Micro - Entreprise Cybersecurity

MECyS

Overview of Vocational Education & Training

2nd Part of Training Plan

Co-funded by the European Union

Point of Contact	Bettina Schneider
Institution	Fachhochschule Nordwestschweiz (FHNW)
E-mail	bettina.schneider@fhnw.ch
Phone	+41 61 279 17 54

Project Acronym	MECyS
Project Title	Microenterprise Cybersecurity
Funding	Erasmus+/Movetia
Project start date	31/12/2022
Dissemination level	Public
Date of submission	30/06/2023
Lead partner	FHNW
Contributing partners	FHNW, PHF, A.B.IED, CESUR, ANEMO, STHEV
Main Authors	Bettina Schneider (FHNW), Ilya Misyura (FHNW), Natalie Jonkers (FHNW)

Revision History

Version	Date	Author	Comment
0.1	22/02/23	Bettina Schneider, Ilya Misyura FHNW	Initial version of report
0.2	02/03/23	Natalie Jonkers FHNW	Fill existing trainings for Switzerland
0.3	03/03/23	Bettina Schneider	Write draft for first section
0.4	07/03/23	Bettina Schneider	Amend structure based on discussions during kick-off at PHF Freiburg
0.5	14/03/23	Jessica Peichl, Bettina Schneider	Review of v0.4

Contents

List of tables

No table of figures entries found.

List of figures

No table of figures entries found.

1 Purpose and Approach of this Report

The purpose of the overall training report is the identification and compilation of the different general and national conditions concerning business related information and data security training particularly for IT-lay persons. These conditions include the specification of common and divergent learning goals and salient training systems and policies. Vocational training and further education differ significantly between the participating countries, whereas in Germany and Switzerland there are dual vocational educations systems that are organisationally clearly distinct from further education.

As main approach to collect the information, the following inputs will be used and/or following methods applied:

- national reports and expert inputs on the state of cybersecurity and data protection within vocational and business-related training and teaching/training tools
- literature review and focus group interviews in concern of general and target group specific learning hurdles

The training report will consist of three parts:

1. Cybersecurity and privacy in vocational education and training (VET);
2. Insights into specific learning hurdles;
3. Best practices concerning learning tools and methods.

This document is reflecting the part 1.

The insights gained in this report will used in the following work packages. They build on the analysis of the specific conditions and discussions with the target groups on usage scenarios and learning barriers. The report will serve as comprehensive overview to be published on the project website and disseminated to interested stakeholders.

2 Cyprus

2.1 Ecosystem for Vocational Education and Training (VET)

The vocational education and training (VET) system in Cyprus is continuously evolving to meet the demands of the labor market. VET is available at both secondary and tertiary education levels. At the upper secondary level, students can choose between general education programs offered by lyceums and VET programs provided by technical schools. Technical schools offer theoretical and practical 3-year programs, leading to school-leaving certificates equivalent to secondary general education. These programs combine general education subjects with VET subjects and include practical training in enterprises. Apprenticeships are also available for young people aged 14 to 18. The apprenticeship system consists of a preparatory phase lasting up to two years and a core apprenticeship phase lasting three years. Successful completion of core apprenticeship allows participants to continue with evening technical school programs or enter upper secondary programs.

VET at the tertiary level is provided by public and private institutes/colleges, offering accredited programs that can last from two to three years. Completion of these programs leads to a diploma or higher diploma (EQF 5). Vocational training for adults is widely accessible in Cyprus, catering to the employed, unemployed, vulnerable groups, and adults in general. Various public and private providers offer training programs tailored to specific needs. The HRDA provides subsidies through different schemes to support training for both the employed and unemployed.

The main players are:

The Ministry of Education, Culture, Sport and Youth oversees education policy, while the Ministry of Labour, Welfare and Social Insurance handles labor and social policy. The Human Resource Development Authority of Cyprus (HRDA) plays a vital role in vocational training.

The majority of vocational education and training (VET) in Cyprus is provided by public institutions. Secondary VET, which includes evening technical schools and the apprenticeship system, as well as public higher (tertiary/non-university) VET, are offered at no cost to the students. However, certain adult vocational programs may have a nominal fee associated with them.

Specifics and challenges of Cyprus:

Cyprus has a strong emphasis on general secondary education followed by higher education, reflecting a cultural preference for these paths. However, the economic crisis experienced during 2012-2015, coupled with efforts to enhance the appeal of vocational education and training (VET), has led to an increase in enrolments in upper secondary VET programs by 4 percentage points from 2011 to 2017. To address this shift, training initiatives have been redirected to primarily target the unemployed, economically inactive individuals, and the employed population.

One of the significant challenges faced is tackling youth and long-term unemployment. Various measures have been implemented to improve the employability of young people and the long-term unemployed, including personalized guidance, training opportunities, and work placements.

Another challenge lies in promoting adult participation in lifelong learning, as the current rate stands at 4.7% (with a national target of 12% by 2020). Additionally, there is a focus on increasing VET participation among young individuals, which was at 16.9% in upper secondary level in 2019. Key measures to address these challenges include promoting tertiary non-university VET programs, enhancing the curricula of secondary technical and vocational education, and improving the skills and competences of VET teaching staff. Furthermore, there are ongoing efforts, outlined in the 2015-20 strategic plan for technical and vocational education, to upgrade apprenticeship programs and make them more attractive to young people.

2.2 VET Offerings in Cybersecurity and Data Protection

Cyprus recognizes the importance of cybersecurity and data protection in today's digital age. Given the increasing global demand for cybersecurity professionals and the need to protect sensitive data, VET institutions in Cyprus offer courses or programs related to cybersecurity and data protection. In terms of education and training, various institutions in Cyprus provide courses, workshops, and certifications related to cybersecurity and data protection. These offerings aim to enhance the skills and knowledge of professionals in the field and raise awareness among individuals and organizations.

The Cyprus Productivity Center (Miistry of Labour & Social Insurance) has an important role in a national level in Cyprus, as a vocational training provider. Its core mission entails the advancement of management development, training, and productivity, while ensuring the efficient utilization of human and capital resources and fostering an enhanced quality of life within the EU. The Prodictivity Center through the e-gnosis platform (https://www.e-gnosis.gov.cy/training/) offers courses and trainings including training on digital skills.

In addition, the Cyprus Certification Company (CCC) operates a training center approved by the relevant government body (the Human Resource Development Authority - HRDA) and provides training in relevant to its services subjects, and also in specialized areas as those arise from the industry's needs, including cybersecurity and data protection.

There is an important number of IT-related bachelor's and master's degree courses available at both public and private universities (approximately 10 HEIs in Cyprus), such as:

- University of Central Lancashire UCLan Cyprus, MSc Cybersecurity
- Open University of Cyprus, MSc Computer and Network Security
- University of Nicosia MSc Computer Science – Concentrations: 1. Cyber Security, 2. Mobile Systems, 3. Blockchain Technologies

Additional to the formal programmes provided by public and private universities, private training centers, such as KPMG Academy Cyprus and PwC Academy Cyprus, offer specialized cybersecurity training programs and certifications for professionals.

