the Erasmus+ Programme of the European Union


(Project N°.: 2020-1-LT01-KA203-078070)

# 2. STUDY ANALYSIS

## 2.1. The methodology of data collection

To research on existing study programmes and training programmes in the area of cybersecurity and phishing, the leading organisation of IO1 (DOREA Educational Institute) has prepared the template. The template covered the key information such as accreditation and academic title, programme structure and course information.

*Table 1: Template for analysis of existing programs in the area of cybersecurity and phishing*

| **Title of the programme or course** | |
|---|---|
| Type of the programme | |
| Study field | |
| Degree | |
| Organising Institution | |
| Language of instruction | |
| Duration (hours or ECTS) | |
| Target group | |
| Main focus: topics or modules | |
| Learning outcomes | |
| Methodology (if applicable) | |
| Reference link/URL | |

All partners were encouraged to use the Cybersecurity Higher Education Database[27] and do their national research as some study programmes are not yet uploaded in the existing database.

The project partners were also asked to do short research in national policies/strategies for cybersecurity education. The research was carried out in all partner countries – Cyprus, Estonia, Latvia, Lithuania, and Malta. The results of the study analysis were transferred to the National table of findings (structured per country – Cyprus, Estonia, Latvia, Lithuania, and Malta)

The gathered data will be used to identify the skills gaps and prepare recommendations for a new curriculum to strengthen the skills, education, and awareness of internet users on the latest emerging cybersecurity issues and threats, in particular – phishing.

Overall, based on the desktop study outcomes on the existing cybersecurity study curriculum and survey results, the partner consortium will develop training material, knowledge self-assessment and knowledge evaluations tests, and simulations scenarios for training.

[27] The Cybersecurity Higher Education Database (CyberHEAD) is the largest validated cybersecurity higher education database in the EU and EFTA countries. URL https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/education-courses

Funded by the Erasmus+ Programme of the European Union


(Project N°.: 2020-1-LT01-KA203-078070)

## 2.2. Cyprus

All the most prominent universities in Cyprus offer Bachelor and Master studies in computer science or cybersecurity area. The bachelor's degree in Cyprus universities is 240 ECTS credits and a master's degree between 90 to 120 ECTS credits. The study programmes are taught either in Greek or English languages.

*Table 2. Sample of HEI study programmes in the area of cybersecurity in Cyprus*

| **Title of the programme** | **Computer Science** | **Computer and Network Security** | **Cyber Warfare** | **Communications and Network Security** |
|---|---|---|---|---|
| **Type of the programme** | Study programme | Study programme | Study module | Study module |
| **Study field** | MSc in Computer Science | MSc in Computer Science | MSc in Cybersecurity | MSc in Cybersecurity |
| **Degree** | Master's degree | Master's degree | Master's degree | Master's degree |
| **Organising Institution** | University of Nicosia | Open University of Cyprus | University of Central Lancashire (UCLAN) | European University of Cyprus |
| **Language** | English | Greek | English | English |
| **Duration** | 90 ECTS | 90 ECTS | 10 ECTS | 7 ECTS |
| **Target group** | Bachelor's degree or an equivalent degree students | Bachelor's degree or an equivalent degree students | Bachelor's degree or an equivalent degree students | Bachelor's degree or an equivalent degree students |
| **Topics or modules** | • Cyber-physical systems and the Internet of Things;<br>• Cryptography and network security;<br>• Distributed system;<br>• **Cyberwarfare**;<br>• Ethical hacking;<br>• Project in cybersecurity;<br>• Network defence and countermeasures. | • Communication Networks<br>• Computer and Network Forensics<br>• Computer and Network Security<br>• Cryptography<br>• **Security Risk Management of Information and Communication Systems**<br>• Research Methods | • Fundamentals of Cyber Warfare;<br>• The legal status of cyber warfare and ethics ;<br>• Cyberspace battlefield - Weaponising malware (including Psychological Weapons: **social engineering,** SE tactics techniques and procedures, etc.);<br>• Cyberspace challenges and the Future of Cyber War. | • Refresh on fundamental networking principles and devices<br>• The network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats.<br>• Network attacks, including **phishing**.<br>• General protection, prevention and detection |



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


(Project N°.: 2020-1-LT01-KA203-078070)

None of the HEI study programmes in Cyprus teaches phishing or social engineering as a separate module. Instead, these subjects are incorporated in some course modules such as *Cyberwarfare, Communication and Network Security, Security Risk Management, Cybersecurity Risk Analysis and Management*, *etc.*

While some of the bachelor study programmes also include modules focused on soft skills (e.g., public speaking, psychology), most master's degree studies focus on developing students' hard skills, leaving soft skills behind.

