Horizon 2020 Program (2014-2020)
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Assessing the courses for Cybersecurity professionals already developed by CONCORDIA[1] partners

Abstract: This document is part of the CONCORDIA deliverable D3.1 and is providing insights on the courses for Cybersecurity professionals already developed by CONCORDIA partners while placing them in the larger landscape of cybersecurity. The findings reflect the period of assessment between January – October, 2019, and will be further used as a basis for establishing a European Education Ecosystem for Cybersecurity.

Editors	*Felicia Cutas*
Contributors	*EIT Digital – Felicia Cutas* *UMIL – Claudio Ardagna* *UOP – Kostas Lampropoulos* *UT – Mattijs Jonker* *TUDA – Neeraj Suri*

1 This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927

The CONCORDIA Consortium

CODE	Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JUB	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
TUD	Technical University of Darmstadt	Germany
MUNI	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
ICL	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR	Telenor	Norway
ACS	Airbus Cybersecurity	Germany
SECT	secunet Security Networks	Germany
IFAG	Infineon	Germany
SIDN	SIDN	Netherlands
SNET	SurfNet	Netherlands
CYD	Cyber Detect	France
TID	Telefonica I+D	Spain
RD	RUAG Defence	Switzerland
BD	Bitdefender	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens	Germany
Flowmon	Flowmon Networks	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia	Italy
EFA	EFACEC	Portugal
ALBV	Arthur's Legal B.V.	Netherlands
EI	eesy innovation	Germany
DFN-CERT	DFN-CERT	Germany
CAIXA	CaixaBank	Spain
BMW	BMW	Germany
GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia

Table of Contents

Executive summary

Cybersecurity as a concept in industrial and business environment was considered in the past as an after-though of the design and operation of Informational Technology systems process. This had to do with the lack of proper training and security awareness of the business/industrial professionals involved in such environments. Under the light of many cybersecurity attacks that have caused havoc at European and International level and produced considerable risks and damages, this attitude has considerably changed. Thus, nowadays, there is a growing need by the industrial professional community for learning basic but also advanced cybersecurity concepts. This is reflected in the considerable amount of offered cybersecurity courses by various European and international organizations. However, despite the plethora of options to learn there is a profound lack of coherency and holistic planning in this training and awareness effort since each offered course (or series of courses) is designed with different criteria from other courses (by another organization). Hence, in several cases this approach is confusing the trainee on what and how he should perceive cybersecurity concepts, as well as how to use them to cover his professional needs. In Concordia, we acknowledge the problem and try to address it by developing a European Education Ecosystem for Cybersecurity that will include a broad range of courses presented in a consistent and coherent manner, that will take into account the actual needs of both the industry and the industry professionals, and that will indicate the roadmap on how to design new course serving the professionals in the best possible manner.

This document presents the portfolio of courses offered by the CONCORDIA consortium to different categories of industry Cybersecurity professionals within Europe such as technologists, mid-level managers, executives. This endeavor, along with other actions to be developed under the project, aims at contributing to the development of a European Education Ecosystem for Cybersecurity.

The findings presented in this paper will be further used in developing a Cybersecurity specific methodology for the creation of new courses and teaching materials for Cybersecurity professionals, and for potentially identify unmet needs in terms of courses. It will also contribute to developing a Cybersecurity Roadmap for Europe.

The document is organized as a progression of 3 chapters that cover the following:

Chapter 1: outlines the major educational/competence building challenges related to the Cybersecurity sector while also introducing a non-exhaustive collection of available Cybersecurity courses for professionals, both online and offline. The chapter overviews trends in needs of European companies in terms of cybersecurity types/profiles of jobs openings on LinkedIn over the period April – October 2019 and closes by pointing to different models aiming at helping (future) Cybersecurity professionals in developing the needed skills to build their career within the sector.

The intent is to contribute, as viable, to match the "demand and supply" for talent in term of skills development.

Chapter 2: presents the currently available pool of Cybersecurity relevant courses already developed by the CONCORDIA partners. The data on these courses was collected as to reflect their linkage to the five pillars of the data-centric approach to Cybersecurity advocated by CONCORDIA, and also their association to the five core industrial pilots that CONCORDIA is focusing on, namely Telecom, Finance, Transport e-mobility, e-Health and Defense sectors. Furthermore, the CONCORDIA industry partners were queried on their needs in terms of cybersecurity skills and people, in an attempt to get a better understanding of the general skills gap challenge.