2.3 Summary and Intermediate Conclusions

In summary, Cyprus has a well-developed VET system that includes secondary and tertiary education pathways, apprenticeships, and vocational training for adults. These initiatives aim to meet the demands of the labor market and enhance individuals' employability through the acquisition of practical skills and qualifications. VET in Cyprus provides a pathway for individuals to acquire practical skills and qualifications for the labor market. Efforts have been made to increase the attractiveness of VET and address unemployment challenges. In order to meet the evolving needs of the labor market, it is essential to promote and enhance VET participation, improve apprenticeship programs, and enhance the competences of VET teaching staff. Additionally, there is a pressing need to address the growing demand for skilled cybersecurity professionals by continuously adapting and updating VET programs to effectively tackle the ever-changing cybersecurity challenges.

3 France

3.1 Ecosystem for Vocational Education and Training (VET)

France has been seen as a country that invest in the education of its citizen with a lifelong learning system promoted by the State as vocational qualifications that can be acquired. This lifelong learning system caters for the under-18 low-qualified and promotes adult learning by having a regulatory and financial national policy. Another key aspect is the role per regions in France where they implement territorial continuing training and career guidance schemes.

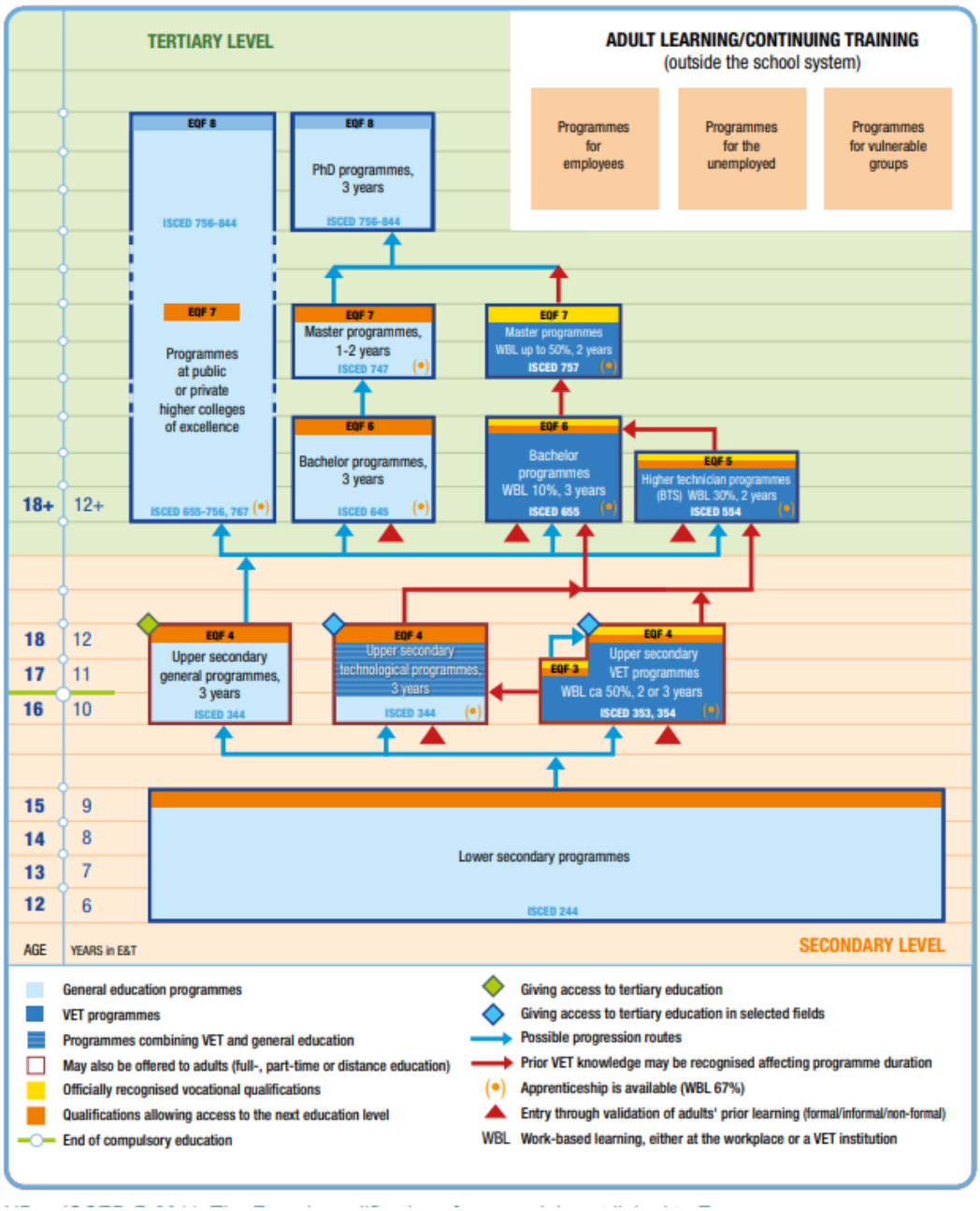
Having into account the resources of VET in France from CEDEFOP "European Centre for the Development of Vocational Training" Vocational education and training in France: short description (europa.eu) , the primary goal of the French educational system is to equip individuals with relevant skills for personal and professional growth while promoting social integration among young people and adults. Vocational education and training (VET) play a significant role, with approximately one-third of learners in upper secondary schools pursuing vocational paths. This approach includes personalized support, enhanced career guidance, and a diverse range of VET diploma specializations across various sectors of the economy.

To provide an alternative to traditional school-based education, apprenticeship training centers offer young people up to the age of 29 the opportunity to combine learning with work, enabling them to gain qualifications and employment. Private organizations and businesses can establish their apprenticeship centers, focusing on in-demand skills within their respective sectors. This is also advantageous for people from 20 to 26 years old in which the government provides the option to do the same learning and working process with more hours at the education center.

The promotion of excellence in VET extends to emerging sectors through the implementation of trades and qualification campuses. Additionally, the state has a formal obligation to provide training opportunities to individuals aged 16 to 18 who are low-qualified and not engaged in education. Efforts are made to enhance their employability through apprenticeships, continuing training, civic service-learning schemes, and support for social and professional integration.

In France, the responsibility for vocational training is shared among the State, regional authorities, and representatives from the business sector. The management of initial vocational education and continuing vocational training is divided between various ministries, each tasked with developing nationally recognized vocational qualifications and certificates. Qualifying criteria are in place for VET teachers and trainers, and funding sources and schemes vary depending on the nature of the training initiatives and the specific group of learners being targeted.