*Table 3. Sample of training courses in the area of cybersecurity in Cyprus*

| **Title of the programme** | **Cybersecurity Awareness** | **Certified Secure Computer User (CSCU)** | **CompTIA Security+ Certification (SY0-601)** | **Applied Cybersecurity** |
|---|---|---|---|---|
| **Type of the programme** | Training course | Training course | Training course | Training course |
| **Study field** | Cybersecurity | Cybersecurity | Cybersecurity | Cybersecurity |
| **Degree** | Certificate | Certificate | Certificate | Certificate |
| **Organiser** | The University of Nicosia and Global training | AKTINA | New Horizons Computer Learning centre | Institute of Public, Cyber and National Security |
| **Language** | English | English | English | English |
| **Duration** | 2 hours | 14 hours | 5 days | 12 weeks (approx. 120 hours) |
| **Target group** | Entrepreneurs, managers, IT personnel, students, etc. | Computer users in general | (IT) professionals and students | IT and cybersecurity professionals and consultants |
| **Topics or modules** | Cybersecurity; **Social engineering/phishing**; Social media attacks, Fake warnings; Phishing emails; Malicious email attachments; Malicious software; Wi-Fi attacks; Passwords; Demonstration. | Securing operating systems; Malware and antivirus; Internet security; Security on social networking sites; Securing email communications, mobile devices, cloud and network connections; Data backup and disaster recovery. | **Threats, attacks, and vulnerabilities**; Architecture and design; Implementation; Operations and incident response. | Cybersecurity and cyber risk; Cyber risk trends, Hands-on experience; NIST cybersecurity framework; Tools and techniques in detecting **cyber-threats**; Creating enterprise threat risk assessments, compliance reports, and mitigation plans. |

Many public and private organisations offer cybersecurity training courses for IT professionals, students, employees, and the general public. The course duration varies from a couple of hours to several months. Depending on the certification provided, the participant has to take an exam to receive the certificate in some training courses.



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


(Project N°.: 2020-1-LT01-KA203-078070)

Most of the longer duration training courses include phishing and social engineering as separate objects. In contrast, short-duration training courses (around one day) mainly focus solely on phishing and social engineering.

Some of the training courses' costs are partly subsidised by Human Resource and Development authority in Cyprus (HRDA)[28] as a part of cybersecurity and digital skills strategies' actions and initiatives.

[28] Human Resource and Development authority in Cyprus (HRDA), UR http://www.hrdauth.org.cy/



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


(Project N°.: 2020-1-LT01-KA203-078070)

## 2.3. Estonia

The key higher education institutions offering study programmes in computer science or cybersecurity are Tallinn University of Technology and the University of Tartu. The bachelor's degree in Estonian universities is between 180 to 240 ECTS credits for bachelor's degree master's degree between 60 to 120 ECTS credits for a master's degree. The study programmes are taught in Estonian and English languages.

*Table 4. Sample of HEI study programmes in the area of cybersecurity in Estonia*

| **Title of the programme** | **Cybersecurity Engineering** | **Cybersecurity** | **Cryptography, specialisation of SECCLO Erasmus+** |
|---|---|---|---|
| **Type of the programme** | Study programme | Study programme | Study programme |
| **Study field** | BSc in Science Engineering | MSc in Science Engineering | MSc in Science Engineering |
| **Degree** | Bachelor's degree | Master's degree | Master's degree |
| **Organising Institution** | Tallinn University of Technology (TalTech) | Tallinn University of Technology (TalTech) and University of Tartu | University of Tartu |
| **Language** | English | English | English |
| **Duration** | 180 ECTS | 120 ECTS | 120 ECTS |
| **Target group** | Secondary school graduates | Bachelor's degree or an equivalent degree students | Bachelor's degree or an equivalent degree students |
| **Topics or modules** | Social, Professional and Ethical Aspects of IT; Electronics in IT; Logic and Discrete Mathematics; Communication Skills; IT Infrastructure Services; Linux and Windows administration; Fundamentals of networking; Introduction to Informatics and Computers; **Introduction to Cybersecurity**; Fundamentals of Programming; Web Technologies; Governance and Management of Cybersecurity; Database Basics; Computer Network Security; **Social Engineering;** Logging and Monitoring; Secure Programming. | Computer Programming; System Administration; Network Technology; Estonian Language and Culture; Entrepreneurship and Business Planning; **Human Aspects of Cybersecurity**; Legal Aspects of Cybersecurity; Cybersecurity Management; Cybersecurity Technologies; Cryptography; Cyber Incident Handling; Secure Software Design; Teamwork Project; Computer Network Security; Information Systems Attacks and Defence; Cybersecurity I and II; Special Topics of Cryptography; Mobile Phone Forensics; Strategic Communications and Cybersecurity; Data mining; Malware; Cyber Defence Monitoring Solutions; Privacy-preserving Technologies; Wireless Technologies and Security; Blockchain; Cryptology. | Cryptographic Protocols; Mathematical Foundations for Computer Science; Research Seminar in Cryptography; Cryptology II, Quantum Cryptography; Type Theory; Introduction to Coding Theory; Mobile Application Development – Projects, Methods in TCS; Special Assignment in Cryptography; Theoretical Informatics Project; Estonian for Beginners I; Master level seminar. |