Chapter 3: closes with some recommendations on the characteristics of courses needed to be offered on the Cybersecurity skills marketplace as to face the current challenges and to support the increasing demand for Cybersecurity professionals.

Chapter 1. The Landscape

What are the key Cybersecurity needs and challenge areas?

The digitization of industries, the constant increase in number of interlinked IoT devices, the dramatic rise in the data volumes and the pervasive use of ICT technologies in all walks of life are expanding the list of Cybersecurity risks.

A survey conducted by TUV Rheinland[1] lists 8 main trends in Cybersecurity for 2019. Relevant to our assessment exercise it's worth mentioning the following trends. Trend 1: Cybersecurity has become a board-level issue, Trend 5: The Cybersecurity skills shortage will distort the labor market, and Trend 8: Cybersecurity will define digital economy winners and losers.

Indeed, it is important to acknowledge that Cybersecurity it is not strictly an "IT matter" any longer, but it impacts all levels of the businesses and turned into a business risk. Cybersecurity strategies should address horizontally all departments of an organization and would need to be allocated reasonable funding, both for investing in technologies and in people at different levels. Thus, it becomes paramount to increase the trained workforce pool and to upskill the existing one, both in general knowledge but also in very technical ones.

According to the Varonis' infographics The future of Cybersecurity budgeting[2], most C-level executives (60%) interviewed consider that the current solutions they have implemented in their organizations keep them safe from cyber threats, thus do not prioritize investment in information security products and services. The disagreement over priorities between the senior management and the Cybersecurity experts contributed to exposing the companies to data breaches. Nevertheless, the importance of cyber protection is more and more acknowledged and 75% of the organizations studied have increased their Cybersecurity investments in the past 12 months. It is not clear though to which extent, part of this budget is allocated to skills development within the organization.

More than 40% of cyberattacks[3] are targeting small businesses. Besides, to date, 60% of small companies go out of business within six months of a cyber-attack. The skills shortage estimated to reach 1.5 million globally by 2020 will lead to an increase in salaries, making it challenging for the small organizations to attract talent so as to protect their organization. Consequently, if little investment in developing Cybersecurity skills within the organization is made, the cyber risk will turn into the main business risk.

1 https://img06.en25.com/Web/TUVRheinlandAG/%7B72babaf7-4989-4086-a89b-2536d75429b5%7D_TÜV_Rheinland_Cybersecurity_Trends_2019_EN.pdf
2 https://techaeris.com/2019/05/11/infographic-the-future-of-cybersecurity-budgeting
3 https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

The Cybersecurity sector has a strong annual growth rate, as the worldwide market for information security is expected to reach €145 billion by 2020. Part of this growth is generated by startups and young companies from the Network and Information Security sector, those innovative and agile way of acting bring an added value to the sector. An ENISA analysis on Challenges and opportunities for EU Cybersecurity startups[1] confirmed that the start-ups are as well impacted by the skills shortage because of the scarcity of the appropriate profiles and the cost of sourcing, which reduce their chances to scale-up. The same analysis identifies that on top of the category of investment and funding channels for the NIS start-ups are the following: investors specialized in Cybersecurity (e.g. accelerators); investors non-specialized in Cybersecurity; private stakeholders that provide support other than funding to NIS start-ups, such as private incubators, private accelerators and corporate open innovation in large companies. Some of these categories could be also looking into developing knowledge and be kept updated in the Cybersecurity area for the benefit of the startups they are investing in, and of the European Cybersecurity industry as a whole.

But the investors are not the only "un-conventional" category of professionals those activities would benefit from acquiring knowledge on cybersecurity. Following the trend of digitization, the cyberattacks are threatening an increased range of industries, thus forcing a shift in skills needed to perform traditional tasks. For instance, in the health sector, physicians would not only need to take care of the patients but also to protect their data. The cybersecurity threats and some of the associated vulnerabilities that currently affect the health sector are well described in the publication Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients [2] which also recommend cybersecurity practices for small organizations[3] and for medium and large organizations[4]. Same goes in the legal area where the practitioners would not only need to understand cybersecurity field if interested to become a cybersecurity lawyer but also to protect the information they are working with as a significant amount of data is collected during the process. Universities are expanding their offers as to prepare the new generations, but the practitioners should also get an understanding of the cyber domain and develop basic security skills.

When it comes to the IT professionals, the Tripwire Skills gap survey 2019[5] revealed not only that the skills gap is growing and it is getting harder for the companies to hire skilled security professionals, but also the fact that the skills required to be a great IT security professional are changing at a faster pace.