At the national level, the Ministry of National Education, Youth and Sports oversees upper secondary vocational education and training (VET), while the Ministry of Higher Education, Research and Innovation is responsible for tertiary VET. Other ministries, such as those in charge of social affairs, agriculture, culture, defence, finance, and health, handle VET qualifications and programs relevant to their respective domains. These ministries collaborate with representatives from the business sector to establish standards for VET qualifications, define examination regulations, and issue and award VET diplomas and qualifications. Additionally, they offer school-based VET programs, recruit and train VET teachers, and monitor the quality of training, outcomes, and resources.



Source: Cedefop and ReferNet France, 2021

3.2 VET Offerings in Cybersecurity and Data Protection

In France, Vocational Education and training plays a crucial role in equipping individuals with the skills and knowledge needed for a successful career in various industries. The VET system in France is known for its comprehensive and well-structured approach, offering a wide range of training programs to meet the diverse needs of learners.

The VET ecosystem for cybersecurity involves multiple stakeholders. Government bodies, such as the Ministry of Education and the Ministry of Higher Education, Research, and Innovation, provide guidance and set standards for cybersecurity training programs. They collaborate with industry experts and professional associations to ensure that the curricula align with industry needs and best practices.

Among the trainings regulated by the French federation of cybersecurity:

- The Fédération de la Cybersécurité Française (French Federation of Cybersecurity) offers a wide range of training programs and initiatives to enhance cybersecurity skills and promote best practices in France. The federation offers certified training courses in various cybersecurity domains, including ethical hacking, incident response, secure coding, network security, and data protection. These courses are designed to provide participants with practical skills and knowledge through hands-on exercises and real-world scenarios.
- Agence nationale de la sécurité des systèmes d'information (ANSSI), the French National Agency for the Security of Information Systems, provides training courses and workshops on cybersecurity for individuals, professionals, and organizations. Their programs cover topics like secure coding, cryptography, incident response, and risk management.

Private training providers and cybersecurity firms also contribute to the VET landscape in France. They offer specialized courses, workshops, and boot camps that focus on specific cybersecurity domains or skillsets. These programs provide opportunities for individuals to enhance their knowledge and gain industry-recognized certifications:

- Guardia cybersecurity school offers a range of comprehensive training programs and services to prepare individuals for successful careers in the field of cybersecurity.
- Aston école offers a Master program in digital security expert.
- 2600 Ecole de cybersécurité offers a range of certifications designed to equip individuals with the necessary skills and knowledge in the field of cybersecurity.

In addition to formal vocational education and training (VET) approaches, there are also informal VET approaches that provide valuable learning opportunities in France. These informal approaches often complement formal training and offer practical experiences and hands-on skills development. Online Learning Platforms: Various online platforms offer cybersecurity courses, tutorials, and resources that individuals can access at their own pace. These platforms provide flexibility and convenience for individuals seeking to acquire cybersecurity skills and knowledge outside of formal education settings:

- Root-Me: provides a virtual environment where users can test their skills in a safe and legal way, and learn from their mistakes. The platform also offers tutorials and explanations for each challenge to help users improve their knowledge and understanding of cybersecurity.
- Hackademics: is an online learning platform that provides cybersecurity training and courses. It offers a range of educational resources, including interactive lessons, practical exercises, and assessments, to help individuals develop their skills and knowledge in cybersecurity.

3.3 Summary and Intermediate Conclusions

When examining the specifics of the vocational education and training (VET) ecosystem in cybersecurity in France, several notable aspects stand out. Firstly, the emphasis on professional certifications. These certifications provide individuals with a clear pathway to acquire the necessary expertise and demonstrate their proficiency in cybersecurity. Additionally, the presence of specialized cybersecurity schools like Guardia offers targeted and focused training programs.

One aspect is the need for accessible training. It is important to ensure that cybersecurity VET programs are accessible and affordable to a wider range of learners, including individuals from diverse backgrounds. This can be achieved through initiatives that provide financial support, scholarships, or flexible learning options, making the training more inclusive and reaching a broader audience. Another key area for improvement is industry collaboration. Strengthening collaboration between VET providers and industry stakeholders is vital to ensure that training programs align with current industry needs and technological advancements.

In conclusion, the vocational education and training (VET) ecosystem in cybersecurity in France showcases a wide range of options and opportunities for individuals interested in pursuing careers in this field. The emphasis on professional certifications highlights the industry's focus on recognized and standardized skills. This ensures that learners gain the necessary competencies to thrive in the cybersecurity domain.

4 Germany

4.1 Ecosystem for Vocational Education and Training (VET)

At the core of the German vocational education system is the dual approach, that is considered widely as the backbone of the high-quality work force in Germany.

The dual system has a long history, partially dating back to guilds. Despite its integration of a wide range of stakeholders, it proves to be very adaptive to the changing requirements of modern labour markets. The system integrates on its different levels councils with representatives from chambers of commerce and crafts as well as in some forms also from unions. Usually for three years apprentices are educated both at public schools and in companies, i.e. typically at different days during the week. Apprentices, potentially starting after 9th or 10th grade, are paid by their companies, which makes is an attractive career path also in comparison to academic education. On the opposite, it is attractive for many companies to have apprentices, first to have a kind of cheap labour, as well as well second well trained staff in the future. However, companies that want to have apprentices need to provide staff with proven training competences. These are e.g. part of the curricula for Master of Crafts (Meister).

Whereas education is usually regulated at state level in Germany, vocational education is regulated on a federal level. The Bundesinstitut fürBerufsbildung (BiBB - Federal Institute of Vocational Education) is responsible for defining the standards of more than 300 vocations (https://www.bibb.de/dienst/publikationen/de/17944).

In addition to the dual system there are educational pathways leading to similar degrees as the dual system solely based on courses at vocational schools. There are also formal one- and two-year courses on top of the dual vocational courses (Aufstiegsfortbildung) leading to degrees equivalent to Master of Crafts, like e.g. state-certified technician for informatics (Staatlich geprüfter Techniker für Informatik - https://web.arbeitsagentur.de/berufenet/beruf/58471#ueberblick), which includes IT-Security Management in its curriculum.

Academic pathways, requiring 11 or 12 years of school (or other forms of university entrance diplomas, like a dual vocational education), can also lead to specific vocations. Apart from universities of applied sciences and other specialized universities there are also at Cooperative State Universities that have dual study courses, typically leading to a bachelor's degree.

Within the German Quality Framework (https://www.dqr.de/dqr/en/home/home_node.html) a dual vocational education has the same level a university entrance diploma (Abitur); a Master of Crafts (Meister) is equivalent to bachelor. The German and the European Quality Framework both have 8 Levels, which can be seen rather in parallel.

4.2 VET Offerings in Cybersecurity and Data Protection

At vocational schools, classes for specific subjects will be mixed with students from different vocations in so far these subjects are part of their course structure. Teachers for vocational specific subjects will usually have a practical background in this vocation (general education subjects are usually taught by teachers from university).