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


(Project N°.: 2020-1-LT01-KA203-078070)

The analysed HEI study programmes in Estonia do not seem to teach phishing as a separate module. However, the phishing information may be incorporated in other course modules such as *Introduction to Cybersecurity, Computer Network Security* and others.

However, the Cybersecurity Engineering study programme offered by Tallinn University of Technology includes Social Engineering as a separate module. The module aims to provide students with basic knowledge of the nature of social manipulation (mainly in the context of ICT ) and its basic forms, techniques, and techniques (including hybrid attacks with a technological component) and protection against it. The module's duration is 3 ECTS credits.

The cybersecurity study programme offered by Tallinn University of Technology and the University of Tartu includes *Human Aspects of Cybersecurity*. The module aims to provide an overview of cybersecurity's human aspects, specifically the elements of social manipulation and protection mechanisms against them. The module's duration is 6 ECTS credits.

The study programmes include a wide range of specialised study modules, offering a good ratio between theoretical knowledge acquired and practical study. They also have course modules in softs skills, such as communication skills, entrepreneurship, psychology, etc.

*Table 5. Sample of training courses in the area of cybersecurity in Estonia*

| **Title of the programme** | **Web Application Security** | **Network Security Administrator** |
|---|---|---|
| **Type of the programme** | Training course | Training course |
| **Study field** | Ethical hacking/pentest | Network's security |
| **Degree** | Certificate | Certificate |
| **Organiser** | Clarified Security | NobleProg |
| **Language** | English | English |
| **Duration** | 4 days | 5 days |
| **Target group** | WebApp developers, maintainers, web server or hosting providers/administrators, information security specialists, etc. | System administrators and network administrators, anyone interested in defensive network security technologies. |



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

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. (Project N°.: 2020-1-LT01-KA203-078070)

| | | |
|---|---|---|
| **Topics or modules** | Client-Side attacks: (Security, Information sources, Client-Server communication, HTTP vs HTTPS, HTTP request methods, JavaScript and JavaScript injection, URL and URL manipulation, Cookies and cookie manipulation, Session and session hijacking, session fixation, Request forgery attacks (CSRF & OSRF), UI Redress Attacks, Using 3rd party content, Combined client-side attacks)<br>Server-Side attacks: (Authentication, passwords and hashes, Authorisation vulnerabilities, Business logic issues, Google hacking, Web server configuration and the file system, Command injection, File handling, File inclusion attacks, File upload, XXE (XML eXternal Entity) attacks, SQL injection) | Introduction to Network Security, Network Protocols, Security Policy, Physical Security, Network Attacks (Current Statistics, Defining Terms: Threats, Attack and Exploit, Classification of Hackers and Attacks, Spoofing; Spamming; Eaves Dropping; **Phishing;** War Dialing; Password Cracking, Web Page Defacement; SQL Injection; Wire Tapping; Buffer Overflow, WarDriving; War Chalking; War Flying Denial of Service (DOS) Attacks and Distributed DOS), Intrusion Detection System, Firewalls, Packet Filtering and Proxy Servers, Bastion Host and Honeypots, Hardening Routers, Hardening Operating Systems Security, Patch Management, Application Security, Web Security, Email Security; Encryption, Virtual Private Networks, WLAN, Creating Fault Tolerance, Incident Response, Disaster Recovery and Planning, Network Vulnerability Assessment |

There is a number of private (Clarified Security, NoblePro, Cyberexer, Rangeforce, CTF Pärnu, etc.) organisations offering training courses in various topics such as e-learning for cyber hygiene and data protection, vulnerability visualisation, risk assessment, cybersecurity, phishing, etc. The courses are mainly targeting IT professionals, companies and the general public interested in the topic. Depending on the certification provided, participants may have to take an exam to receive the certificate.