Both higher education industry and the professional training providers are working to address the increase skills need. But, as reflected in the ECSO paper Gaps in

1 https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups
2 https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf
3 https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol1-508.pdf
4 https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol2-508.pdf
5 https://www.tripwire.com/misc/skills-gap-survey-2019/

European Cyber Education and Professional training [1] there is a need for a transformation in the area. Cybersecurity is to be viewed as an emerging meta-discipline and not just an academic discipline. The academic education system approaches Cybersecurity from a holistic perspective whereas the professional training is usually focused on specific skills. As are addressing different learning needs, they should both be part of a career development path. Besides, they should not work in isolation but cooperate and exchange knowledge.

One of the challenges the organizations are facing today when looking for Cybersecurity specialists, is the difficulty in matching the recruitment criteria with the studies and the qualifications listed in the CVs of the applicants because of the use of non-standard terminology. The adoption of a standard lexicon, including cyber role responsibilities[2] will help on the one hand companies identifying the right talent for the job, and on the other hand the education providers better shape their curriculum to match the cyber workforce needs.

Finally, as the cyber threats an organization is facing are diverse and would require different type of skills and perspectives, a diverse team[3] should be built. The diversity within the team would require different backgrounds and personalities (techies, creative people, problem solvers, communicators, …) but also different age and gender. It will bring the advantage of reaching better outcomes as will help assessing situations from different perspectives and providing different approaches to problem solving.

What are the different Cybersecurity competencies needed?

In the context of the CONCORDIA project and for the purpose of this analysis we use the term "**Cybersecurity professionals"** as including academia thought mostly the broad group of industry representatives such as IT technical team members and experts, middle managers leading IT or non-IT technical departments, and executives of the companies.

Since Cybersecurity is a horizontal issue impacting all digitized industries, the needs in terms of competencies might differ but the following elements could be considered generally valid:

- IT Technical team members – are looking for acquiring new knowledge, developing new skills, and to upskill the existing ones. This category could incorporate also the recent graduates and the students coming back to the universities to follow only specific Cybersecurity related modules.

1 https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf
2 https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity talent identification and assessment.pdf?trackDocs=cybersecurity%20talent%20identification%20and%20assessment.pdf
3 https://www.forbes.com/sites/extrahop/2019/07/19/how-to-combat-the-security-skills-shortage/#27db2e464eae

- IT Technical experts and freelancers – are looking for expanding their Cybersecurity knowledge, or to test their skills in different scenarios.

- Middle-managers leading IT departments – are looking into learning about new techniques and/or solutions to identify, protect, detect, react fast and recover from a cyberattack.

- Middle-managers leading non-IT departments – are looking into understanding the general cyber related risks, and into practical techniques to be implemented as to avoid a cyberattack, and to recognize and know how to react in case such an event occurs. This category could include also non-traditional categories such as physicians, lawyers.

- Executives – are looking into having a general understanding of the Cybersecurity area and its impact on the business, investment and insurance wise included, as Cybersecurity is becoming a business risk. Cybersecurity Auditors within companies are also part of this group. This category incorporates also the startups and scaleups which do not afford having a specialized IT department to protect their business thus need to cover all the aspects of the business.

- Investors looking into in developing knowledge and be kept updated in the Cybersecurity area, in view of placing funding in different cyber or non-cyber related businesses.

- Academia – are looking for enriching their theoretical knowledge with information on new protocols, techniques, products, services developed by the industry

- Non-IT employees – not necessarily actively looking into developing Cybersecurity skills but being asked by the company procedures to have a basic knowledge in the field in order to prevent and/or react properly in case of a possible cyber-attack. This category could include also the users in general.

Besides, in order to build a career in Cybersecurity one should be aware that apart of technical skills, soft skills such as analytical-, communication-, writing-, leadership skills should ideally be developed.

These needs are backed by the findings of the International Information System Security Certification Consortium (ISC)2 in their 2018 (ISC)2 Cybersecurity workforce study1 in which Cybersecurity experts identified common challenges that could be addressed at the company level such as: the lack of security awareness among end-users; a lack of funding; not enough skilled staff available; a general lack of

1 https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

support/awareness from management about the urgency of Cyber- security initiatives overall.

Furthermore, the (ISC)2 study also depicts different skills areas identified by Cybersecurity professionals as important to be improved or enhanced in the future.