Among the currently 324 vocations regulated by the Federal Institute of Vocational Education there are also IT-based vocations. If these vocations are present at a certain school, the students might share the same classes:

- Elektroniker für Informations- und Systemtechnik / Electronics technician for information and systems technology

- Fachangestellter für Medien- und Informationsdienste / Specialist for media and information services
- IT-System-Elektroniker / IT systems electronics technician
- Kaufmann für Digitalisierungsmanagement / Digitalisation manager
- Mathematisch-technischer Softwareentwickler / Mathematical-technical software developer
- Mediengestalter Digital und Print / Digital and print media designer
- Technischer Systemplaner / Technical systems planner

The competence list for the IT systems electronics technician (https://www.bibb.de/dienst/berufesuche/de/index_berufesuche.php/regulation/IT_System_Elektroniker_2020.pdf) includes among others:

- implementing, integrating and testing measures for IT security and data protection
- installing and configuring IT equipment and IT systems,
- install network infrastructures and transmission systems transmission systems,
- plan and prepare servicing and maintenance of IT equipment and systems and their infrastructure systems and their infrastructure,
- completing orders and supporting users in dealing with IT equipment and IT systems and their infrastructure,
- IT security and data protection in IT systems, network infrastructures and transmission systems.

In addition to these IT-dominated vocations, there are dozens of other vocations that integrate IT-related competencies, i.e. managers and technicians for different fields.

IT-related BS and MS courses at state and private Universities, Universities of applied Science and at Cooperative State Universities are many hundreds, e.g.:

- BA in Cyber Security at Hochschule Mannheim (https://www.informatik.hs-mannheim.de/vor-dem-studium/angebot-bachelorstudiengaenge/cyber-security.html), which includes e.g.: Security Management and Secure Softwaredevelopment
- MA in Applied IT Security / Angewandte IT-Sicherheit at the Ruhr-Universität Bochum (https://informatik.rub.de/studium/studiengaenge/its/maits/), which includes e.g.: BSI-Grundschutz und ISO 27001, Human Aspects of Cryptography Adoption and Use.

Apart from these formal education programs, mainly provided by public institutions, there is a broad set of national and regional education providers, public and private, that provide varied – often certification oriented – course structures for initial training and continuous professional development, e.g.

- TÜV, usually known for technical facilities including cars, is also a nation-wide provider of a vast amount of further education courses in technological fields, mostly one to several day courses – physical and online – this includes varied courses on IT-security as well as data protection. Whereas the TÜV still has the legal form of an association (the V stands for Verein) like e.g. also the bitkom (a big association of IT companies) there are also nation-wide private further education providers like e.g. the Haufe-Akademie (https://www.haufe-akademie.de/).
- Big communal adult education centres might also offer respective courses; e.g. the Volkshochschule München (https://www.mvhs.de/kurse/it-digitales/it-sicherheit-datenschutz/seminar-it-sicherheit/pc-netzwerk-cloud-460-C-Q488880) offers a 4-day basic course on IT-Security, including e.g. network security, cloud security, email encryption
- On local and regional level there is an undefinable number of smaller companies and associations that provide courses in the pertinent field.

4.3 Summary and Intermediate Conclusions

The German vocational education system is clearly focused on formal and non-formal certifications that on the one hand allow employers to fulfil warranty requirements and on the other allows employees having opportunities on the labour market.

Accordingly, the system for assessing and acknowledging informally acquired competences is not well developed. For IT-specialists, which are heavily searched for and can find good jobs also without broach certifications, this limitation is not as strong as for other vocations.

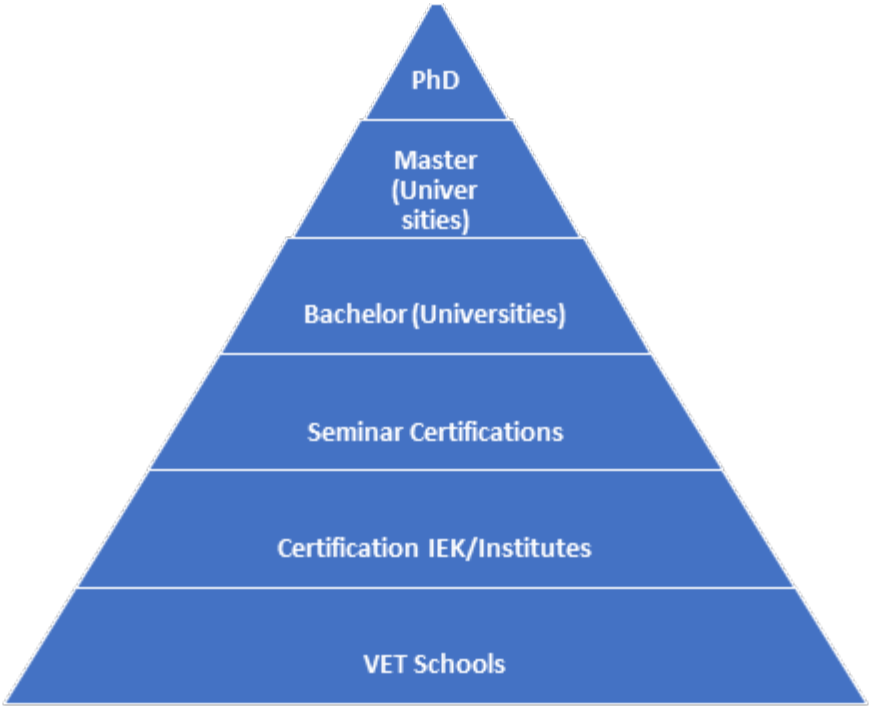
5 Greece

5.1 Ecosystem for Vocational Education and Training (VET)

In Greece, the Ministry of Education and Religious Affairs is the body responsible for education and religion. The respective municipalities of each regional unit are responsible for the proper organisation of schools. For this purpose, the Primary Education Committee and the Secondary Education Committee have been established. Education is compulsory between 5-15 years of age.

Primary education includes nursery school (lasting 1 year) and primary school (lasting 6 years). Secondary education includes Gymnasium (duration 3 years - daytime or 4 years - evening) and Lyceum (duration 3 years) and at this stage they can choose general or vocational education. They are also given the choice of schools with directions such as music and art schools. On completion of the course and through national level examinations they can enter Tertiary education. According to the final law on Vocational Education and Training (VET) (Law 4186/2013), in addition to the choice of general high school, students can choose:

1. 2nd cycle of secondary education in vocational high school (day or evening).
2. In the context of non-formal education, school, vocational education and training, IEK, KDBM and colleges.