To help local businesses counter the cybersecurity threats, the Estonian Information System Authority has also launched an information campaign targeting small and medium-sized enterprises. The campaign focus on the types of cyber incidents that have incurred the most financial damage to companies in recent years[29].

[29] Cyber security campaign, URL https://itvaatlik.ee/



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


(Project N°.: 2020-1-LT01-KA203-078070)

## 2.4. Latvia

The key higher education institutions offering the study programmes in computer science or cybersecurity are Turiba University, Riga Technical University, Vidzeme University of applied science, BA School of Business and Finance. The bachelor's degree in Latvian universities is between 160 to 240 ECTS credits, and the master's degree is 120 ECTS credits. The study programmes are taught in Latvian and English languages.

*Table 6. Sample of HEI study programmes in the area of cybersecurity in Latvia*

| **Title of the programme** | **Computer Systems** | **Cybersecurity Engineering** | **Information Technologies** |
|---|---|---|---|
| **Type of the programme** | Study programme | Study programme | Study programme |
| **Study field** | BSc in Computer Systems | MSc in Cybersecurity Engineering | MSc in Information technologies |
| **Degree** | Bachelor's degree | Master's degree | Master's degree |
| **Organising Institution** | Turiba University | Riga Technical University | Vidzeme University of applied science |
| **Language** | Latvian and English | English | English |
| **Duration** | 240 ECTS | 120 ECTS | 120 ECTS |
| **Target group** | Secondary school graduates | Bachelor's degree or an equivalent degree students | Bachelor's degree or an equivalent degree students |
| **Topics or modules** | English and Latvian languages; Civil and Environmental Defence; Computer Architecture, Computer Engineering and Systems; Mathematics; Software Development Fundamentals; Design thinking; Economics and Entrepreneurship; Software Testing and Quality; Coding and Cryptography; **IT security and risk management**; Machine Learning and Intelligent Analytics; Software Project Management; Data Analysis and Benchmarking; Green/IT Systems and Methods; Introduction to Operations Research; Finance and Accounting; IT law and copyright; Robotics. | **Cybersecurity**; Reliability of Information Systems; Enterprise Information Technology Architecture; Control Fundamentals of Critical Infrastructures; Industrial Safety; **Network Security**; Software Security; Cryptography and Data Security Technologies; Design of Adaptive Systems; Engineering Systems Security; Sociotechnical Systems Modelling; Data Mining and Knowledge Discovery; Project Management; Secure E-Commerce Technologies; Data integration technologies; Social Responsibility and Business. | Ethical hacking; Reverse engineering; Network, mobile and cloud security; Digital forensics; Secure software design; Incident handling and response; System security engineering; Project management; Strategic ICT management; Data mining; Communication; Critical thinking; Social media analysis workshop; **Internet psychology**; Rights, obligations and liability of actors on the internet; Law of data security and investigation; Cybersecurity policy; Information system audits and assurance; **Information security risk management**; Security culture; Cryptography; Innovation and creative problem-solving. |



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


(Project N°.: 2020-1-LT01-KA203-078070)

The analysed HEI study programmes in Latvia do not teach phishing or social engineering as separate modules. However, the information about these topics may be incorporated in other course modules such as *IT security and risk management, Network Security, Cybersecurity and Information security risk management, Internet psychology, etc*.

Like in Estonia, the study programmes offered seem to be broad-based and practically oriented, include the course modules in softs skills, such as communication skills, entrepreneurship, creative problem solving, etc.

*Table 7. Sample of training courses in the area of cybersecurity in Latvia*

| **Title of the programme** | **ESET Remote Cyber Security Knowledge** | **IT security training for users** | **"Kiberdrošība"** |
|---|---|---|---|
| **Type of the programme** | Training course | Training course | Training course |
| **Study field** | Network's security | Cybersecurity | Cybersecurity |
| **Degree** | Certificate | Certificate | Certificate |
| **Organiser** | ESET Latvia | Cybersecurity Academy | "Dialogs AB" Learning centre |
| **Language** | Latvian and English | Latvian, English, Russian | Latvian |
| **Duration** | 2 hours | 4 hours | 1 week (42 hours) |
| **Target group** | Companies and their employees | Business Managers, IT security managers, companies, and the general public | Business leaders, information technology developers, the general public. |
| **Topics or modules** | Threat overview (Types of malware, fraud principles and **social engineering**); Password theory; Working remotely; Security everywhere; **Anti-phishing**; Email security (spam, **phishing** and simple scammers); Application management. | Why is it important to be aware of IT security threats; Knowing your enemy; Physical security; Securing password; **Social engineering; Phishing**; **SMSishing; Vishing**; Security of personal data | Operation and role of information technology; Information resources and their role; **information security threats**, their types and impact; Information security management tools and methods; Importance of cybersecurity documentation. |