Figure A1. Credits: (ISC)2

It is important to note that, in today data-driven environment and data-driven economy, a cyber-security professional must have competences in the area of data analysis. The latter in fact is of paramount importance for guaranteeing and verifying cybersecurity in modern architectures. Even more, the role of the data scientist is fundamental to get rid of novel threats and attacks. In fact, security is moving from application security to data security, meaning that cybersecurity depends on data security and the capabilities of correctly interpreting the data at our disposal. Today, many Artificial Intelligence approaches are applied for guaranteeing cybersecurity, while, in turn, cybersecurity techniques are applied to artificial intelligence to prove some security properties on them. The need of data analysis for cybersecurity is clear in all above boxes in Figure A1. and especially in the dark blue box – "top areas for improvement", where a huge amount of data is collected every day (e.g., Cloud) and the ability of correctly analyzing them become fundamental (e.g., forensics). This is also true in the orange box – "areas to enhance and growth" pointing to the new effort supported by the European Commission in the definition of the EU Cybersecurity Certification Framework[1].

1 https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa

A look into the available course offerings

In the context of CONCORDIA, we consider the **courses/trainings for Cybersecurity professionals** as the courses to which a Cybersecurity professional can have direct access without being constrained to be enrolled in a full programme. These could be organized online, face-to-face, or could be blended.

A search on the Internet reveals that there is a plethora of courses addressing Cybersecurity professionals. The online courses are convenient to professionals as they offer full control on organizing peoples' time for studying thus helping them to cope both with the professional business life and the needs for upskilling or reskilling. These could be doubled by face-to-face courses for middle and senior managers or executives, or by specific competitions such as cyber-ranges for technical experts.

When it comes to the online courses, we identified the main platforms from the viewpoint of the users and of the Cybersecurity related content as being the following:

- Coursera[1] – has 33 million users and it has in its portfolio about 50 courses on Cybersecurity, most of them addressing introductory topics.
- edX[2] platform – has 14 million users to which it offers only around 30 Cybersecurity related courses
- LinkedIn Learning[3] - a learning platform with 9.5 million users, hosts around 120 courses on Cybersecurity, half of them addressing intermediate skill level, closely followed by courses aimed at developing basic skills levels
- Cybrary platform[4] offers to its 2 million users about 500 cyber specific video courses for professionals as to develop their careers, but also for businesses in view of workforce development.
- IASACA[5] (Information Systems Audit and Control Association) provides online, offline and mixed courses of different levels (foundation, practitioner) both for information security and Cybersecurity, including courses for Cybersecurity auditors. The courses are sanctioned by certifications. IASACA is a nonprofit global association that serves 140,000 professionals in 180 countries
- Udacity platform[6] – has 8 million users but has only a small (9) number of security/Cybersecurity courses

Although they are addressing the same market, each platform is structuring the information based on its own model, and without making a reference to any common competence framework. Thus, it makes difficult to compare the different offers and their attractiveness.

In an attempt to measure the reaction of the market to the risks the cyberattacks are bringing within the different industries, we used the public statistics offered by

1 https://www.coursera.org/
2 http://www.edx.org/
3 https://www.lynda.com/
4 https://www.cybrary.it/
5 https://www.isaca.org/pages/default.aspx
6 https://www.udacity.com/

LinkedIn Learning platform over a period of 6 months and monitored the number of "views" of different Cybersecurity related courses. The figures confirmed for instance a reaction to the increased Cybersecurity risk for the business by registering a raise in number of "views" from one month to another (between 7-15%) on courses for managers such as "Reasonable Cybersecurity for business leaders", "Cybersecurity for executives", "Microsoft Cybersecurity: shutting down shadow IT", "Cybersecurity for SMEs: essential training", all launched in late 2018 or early 2019. The biggest increase in views (19-20%) is registered for the course "Transitioning to a career in Cybersecurity", and the newly launched (June 2019) "Cybersecurity for IT professionals" and "The Cybersecurity threat landscape".

With respect to the cyber-ranges, information is very scarce thus difficult to assess at this stage. cyberwiser.eu[1] – the "Civil Cyber Range Platform for a novel approach to Cybersecurity threats simulation and professional training" newly launched end of 2018 and benefiting from H2020 funding, aims at providing a set of innovative tools to generate highly detailed exercise scenarios simulating ICT infrastructures to be used for Cybersecurity professional training, together with tools and solutions to simulate cyberattacks and defensive countermeasures. Cyberwiser.eu offers a "Behind the scenes: an in-depth look at the technology behind the CYBERWISER.eu Platform"[2]

The European Union Agency for Network and Information Security[3] (ENISA) put at the disposal of interested professionals a comprehensive set of training materials in support of developing skills in the Incident Response and in the field of Operational Security. In May 2019, the ENISA CSIRT training material[4] list was comprised of 42 titles, covering four main areas: Technical, Operational, Setting up a CSIRT and Legal and Cooperation. The offer for training courses for Cybersecurity specialists is, on the contrary, very limited. The trainings are available upon request by, for example, the National or Governmental CERT of the Member State, and must follow the EU regulation 526/2013.