The Law on Secondary Education (Law 4186/13) stipulates that vocational education is provided by the EPAL (vocational lyceum). Public and private EPALs are established by the Ministry of Education and Religious Affairs and are divided into morning and evening classes. EPALs provide sectors that have two or more specialisations. The specialisations may be adapted according to national and regional needs. School vocational programmes are accredited by the National Qualifications Certification Agency (EOPEP). They can still enrol in a public VET school or the Labour Employment Agency (OAED), with certification by a public body. They can also enrol in a Greek public university with specific scientific or technical training. All Public Universities provide state certification.

In addition to public VETs and Universities, there are also private ones. Private ones require students to pay a financial fee, are less years of study and the certification is provided by the Interdisciplinary Academic and Information Recognition Organization (DOATAP).

In addition, the National Strategic Framework for the Upgrading of Vocational Education and Training and Apprenticeship, published by the Ministry of Education, provides for the above. It states that: the National Strategic Framework for the Upgrading of VET and Apprenticeship is based on the analysis of the Greek reality and attempts a dynamic identification of the real needs of the economy and society in order to improve the current situation. The effort to reform VET is a complex process which has innovative characteristics for the Greek context.

In addition, many companies provide their employees with organised and systematic workplace training through seminars and fast-track programmes. Finally, non-recognised vocational training programmes are also carried out by the social partners such as the General Confederation of Workers of Greece (GESEE), the General Confederation of Craftsmen and Traders of Greece (GESEBEE), ADEDY, SEV and the Chambers of Commerce, with the aim of upskilling and reskilling the workforce of enterprises.

5.2 VET Offerings in Cybersecurity and Data Protection

Cybersecurity is the knowledge of personal and user security risks to private information and property related to the use of the Internet and self-protection from cybercrime. As the number of Internet users continues to increase worldwide, Internet organizations, governments and agencies have expressed concerns about the safety of individuals using the Internet.

Sensitive information such as personal and user identity, passwords are often linked to personal items (e.g. bank accounts) and their privacy and may present a concern about the safety of users if leaked. Unauthorized access and use of private information may result in identity theft, as well as property theft. Common causes of information security breaches include:

- Electronic phishing
- Online scams
- Malware

The Hellenic Authority for the Security and Privacy of Communications (HSAE) is the central authority in Greece for ensuring the security and privacy of electronic communications networks and services. The Hellenic Communications Authority was established in 2003 and operates under the supervision of the Greek Ministry of Digital Governance, as does the Hellenic Authority for the Protection of Personal Data, which was established in 1997. Its primary role is to enforce and supervise the implementation of the General Data Protection Regulation (GDPR) and other relevant data protection legislation in Greece.

In addition, the European Network and Information Security Agency (ENISA) has undertaken since 2012 the implementation of the European Month of Internet Security in Greece. In this context, programmes are developed by the Member States with awareness-raising activities, common messages and a wealth of information material is made available in order to foster a culture of security in relation to cybersecurity.

The Department of Digital Systems of the University of Piraeus offers academic programs in cybersecurity. They offer a Master of Science (MSc) program which awards a Master of Science (MSc) in Digital Systems Security. The programme focuses on the principles of cybersecurity, risk management, digital forensics techniques and secure software development. In addition, the Athens University of Economics and Business, and specifically the Department of Management Science and Technology of the Athens University of Economics and Business, offers a Master's degree in Information Systems with specialization in Information Security. The program covers topics such as network security, cryptography, secure software development and privacy. Also, the National Centre for Scientific Research "Demokritos" and in particular the "Demokritos" Institute of Informatics and Telecommunications offers cybersecurity training programmes and workshops

for professionals, researchers and students. They cover topics such as cryptography, network security, malware analysis and secure software development.

Furthermore, the Foundation for Research and Technology-Hellas (FORTH) designed a Collective Awareness Platform for Privacy Concerns and Expectations. CAPrice is an initiative launched by FORTH and specifically by the Information Systems Laboratory of the Institute of Computer Science to develop socio-technical solutions that can contribute to the promotion of privacy requirements of users of digital services. Through innovative collective consciousness tools such as citizen participation platforms, graphical explanations, structured consultation systems, etc., consumers and developers can work together in the context of a more trusted and privacy-conscious digital marketplace.

The Hellenic Internet Safety Centre (SaferInternet4Kids.gr) started operating in July 2016, under the auspices of the Foundation for Research and Technology - Hellas and more specifically the Institute of Computer Science. It is the official representative in Greece of the Pan-European Organizations INSAFE / INHOPE, which are developing the European strategy for a safe and quality internet. Through the website SaferInternet4Kids.gr one can be informed and obtain material related to the safe use of the Internet and the use of social networks, with which one can in turn interactively inform children and young people of all ages. This information portal is aimed at parents and teachers as well as teenagers and children and includes appropriate multimedia material.

The Institute of Computer Technology and Publishing "Diophantus" (ICTP) is a research and technological institution aiming at the research and effective use of Information and Communication Technologies (ICT). Particular emphasis is given in the field of education, with the development and application of conventional and digital media in education and lifelong learning, the publication of printed and electronic educational material, the administration and management of the Panhellenic School Network, as well as the support of the organization and operation of the electronic infrastructure of the Ministry of Culture, Education and Religious Affairs and all educational units.

Furthermore, the Hellenic Cyber Security Team (H.C.S.T.) offers a variety of training courses and certifications in the field of cyber security. Their programs cover topics such as ethical hacking, network security, digital forensics and secure coding. They provide hands-on training and practical exercises to enhance the skills of participants.

In addition, the Greek Computer Security Incident Response Team (GR-CERT), which is a unit of the Hellenic Research and Technology Network, conducts cybersecurity training programmes for IT professionals, system administrators and security officers. Their courses cover areas such as incident response, vulnerability assessment and secure systems management.

Finally, the Internet Safety Information Hub of the Panhellenic School Network (PSN) provides information material for children, adolescents, teachers and parents on Internet safety. The rich information material of the hub is addressed to pupils, teachers and parents and includes many thematic sections with articles, electronic forms, FAQs, links and audiovisual material. It also provides, among other things, guidelines on what social media users should and should not do when using Facebook and other similar social media.

5.3 Summary and Intermediate Conclusions

In Greece, the educational system offers a range of options, including both academic and vocational pathways, to meet the different needs and aspirations of students, with the aim of equipping them with the necessary knowledge and skills for their future endeavours. For this reason, emphasis is placed on vocational training schools, such as EPAL (Vocational Lyceums) and later IEK (Institutes of Vocational Training). In recent

years, the Ministry of Education has aimed to upgrade Vocational Education and Training (VET), which is a complex process and has innovative features for Greece.

Regarding Internet security (cybersecurity) and data protection, various trainings in Schools, Institutes and Universities can serve to inform pupils and students about the benefits of cybersecurity and personal data protection in order to stay safe. Overall, Greece has created a comprehensive framework of organisations, educational programmes and initiatives to address cybersecurity issues, protect personal information and promote a safer and more secure digital environment for its citizens.