Based on the research done, several organisations offer cybersecurity training to companies, IT professionals, and the general public. While the shorter duration training courses tend to focus solely on different types of threats, including phishing, social engineering, and ways to protect oneself, longer duration training courses provide a broader perspective on cybersecurity. The training providers primarily target business managers, general employees, IT professionals, and the general public interested.



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

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. (Project N°.: 2020-1-LT01-KA203-078070)

Since 2018 information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV) has been implementing an action called "Improving Cybersecurity Capacities in Latvia". During the campaign, CERT.LV has developed an informative guidebook and videos, organised a Cybersecurity conference, and launched a website[30] containing cybersecurity resources at the workplace.

Latvian Safer Internet Centre[31] also offers free online webinars for students about safety on the Internet. In contrast, Latvian Local Government Training Center offers courses for adults about the safe use of the Internet and social media.

[30] Cyber Security campaign, URL https://www.esidross.lv/
[31] Latvian Safer Internet Centre, URL https://drossinternets.lv/lv/nodarbibas



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


(Project N°.: 2020-1-LT01-KA203-078070)

## 2.5. Lithuania

Most universities and colleges in Lithuania offer Bachelor and Master studies in computer science or cybersecurity area. The bachelor's degree in Lithuanian HEI is between 180 to 240 ECTS credits and master's degree is between 90 to 120 ECTS credits. The study programmes are taught in Lithuanian and English languages.

*Table 8. Sample of HEI study programmes in the area of cybersecurity in Lithuania*

| **Title of the programme** | **Information Systems and Cybersecurity** | **Information and Information Technologies Security** | **Cybersecurity Management** |
|---|---|---|---|
| **Type of the programme** | Study programme | Study programme | Study programme |
| **Study field** | BSc in Computing | MSc in Cybersecurity Engineering | MSc in Business management |
| **Degree** | Bachelor's degree | Master's degree | Master's degree |
| **Organising Institution** | Vilnius University | "Vilnius Gediminas Technical University | Mykolas Romeris University |
| **Language** | Lithuanian and English | English | Lithuanian and English |
| **Duration** | 210 ECTS | 120 ECTS | 90 ECTS |
| **Target group** | Secondary school graduates | Bachelor's degree or an equivalent degree students | Bachelor's degree or an equivalent degree students |
| **Topics or modules** | Algorithm Theory and Data Structures; Mathematics; Legal Regulations for Cybersecurity; Introduction to Programming; Information Systems and Databases; Digital Forensics; Operational Systems and their Security; Programming Languages; WWW Development Technologies; Creation of Information Systems; E-Transactions and their Security; Ethical Hackings; **Information Security and Risk Management**; **Computer Networks and their Security**; Data Security and Cryptography; Design Computer Infrastructures; Virtual Systems; Data Mining; Information Systems Testing and Quality Assurance; Forensic Analysis of Digital Content and Analysis of Malware. | Information Technology Security Methods; Databases and Electronic Document Security; Cryptographic Systems; Fundamentals of Scientific Research and Innovations; Computer Networks and Operating System Security; Virtual Infrastructure and Cloud Computing Security; Ethical Hacking Techniques; Cyber Forensics; **Information Security Management**; Secure Programming**.** | The studies cover system and network security methods, cryptography, ethical intrusion technologies, cybercrime investigation, information security management and other specific course units.<br>Compulsory courses: Decisions of E-governance and E-Democracy; Legal Environment of Cybersecurity; Management of Cyber-security; Public Relations Strategy; **Privacy and Data Protection**; Security Economics; Intellectual Property; Management of IT Project; Modelling of Electronic Information Security. |



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


(Project N°.: 2020-1-LT01-KA203-078070)

The analysed HEI study programmes in Lithuania do not teach phishing or social engineering as separate modules. However, the information about these topics may be incorporated in other course modules such as *Cybersecurity, Information Security and Risk Management; Computer Networks and their Security; Privacy and Data Protection, etc.*

Contrary to study programmes offered in Latvia and Estonia, both bachelor and master studies in Lithuania seem to be focused on mainly developing students' hard skills, putting less emphasis on the importance of soft skills.