ENISA and the Network and Information Security (NIS) education partners put together a NIS universities map[5] under which there are grouped together courses and certification programmes linked to Network and Information Security, most of them for undergraduates, postgraduates or at master level. Out of the 551 courses spread around the EU28, 538 are offline courses (data valid in May 2019). Most of the courses are requiring registration in a full curriculum thus they are not specifically addressing the Cybersecurity professionals and their needs as defined in this paper. Nevertheless, the map provides valuable content mainly to technical people

1 file://cyberwiser.eu
2 https://www.cyberwiser.eu/news/behind-scenes-depth-look-technology-behind-cyberwisereu-platform
3 https://www.enisa.europa.eu/
4 https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
5 https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

interested in developing a career in Cybersecurity industry, not necessarily engaged in a business activity and with no time restrictions.

Different international consulting companies and organizations include in their offers courses covering Cybersecurity topics:
Deloitte EMEA Cyber Academy[1] – offers online trainings, awareness programs, onsite trainings and a Hackazone Zone, an online learning platform containing over 125 challenges for performing hands-on exercises related to various Cybersecurity topics. They are targeting highly-qualified technical people but also executives and directive boards, technical and non-technical managers and executives and other employee grades. The Deloitte Academy area of expertise covers Ethical Hacking, Secure Software Development, Reverse Engineering, Monitoring and correlation, DDoS, Advanced persistent threats, Forensic Analysis, Cyber Intelligence, Cybersecurity and Mobile Device Security.
PwC's Academy [2] is offering specialized courses to professionals, companies, industries and government bodies in trending domains, between them the face-to-face course "Cybersecurity for Non-Cybersecurity Professionals during which the participants will be getting involved in a proprietary virtual game – Game of Threats[3].
EY Certify point[4] – is offering courses for certifying auditors on different standards such as ISO/IEC 27001:2013 - Information Security Management System, or SS 584: 2015 - Specification for multi-tiered cloud computing security, commonly known as MTCS
KPMG Cyber Academy[5] offers a blended framework of e-learning, virtual classrooms and workshop-based face to face training. Their offer ranges from penetration testing and security architecture to identity access management and cyber maturity assessment.

What are the companies looking for?

Despite the large offer for free courses, companies are facing difficulties for filling up their Cybersecurity related positions. According to the job openings published on LinkedIn and monitored for 6 months between April-September 2019, the total number at the level of EU28 remains pretty much stable from one month to another and it is around 3500 ± 5%. In general, the average period for a position opened on LinkedIn is one month. The fact that the total number remains almost the same it's a proof of the continuous need for professionals in the area. UK counts for one third of the positions opened followed in top 10 by The Netherlands, Germany, Portugal, France, Poland, Spain, Italy, Ireland and Belgium. (See Figure A2)

1 https://www2.deloitte.com/bd/en/pages/risk/solutions/deloitte-emea-cyber-academy.html
2 https://www.pwc.com/sg/en/academy.html
3 https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/game-of-threats.html
4 https://www.ey.com/gl/en/services/specialty-services/certifypoint/certifypoint---training-courses
5 https://home.kpmg/md/en/home/services/advisory/consulting/cyber-security/cyber-academy.html