In conclusion, cybersecurity is a vital issue in Greece, as it is globally, given the increasing number of Internet users and the associated risks to personal information and property.

6 Spain

6.1 Ecosystem for Vocational Education and Training (VET)

In Spain, education is a responsibility shared between the central government (Ministry of Education and Vocational Training) and the autonomous communities (17 regions and 2 autonomous cities).

The Ministry of Education and Vocational Training is responsible for setting the general educational policies and regulations at the national level, including the approval of the curricula and the establishment of educational objectives. It also manages and funds some national education programs, such as scholarships and grants, and provides technical and financial support to autonomous communities.

On the other hand, the autonomous communities are responsible for the implementation and management of the education system within their respective territories. They have the power to adapt the general educational policies to their specific needs, establish their own educational objectives and curricula, and manage their own educational resources. They also have their own education departments and regional education authorities that oversee the educational centers and programs within their territories.

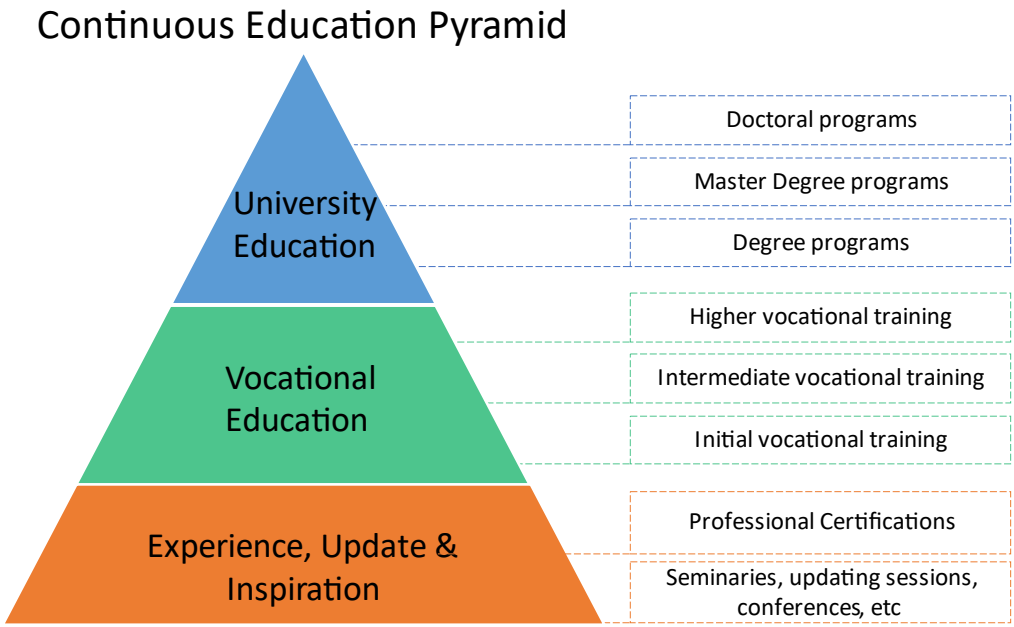
Therefore, the main players are:

- Governmental bodies:
    - Ministry of Education and Vocational Training (Ministerio de Educación y Formación Profesional): As mentioned earlier, this is the central government body responsible for education policy and regulation in Spain.
    - Autonomous Community Education Departments: As previously mentioned, the 17 autonomous communities and 2 autonomous cities in Spain have their own education departments responsible for managing the education system within their territories.
- Public institutions:
    - Public Universities: Spain has over 70 public universities spread across the country, each with its own administration and faculty. These universities are responsible for providing higher education to Spanish students and conducting research in various fields.
    - INCIBE, CCN-CERT, and OSI are some of the public institutions in charge of cybersecurity. INCIBE has a role oriented to help companies in this topic. Also, it is the Spanish authority that must be informed by private companies in case they suffer a cyber-attack. CCN-CERT has a similar role in cybersecurity for public institutions and critical infrastructures, and OSI is oriented to the citizen, to help them overall in the good use of the internet.
- Private institutions and associations:
    - In Spain there are around 40 private universities. These universities have the same competencies and regulations than public one. Therefore, they can offer homologated Degree and Maters programs. In addition, they can design their own programs such curses, boot camps.
    - Business schools. Many of these schools are internationally recognized and attract students from all over the world. They often have partnerships with other top business schools around the globe and offer exchange programs, allowing students to study abroad and gain international experience. This type of institution usually can offer degree or master programs by agreements with other universities as well.
- Employers play an important role in VET. In the Spanish VET system, employers are involved in several actions.
    - The Design: Employers often work with VET providers (private institutions) to design training programs that are tailored to the specific skills and knowledge needed in the industry or sector. This gains the possibilities for work once the student finalized VET.
    - Work-based learning: Many VET programs in Spain include work-based learning components, such as apprenticeships or internships.
    - Assessment and certification: In some cases, employers may be involved in the assessment and certification of VET students. They may provide feedback on a student's performance

during work-based learning placements, or they may participate in assessment panels that evaluate a student's competencies.

In general, the Spanish VET ecosystem is formal. Students can access different programs of education about cybersecurity. They will find several options and they will choose between public or private universities or High schools to develop their education in this topic.

Find the levels of the Spanish education system below, ordered by access requirements from bottom to the top:



6.2 VET Offerings in Cybersecurity and Data Protection

The main sources of information used were the official journals of the state and of the autonomous communities, which officially disseminate the educational offer for VET. But, in addition, specialized government agencies dedicated exclusively to cybersecurity provide reports, which have been extremely useful for the discovery and compilation of all the training available for learning in cybersecurity. This report from INCIBE can be used as a reference, *Información Regladda en Ciberseguridad en España*.[1]

There are only three university degree programs dedicated exclusively to learning cybersecurity. An example of these degrees would be *Grado en Ingeniería de la Ciberseguridad*[2], offered in more universities than the other two options. Despite the existence of university degrees dedicated exclusively to cybersecurity, there is a greater offer at the master's level for learning this field, with a more specialized perspective after the study of an engineering degree or the study of a university education related to ICT.

Some of these master's programs would be:

Máster en Ciberseguridad[3], is more focused on cybersecurity as a general matter. *Máster en Ciberseguridad y Privacidad*[4], focused also on privacy and information security, and masters such as the *Máster en Security Operation Center (SOC)*[5] or *Master en Ciberdefensa*[6] are more intensive on day-to-day operations.

[1] Información Reglada en Ciberseguridad en España
[2] Grado de Ingeniería de la Ciberseguridad
[3] Máster en Ciberseguridad
[4] Máster en Ciberseguridad y Privacidad
[5] Máster en Security Operation Center (SOC)
[6] Máster en Ciberdefensa

On the other hand, two different specialization training in cybersecurity is available for VET students. *Ciberseguridad en Entornos de las Tecnologías de la Información*[7] and *Ciberseguridad en Entornos de las Tecnologías de la Operación*[8]. The first one is more oriented to information systems and communications. In the case of the second one, you can find more subjects about industrial operations and IoT.