*Table 9. Sample of training courses in the area of cybersecurity in Lithuania*

| **Title of the programme** | **ESET Remote Cybersecurity Knowledge Training** | **IT security awareness training** | **The Basics of Cybersecurity for Consumers** |
|---|---|---|---|
| **Type of the programme** | Training course | Training course | Training course |
| **Study field** | Cybersecurity | Cybersecurity | Cybersecurity |
| **Degree** | Certificate | Certificate | Certificate |
| **Organiser** | ESET | UAB "Hermitage Solutions" | Vilnius University |
| **Language** | Lithuanian | Lithuanian | Lithuanian |
| **Duration** | 2 hours | 6 hours | 8 hours |
| **Target group** | Companies and employees | Business Managers, IT security managers, companies, employees, and the general | General public |
| **Topics or modules** | **Phishing**, Remote Work; Connecting to a corporate network; Preventive measures; Threat overview; Password policy; Internet security; Internet of Things; El. email protection; Practical advice | Why is IT security literacy important to everyone; Recognition of the threat; Physical data protection; Passwords; **Social engineering; Phishing**; Mobile data protection; Protection of personal data. | Principles of personal data security; strong passwords; social networking activities; Principles of Wi-Fi usage; **Social engineering** (the most popular attacks on social engineering; how to recognise social engineering attacks; security measures). |

Several public and private organisations offer cybersecurity training courses for IT professionals, companies, employees, and the general public. There are also several organisations organising tailor-made courses in the area of cybersecurity targeting companies and their employees. The courses include phishing and social engineering topics, and their duration varies from a couple of hours to several days.



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


(Project N°.: 2020-1-LT01-KA203-078070)

In 2020, the "Create Lithuania" team in cooperation with the Ministry of National Defence and National Cybersecurity Centre, conducted research and released a guidebook " Cyber Security and Business. What every company manager should know[32]". The guidebook discusses the importance of cybersecurity and provides practical advice on assessing the risks of threats and recommendations on managing potential cyber incidents, etc.

[32] Create Lithuania (2020): “Cyber Security and Business. What every company manager should know”, UR https://www.enterpriselithuania.com/naujienos/isleistas-leidinys-kibernetinis-saugumas-ir-verslas-ka-turetu-zinoti-kiekvienas-imones-vadovas/ (accessed 17/03/2021)



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


(Project N°.: 2020-1-LT01-KA203-078070)

## 2.6. Malta

The key higher education institutions offering study programmes in computer science or cybersecurity are the University of Malta (UoM) and the Malta College of Arts, Science and Technology (MCAST). The bachelor's degree in Maltese universities is between 180 to 240 ECTS credits for a bachelor's degree and between 60 to 120 ECTS credits for a master's degree. The study programmes are taught in the English language.

*Table 10. Sample of HEI study programmes in the area of cybersecurity in Malta*

| **Title of the programme** | **Science in Information Technology** | **Information and Information Technologies Security** | **Information Technology and Systems** |
|---|---|---|---|
| **Type of the programme** | Study programme | Study programme | Study programme |
| **Study field** | BSc in Cybersecurity | MSc in Cybersecurity Engineering | MSc in Information Technology and Systems |
| **Degree** | Bachelor's degree | Master's degree | Master's degree |
| **Organising Institution** | STC Higher Education | American University of Malta | Malta College of Arts, Science and Technology |
| **Language** | English | English | English |
| **Duration** | 180 ECTS | 96 ECTS | 90 ECTS |
| **Target group** | Secondary school graduates | Bachelor's degree or an equivalent degree students | Bachelor's degree or an equivalent degree students |
| **Topics or modules** | Skills for Computing; Computer Systems; Computer Networks; Databases; Designing & Developing a Website; Software Development Techniques; Designing & Developing Object-Oriented Programs; Office Solutions Development; **Cybersecurity Architecture and Operations**; Computer Networking; Network Security; Ethical Hacking; Object-Oriented Design and Programming; Data Mining; Advanced Networks; Digital Forensic Risk and **Cybersecurity Management**; Systems Architecture and Internet of Things; Project and Professionalism with Cybersecurity artefact; Cyber Intelligence. | Information Technology Security Methods; Databases and Electronic Document Security; Cryptographic Systems; Fundamentals of Scientific Research and Innovations; Computer Networks and Operating System Security; Virtual Infrastructure and Cloud Computing Security; Ethical Hacking Techniques; Cyber Forensics; **Information Security Management**; Secure Programming**.** | Information Systems and Management; Operating Systems and Cloud Computing; Network Protocols and Network Automation; Data Science and Predictive Analysis; **Foundations of Cybersecurity**; Web Technologies and Secure E-Commerce; Mobile Computing and 5G Networking; Internet of Things (IoT); Financial Computing and Cryptocurrencies; **Entrepreneurship and Innovation Management.** |