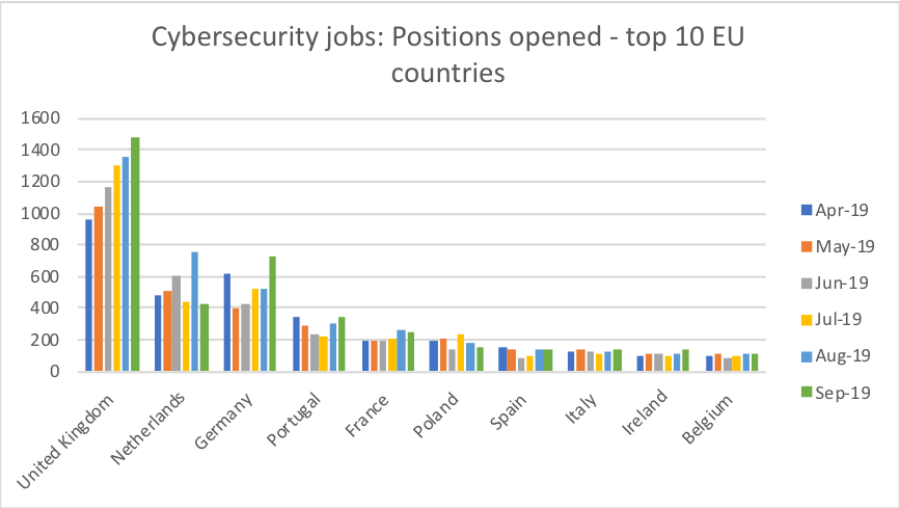


Figure A2: Cybersecurity jobs: positions opened – top 10 EU countries

When it comes to the experience required by the employer, the "Associate" level is most in demand, closely followed by the "entry level" positions. The most in demand job category in the cyber-domain is the IT, followed by far by the engineers. (Figure A3)

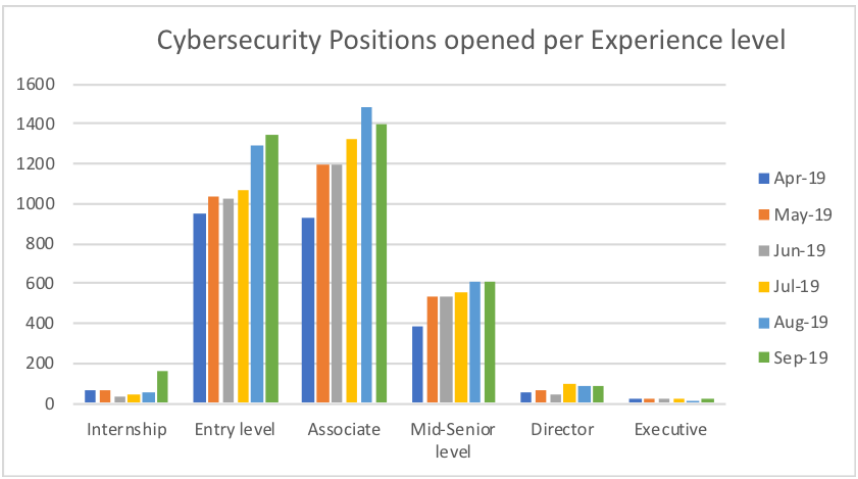


Figure A3: Cybersecurity positions opened per Experience level

If we contrast these data with the offer of courses displayed on the ENISA map with no pretention of an exhaustive analysis and aware about the limitations given by the subjectivity of the data, it can be observed that, countries with a big offer of courses, thus with presumably more entry level Cybersecurity skilled people, are not necessarily the ones also looking for hiring them and the other way around. For instance, Poland has 145 jobs opened in the Cybersecurity industry, but no course was reported on the NIS map. On the other hand, Slovenia encoded information about 12 courses on the NIS map, but the Slovenian companies have no positions open for entry and associate levels. (**Annex A.5.**)

How to match the companies needs with the skills offers?

Companies are usually looking for hiring already skilled IT technical people. Yet, in their absence, the companies try to re-skill and/or up-skill existing employees. This trend is confirmed also by the CONCORDIA industry partners questioned on the matter and described in the next chapter.

But the process of developing, displaying, searching for specific skills should be based on a generally agreed structure as to ensure a common language on the skills market.

In support of this endeavor one can get inspired from the US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework which depicts for different Cybersecurity workforce categories the necessary associated knowledge & skills and the list of tasks to be performed: NIST Special Publication 800-181[1]. This framework document is of use for different workforce development, education, or training purposes. At the European level, as already mentioned, ECSO is calling for a specific framework for professional development in Cybersecurity, to be jointly developed with the relevant actors in the field.

The Cybersecurity Career Pathway[2] proposes an interactive structure by listing the core Cybersecurity roles at entry- mid- and advanced-level and details the top skills and the top certifications requested for each position. As there is no clear and generally agreed taxonomy on the job titles in the industry, a useful information is also provided on the common job titles employers list in job openings for each role while also positioning the individual roles in the most common NICE Cybersecurity workforce framework categories. An example for an entry level role is depicted in **Annex A.1**.

The tool is mainly designed for the use of those interested to start and develop a career in Cybersecurity. Nevertheless, the structure could be used also by the companies when deciding to open a new position on the job market, not only by benchmarking the salary expectations with respect to the competition and the demand but also using similar keywords when describing the tasks as to ease the match between their needs and the skills and qualifications listed by the applicants in their CVs.