To conclude the analysis of formal education programs. In the Spanish landscape of continuing education exist another type of program known as *Professional Certification*[9]. This program validates and regularizes the knowledge of individuals who wish to work in cybersecurity. Obtaining this Professional Certification demonstrates that a person has sufficient knowledge to work in a cybersecurity position.

Apart from formal academic programs, university courses and traditional continuing education, private and public organizations also offer apprenticeships. This can provide an alternative way to receive training in cybersecurity. Some available resources include webinars, self-directed learning, and awareness modules. These modules aim to increase awareness about the proper use of technology and also help individuals implement more effective protective measures against cyberattacks.

The most significant examples of this kind of resource are available from INCIBE or CCN websites which are the governmental organizations dedicated to helping MEC and public organisms with cybersecurity respectively. Also, CCN procures a training itinerary to go on in its platform. (e.g., KIT de concienciación of INCIBE, Training itinerary of CNN)

Several cybersecurity companies and private academic institutions organize webinars on cybersecurity, as well as awareness and technical training sessions to help identify, detect, protect, respond and recover from cyber-attacks. For instance, Telefónica Tech disseminates information about these webinars through its social media channels. (e.g., Telefonica Tech Twitter)

Another example of private companies that publish this kind of resources to keep updated in Cybersecurity could be, Recorded Future, radaware or ISACA.

There are also other types of multimedia resources that make us easier to keep up to date on cybersecurity and data protection such as podcasts. However, these podcasts are usually oriented toward people with at least basic knowledge about cybersecurity. Find below some of the most relevant ones:

Name	Description	Link
Tierra de hackers	Cybersecurity news	https://www.tierradehackers.com/
Cosas de hackers	Discussions and cybersecurity news	https://www.ivoox.com/en/podcast-cosas-hackers_sq_f1876480_1.html
Securizando	This is a podcast that has a main objective explain cybersecurity easiest as possible.	https://securizando.com/category/podcast/
CyberAfterWork	It talks about everything related to cybersecurity at many levels, definitions, news, technical solutions and much more.	https://www.capitalradio.es/programas/ciber-afterwork

6.3 Summary and Intermediate Conclusions

Overall, the field of cybersecurity has several formal academic options, although they exhibit homogeneity as they share subjects and primarily emphasize a generalist approach.

[7] Ciberseguridad en Entornos de las Tecnologías de la Información
[8] Ciberseguridad en Entornos de las Tecnologías de la Operación
[9] Professional Certification

The offered degree programs have a strong engineering base and electives which are the big difference between a degree program in computer engineering or telecommunications and a degree in cybersecurity.

The master's degree programs are very similar, they share many subjects, and the content in hours is usually 60 ECTS, except for some that exceed it and reach up to 72 ECTS. On the whole, these master's programs include subjects such as threat intelligence, ethical hacking, hardening and cyber defense, computer forensics, regulation, and business continuity.

The biggest weakness found has been the lack of cybersecurity content for people who know nothing about the subject. Academic offerings are scarce for individuals who possess limited or no knowledge in the field of cybersecurity. In general, most of the existing content is available for professionals.

Another aspect to consider is that numerous intermediary institutions offer access to higher education through agreements with the universities, without being universities themselves. These centers are usually higher education or business centers. Some of them are offering the best masters in cybersecurity according to the ranking of the postgraduate world.

Find here some examples: IMF Smart Education, Immune Technology Institute, IEBS Digital School, INESEM Business School or EUROINNOVA Business School

7 Switzerland

7.1 Ecosystem for Vocational Education and Training (VET)

Switzerland is a country with a strong focus on innovation. The country is committed to actively shape the digital transformation[1]. Switzerland is a federal country. The Confederation consists of 26 Cantons. This structure is also reflected in the education and training system, as the Confederation, the Cantons, and organisations all contribute to the high standard of VET and strive to ensure that an adequate number of apprenticeships is available. VET is a valid learning basis and serves as a strong opportunity for many occupations.

VET imparts the skills and knowledge needed to work in specific occupation. According to the State Secretariat of Education, Research, and Innovation (SERI), two-year VET programmes lead to the issuance of a Federal VET Certificate; three-year and four-year VET programmes lead to the issuance of a Federal VET Diploma, during which, students have the option to attend general education courses in preparation for the Federal Vocational Baccalaureate Examination. The Federal Vocational and Professional Education and Training Act provides many opportunities, ranging from regulated and structured procedures for vocational groups to individual qualification procedures.

There are following main players of importance to the VET ecosystem:

- Governmental bodies on the Federal level: The National Cybersecurity Centre (NCSC) is the Confederation's competence centre for cybersecurity and acts as the first contact point for businesses, public administrations, educational institutions, and the general public for anything cyber-related. It is responsible for the coordinated implementation of the "2018–2022 national strategy for the protection of Switzerland against cyber-risks (NCS)". The Federal Data Protection and Information Commissioner is tasked, among others with the following: supervision of federal bodies, assistance to Federal and Cantonal authorities in the field of data protection, cooperation with national and international data protection authorities etc. In the private sector, in addition to his supervisory function, the FDPIC also carries out advisory tasks. He can provide insight and comments on the legal provisions about Data Protection, offer advice for the registration of data files, for the registration of transborder dataflows, and for requests about of the right of access. He also considered the first contact point for questions concerning legal problems or technical aspects of data security.
- Governmental bodies on the Cantonal level: In addition to the governmental bodies on the Federal level, each of the 26 Cantons also has an acting Data Protection and Information Commissioner. They supervise the application of the Cantonal Data Protection Act by each canton, the communes and the public-law corporations and institutions. In addition, they monitor compliance with the provisions on data protection, advise data subjects on their rights, mediate between data subjects and responsible bodies, and advise public bodies on data protection issues. Examples of Data Protection and Information Commissioners for Basel and Zürich.
- Public Institutions: Universities, schools and other public institutions also offer additional educational programmes for further education of VET.
- Private Institutions and associations: In addition to the public schools and institutions, private companies and associations also provide educational courses and trainings in the area of cybersecurity and data protection.

Overall, the Swiss VET ecosystem is formal. As one specificity, there exist certain types of certificates in continuing education. The certified programmes lead to qualifications awarded by the respective universities, federal institutes for technology or the universities of applied sciences recognised by the Swiss Confederation. The following recognised certifications can be achieved_

MAS – Master of Advanced Studies
An MAS (Master of Advanced Studies) is awarded upon completion of a programme lasting at least one year, a written examination and a dissertation. It generally results in a minimum of 60 ECTS credits. For example,

MBAs (Master of Business Administration), EMBA (Executive Master of Business Administration) or LL.Ms (Legum Magister) fall into the MAS category.