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


(Project N°.: 2020-1-LT01-KA203-078070)

As in other analysed countries (except Estonia), Malta's HEI study programmes do not offer phishing or social engineering as a separate module. However, the information about these topics may be incorporated in other course modules such as *Cybersecurity management, Cybersecurity Architecture and Operations, Information Security Management, Foundations of Cybersecurity, Security and Information Assurance*, etc.

The majority of the study programmes are focused on hard skills development. Out of all study, programmes analysed, only Malta College of Arts, Science and Technology and the University of Malta offer study modules focusing on soft skills, such as *Entrepreneurship and Innovation Management, Entrepreneurship: Start-up your Innovative Business, Project management etc.*

*Table 11. Sample of training courses in the area of cybersecurity in Malta*

| **Title of the programme** | **Ethical Hacking Course** | **The Certified Information Systems Security Professional (CISSP** | **Information & Cybersecurity Practitioner** |
|---|---|---|---|
| **Type of the programme** | Training course | Training course | Training course |
| **Study field** | Cybersecurity | Information Systems | Cybersecurity |
| **Degree** | Certificate | Certificate | Certificate |
| **Organiser** | ICE Malta | Cybersecurity Malta | Lead training |
| **Language** | English | English | English |
| **Duration** | 24 hours | 5 days | 12 days/ 6 ECTS credits |
| **Target group** | Students and the general public | IT security-related practitioners, auditors, consultants, investigators, or instructors. | Managers, Information Security and IT Professionals, Compliance Officers, Accountants, etc. |
| **Topics or modules** | Introduction to Ethical Hacking; Networking Foundations; Footprinting and Reconnaissance; Scanning; Passwords; Sniffing; **Social Engineering**; Cryptography; Hacking Wireless Systems | Security and Risk Management; Asset Security; Security Engineering; Communication and Network Security; Identity and Access Management; **Security incidents** – Preparing, responding and recovering; Security Assessment and Testing; Security Operations; Software Development Security. | Foundations of Information Security, **Cyber Assessments & Incident Response**, Information Systems Auditing and Management |

Several public and private organisations offer cybersecurity training courses for IT professionals, security-related practitioners, companies, employees, students, and the general public. There is also a number of private organisations offering tailor-made courses in cybersecurity and penetration and social engineering testing services. Most of the examined training courses provide a broader perspective on cybersecurity instead of focusing only on phishing or social engineering topics.



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


(Project N°.: 2020-1-LT01-KA203-078070)

In 2018, the National Cybersecurity Awareness and Educational Campaign in Malta was launched. The campaign aimed to raise awareness of how digital security can be improved by emphasising the need for longer passwords, characteristics and change them regularly, increasing cautiousness on providing personal data and purchasing. The campaign also aimed to educate people on identifying spam emails, responsible use of social media and the phenomenon of phishing.

Furthermore, in collaboration with the Parliamentary Secretary for Financial Services and Digital Economic and Innovation, the same year Malta Information Technology Agency has launched a new scheme to promote and strengthen cybersecurity preparedness in the private sector. The scheme helps the private sector to assess their digital assets' posture against cybersecurity threats and provides training to employees[33].

The Malta's BeSmartOnline![34] project aims to raise awareness and educate children, youth and their support network, such as carers, parents and educators, on the safe use of the internet by establishing, operating and promoting reporting facilities for internet abuse.

[33] B-SECURE Scheme, URL https://cybersecurity.gov.mt/bsecure/#1569427288152-9f8f5200-6588
[34] BeSmartOnline! project, URL https://www.besmartonline.org.mt/



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


(Project N°.: 2020-1-LT01-KA203-078070)