A Cybersecurity Competency Model Clearinghouse[3] was developed few years ago in the US in view of promoting skill sets and competencies essential to educate and train the workforce. The model is structures on 5 tiers: Personal Effectiveness Competencies, Academic competencies, Workplace Competencies, Industry-Wide Technical Competencies, Industry-Sector Functional Areas.

Annex A.2. includes more details linked to the different areas from Tiers 4 and 5 depicted in Figure A4: Cybersecurity Competency Model.

1 https://www.nist.gov/file/372581
2 https://www.cyberseek.org/pathway.html
3 https://www.slideshare.net/colleenlarose7/competency-model-clearinghouse

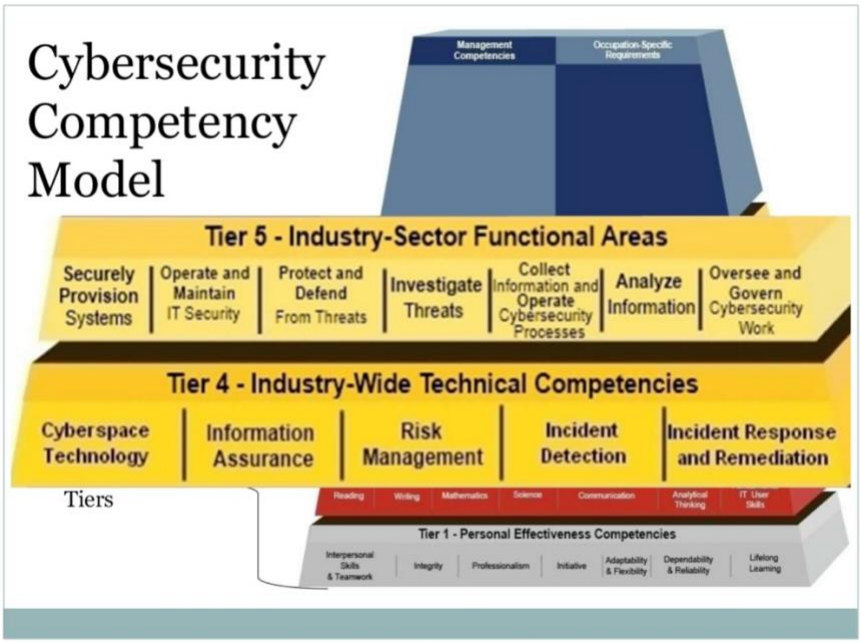


Figure A4: Cybersecurity Competency Model

At the European level, a concerted work on defining what are the competences needed to be owned/developed by different European actors playing a role in the Cybersecurity market or impacted by it, is currently pursued by ECSO in collaboration with their members, and the 4 Cybersecurity pilot projects. It will be based on existing competences frameworks such as European e-Competence Framework (e-CF)[1], NICE. The work will build, between others, on the ECSO Information and Cybersecurity Professional Certification [2] paper which looked into the professional security certification schemes and frameworks in Europe as well as internationally. The main findings are around the fact that the industry is still very dependent on US-centric certificates which are not based on formal training. And, even if in some European countries first steps have been taken to set up a certification scheme, the uptake of these schemes is very limited. The authors of the paper recommend the establishment of an EU-wide certification and accreditation scheme as well as a European framework for professional development in Cybersecurity.

Also, the ECHO pilot project is looking for developing a Cyber-skills framework (E-CSF) as to address the needs and skills gap of cybersecurity professionals based on a mapping of the cybersecurity multi-sector assessment framework. It is intended that the E-CSF will be made up of learning outcomes, competence model and generic curriculum in order to establish a mechanism to improve the human capacity of cybersecurity across Europe. In view of achieving this goal, the ECHO pilot will leverage a common cyber-skills reference, derived and refined from ongoing and related work in the field (e.g., ECSO, e-Competence Framework, European Qualification Framework).

1 https://www.ecompetences.eu/
2 https://ecs-org.eu/documents/publications/5bf7e0d81b347.pdf

Chapter 2. CONCORDIA ecosystem

We asked our CONCORDIA industry about their needs in terms of skills and technical people

In view of capturing the data, we invited the CONCORDIA industry partners to fill in a survey organized around two topics: Topic A - their practice in hiring cybersecurity related professionals, and Topic B - their needs in terms of developing cybersecurity skills within their organization.