DAS – Diploma of Advanced Studies
A DAS (Diploma of Advanced Studies) is awarded upon completion of a programme comprising at least 250 contact hours, a written examination and, in most cases, a dissertation. It may result in between 30 and 59 ECTS credits. A DAS may in certain cases comprise part of an MAS.

CAS – Certificate of Advanced Studies
A CAS (Certificate of Advanced Studies) is awarded upon completion of a programme comprising at least 120 contact hours, a written examination and, in certain cases, a dissertation. It can result in between 10 and 29 ECTS credits. A CAS may in certain cases comprise part of an MAS or a DAS.

Another specificity of the Swiss market are the three national languages of the country – German, French and Italian. This leads to a variety of offers in the national languages. Moreover, also English-speaking offers are arising.

7.2 VET Offerings in Cybersecurity and Data Protection

As main source for the formal VET existing in Switzerland, a 2021 national report on cybersecurity trainings and education in Switzerland from the National Cyber Security Center (NCSC) was used.

There is a variety of study programs from universities. This spread from Bachelor to Master programs up until Doctoral Programs. Programs may be specifically focus on Cybersecurity, such as the BSc SUBSI Cyber Security[2] from the Fernfachhochschule Schweiz. Other offerings are more generally technical/IT-related and offer a specific branch in cybersecurity. One example is the BSc Computer Sciences – iCompetence study program[3]. Generally, the Bachelor program is perceived as a generalist education in Switzerland. Hence, it is more common, to have a focus on cybersecurity and/or data protection starting from the Master level. Several cybersecurity master programs exist in Switzerland, such as the Master in Cyber Security from École Polytechnique Fédérale de Lausanne EPFL / Eidgenössische Technische Hochschule Zürich ETHZ[4]. Still, there are a lot of Computer Science Master programs that have dedicated modules on cybersecurity, e.g., the MSc in Computer Science of the Eidgenössische Technische Hochschule Zürich ETHZ with a specialisation on cybersecurity[5]. Moreover, doctorate programs are offered in the field of cybersecurity – mainly these are Informatics or Computer/Computational Sciences programs. An example is the PhD in Information systems offered by the University of Lausanne[6]. For our report, we identified only one offering from CYD Fellowships dedicated to Cyber-Defense Research[7].

Besides Bachelor, Master and Doctorate, the topic of cybersecurity is getting prominence in continuing education. As described previously, Switzerland offers a set of continuing education formats that can build

upon each other/lead into each other. On a small scale, there exists a 3-day seminar offered by the University of Applied Sciences and Arts Northwestern Switzerland FHNW on data protection[8]. On a larger scale, a seminar by University of Lausanne on Cybersecurity is taking 7 days[9]. Some universities are very advanced and offering a full course catalogue. An example the Center for Digital Trust (C4DT) of the EPFL[10]. Their academy educates through tailored training programs led by experts on trust-building technologies. Going beyond seminars in the learning pyramid are the certificates of advanced studies (CAS). The courses are tailored to different target groups – ranging from courses with legal focus, to management focus to a rather technical focus. In addition, these courses might lead towards dedicated job profiles. Examples for this are the CAS Data Protection Officer of the Zürcher Hochschule für Angewandte Wissenschaften ZHAW[11] or the CAS for Security Incident Managers of the Berner Fachhochschule BFH[12]. Stepping to the Diploma of Advanced Studies (DAS) then these programs seem to be more seldom in Switzerland. We identified just four programs, e.g., the DAS-InfoSec Securite de l'Information of the University of Geneva UNIGE[13]. On the largest scale of the continuing education, there exist the Master of Advanced Studies (MAS). MAS in Cyber- or Information Security and Privacy are common formats here. Examples are the offerings of the Haute école de gestion de Genève HEG-GE [14] or the University of Lucerne[15]. As final offering in the category, we need to mention the advanced vocational trainings that lead to Swiss Federal Certificates & Diplomas. One example is the so-called "Cyber Security Specialist mit eidgenössischem Fachausweis"[16].

Turning away from university programs and classical continuing education, there also exist learning offerings from private institutions or chambers of commerce. In the following section, we provide several examples of such offers. These examples reflect the state on the Swiss market in May 2023 and thus the number, specificity, and form of the offers can be subject to change.

For example, the ISACA Swiss Chapter, an international professional association focused on security, control, audit, and management of information systems, offers annual advanced training courses as well as online courses for professionals in the field.

The Weblaw AG in Bern has been working at the interface of technology, for more than 20 years and offers an online platform, legal publications with a wide reach and information on projects at the federal level. In addition, the Weblaw Academy offers a wide range of courses for legal professionals at the interface of technology.

The Swiss Cyber Institute (SCI) is another education provider that focuses on helping society build a secure ecosystem. Relying on its industry-leading cybersecurity network, SCI offers training and access to an exclusive global cyber security community, while hosting international conferences that build bridges between security professionals, business experts, and academics.

Steiger Legal, a law firm with expertise in law in digital environments, offers many publications and podcasts on the topics of data privacy and security from various perspectives.

Isolutions, a Swiss cybersecurity company, offers various workshops for customers, employees and the public on various topics in cybersecurity.

Information Security Society Switzerland (ISSS), an independent organisation that connects over 1000 security professionals in Switzerland, offers various workshops on the topic of cybersecurity.

7.3 Summary and Intermediate Conclusions

The examples above show that, there are many offers, formal and informal, in an ever-changing educational landscape. It can be seen that Switzerland is a country with a strong formalism in the educational market. Employees of certain fields are required to obtain the qualifying certificates or diplomas mentioned above to officially certify their validity in the field. Merely learning on-the-job and thus gaining qualifications does not suffice. Therefore, the focus lies on the formal education offers, which, due to the national certification scheme, share a common qualification standard.

As for the nonformal offers from private companies and institutions that do not follow the national certification scheme, there can be no guarantee for quality. However, such offers can raise awareness and possibly incentivize customers to gain a more thorough understanding of the field.

In the field of data protection, offers are expected to increase in the Swiss market, as the new data protection law will come into force on 1. September 2023. Thus, the respective offers are expected to increase and adapt to the new issues that will inevitably arise for small businesses.

Both topics, cybersecurity and data protection, are very complex and difficult to understand, especially for small businesses. Therefore, all offers should be considered carefully because, for example, scattered single trainings can serve as awareness but more guidance would be needed to fully understand the business' requirements regarding cybersecurity and data protection.

8 Overall Summary and Conclusions

There are - at least previously - more company-based training systems like in Spain and school-based or academic ones in Cyprus and Greece, as well as the drivers French system that systematically includes the validation of non-formal and informal learning, which show more overlap between initial and further vocational training. Such systemic differences can play an important the role in concern of the uptake of cross-sectional topics, like information and data security, so they can differ significantly. Apart from these objective conditions there are also more subject-related ones.