# 3. SUMMARY AND MAIN FINDINGS

- The cybersecurity skills shortage has affected 74 % of organisations worldwide. 57% of organisations had unfilled cybersecurity vacancies in 2019. The time needed to fill in these positions usually was three months.
- The most critical skills shortages include cloud computing security (33%), application security (32%), and security analysis and investigations (30%).
- One of the main reasons indicated by respondents to the positions remain unfilled is the lack of qualified applicants. Almost one-third of organisations claimed that almost 75% of candidates did not possess the right qualifications for the job. The most significant skills gaps indicated by respondents were lack of soft skills, IT knowledge, insufficient business insight, cybersecurity technical experience and practical experience.
- In 2020, the estimated global shortage of cybersecurity workforce was around 3.12 million professionals. In contrast, in Europe alone, the cybersecurity workforce gap is estimated to be 350 000 workers by 2022. This number has doubled from what was estimated in 2018.
- ENISA, in their "Cybersecurity skills development in the EU "report, has identified four leading causes that might be attributed to the cybersecurity skills shortage. Two of them are focused on workplace issues, while the remaining two are associated with issues in the education and training system.
- In 2013, the European Commission published its first cybersecurity strategy, highlighting awareness-raising and skills development as key strategic objectives. Since 2017, all EU Member States have developed and published their national cybersecurity strategies (NCSS).
- One of the key targets in national security strategies' of all project partner countries is the enhancement of cyber education and awareness by targeting academia, the public and private sector and the general public.
- The national security strategies in all project partner countries also emphasise public, private, and academic partnerships to strengthen cybersecurity systems' resilience, investments in ICT security, personnel training, and the development of students' cybersecurity skills to meet market needs.
- The analysis of HEI study programmes in all project partner countries except Estonia does not include phishing and social engineering topics as separate modules. However, the information about these topics may be incorporated in other course modules. 2 HEI study programmes in Estonia include study modules focused on social engineering. The average duration of such modules is 4,5 ECTS.

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

- The analysed HEI study programmes in Estonia, Latvia and Malta, include course modules in softs skills, such as communication skills, entrepreneurship, psychology, etc. Contrary, HEI study programmes in Cyprus and Lithuania are mainly focused on hard skills, putting less emphasis on the importance of soft skills.

- In all partner countries, there are a number of public and private organisations offering training courses in cybersecurity targeting Cybersecurity and IT professionals, companies, employees, and the general public. While the shorter duration training courses tend to focus solely on different types of threats, including phishing, social engineering, and ways to protect oneself, longer duration training courses provide a broader perspective on cybersecurity. There are also a number of organisations offering penetration and social engineering test targeting companies and their employees.



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

# 4. BIBLIOGRAPHY


1. (ISC)2 (2019): (ISC)² Study Reveals the Cybersecurity Workforce Has Grown to 3.5 Million Professionals Globally, URL https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/11/11/ISC2-Study-Reveals-the-Cybersecurity-Workforce-Has-Grown-Globally
2. (ISC)2 (2019): Cybersecurity workforce study, URL https://www.isc2.org/Research/Workforce-Study
3. Cyber Wiser (2021): Education and training in national cybersecurity strategy (LT), URL https://www.cyberwiser.eu/lithuania-lt
4. Cyber Wiser (2021): Education and training in national cybersecurity strategy (MT), URL https://www.cyberwiser.eu/malta-mt
5. Cyber Wiser (2021): Education and training in national cybersecurity strategy (LV), URL https://www.cyberwiser.eu/latvia-lv
6. Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy
7. ENISA, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Latvia
8. European Commission (2013): Cybersecurity Strategy of the European Union, URL https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
9. European Commission (2019): Four EU pilot projects launched to prepare the European Cybersecurity Competence Network, URL https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network
10. European Commission (2020): Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2027, URL https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu75-billion-funding-2021-2027
11. European Union Agency for Cybersecurity (2019): Cybersecurity skills development in the EU
12. European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
13. Government of the Republic Of Lithuania (2018): Resolution on the approval of the national cybersecurity strategy, URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf
14. ISACA (2020): State of Cybersecurity 2020 Part 1: Global Update on Workforce Efforts and Resources, URL https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf
15. Jon Oltsik (2019): The Life and Times of Cybersecurity Professionals 2018, URL https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/surveys/esg-issa-2018-survey-results.pdf
16. Latvian Defence Ministry (2019): Latvia approves new Cyber Security Strategy 2019-2022, URL; https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
17. Latvian Defence Ministry (2019): Latvia's cybersecurity strategy for 2019 – 2022, URL https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
18. OCECPR (2012): Cybersecurity Strategy of the Republic of Cyprus, URL https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus
19. The Republic of Estonia, Ministry of Economic Affairs and Communication (2019): Cybersecurity Strategy, URL https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
20. The Malta Information Technology Agency (2016): Malta Cyber Security strategy 2016, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Malta




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