The CONCORDIA industry partners are mainly representatives of the national and international corporate segment, and to a lesser extent the SMEs one. Less than 30% of the respondents are covering through their activities one or two of the Cybersecurity domains (see list and descriptions in **Annex A.5.3.**), while most of them develop activities touching 3-5 domains, with the Network-, Data/Application-Centric Security domains profiling on the top. When it comes to the industries they are active on, apart of the five CONCORDIA focus areas (telecom, finance, transportation, e-health and defence) some of the industry partners are also covering areas like semiconductor industry, energy, automation, IT, law, services.

The outcome of the survey can be summarized as follows:

Topic A. What are the organization's needs in terms of NEW employee categories & the associated skills?

- When looking for hiring new employees, the level of cybersecurity level requested with respect to the open position is depicted in the figure below. As expected, the IT related jobs require medium and high level of cybersecurity skills. Nevertheless, it can be observed that there is not yet a priority in asking non-technical people and executives to have basic skills in the area.

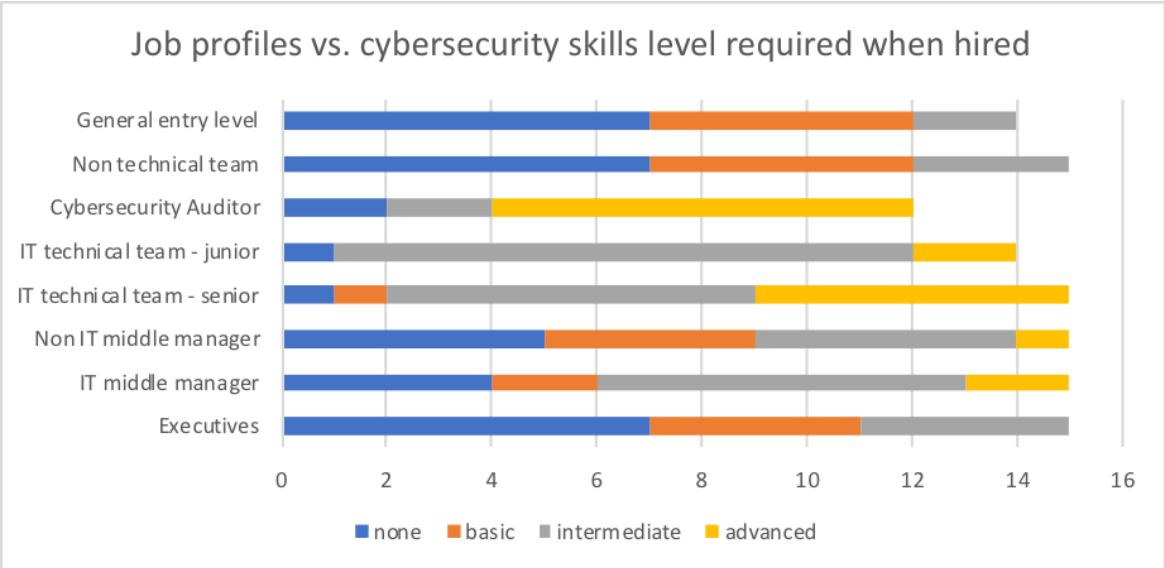


Figure A5. Job profiles vs. Cybersecurity skills level required when hired

- When asked about the relevance of the possession of a CERTIFICATE related to the cybersecurity skills in the process of recruitment, the answers are

almost equally spread between Very relevant for IT positions - Relevant for IT positions – Relevant for all the positions – Not necessarily relevant – Not relevant. It worth mentioning that the Not necessarily relevant – Not relevant options were selected mainly by the SME partners.

- 80% of the companies agree that an EU harmonized taxonomy related to the cybersecurity skills linked to different job positions would be useful in the process of recruitment
- In view of addressing cybersecurity needs within their organization, more than half of the organizations would rather prefer to hire an already skilled person than to re-skill or up-skill an existing employee. Nevertheless, in case they decide to invest in personal development of the employees, the in-house courses are preferred to external courses; yet, sometimes both options are approached in parallel: train and grow internally as well as hire from the outside.
- Additional practices in recruiting new employees were reported such as: hiring young people from academics as part time, and up-skill them via training-on-the-job; hiring from outside EU due to the lack of skilled personnel.

Topic B. What are your company needs in terms of cybersecurity skills development for EXISTING employees?

- When asked about what type of content for the courses the organizations are looking for their employees the vast majority of them pointed towards a mix of technical, hands-on and cyber-business-oriented topics. The weight of the type of knowledge within a course vary though depending on the role the employee is playing in the organization.

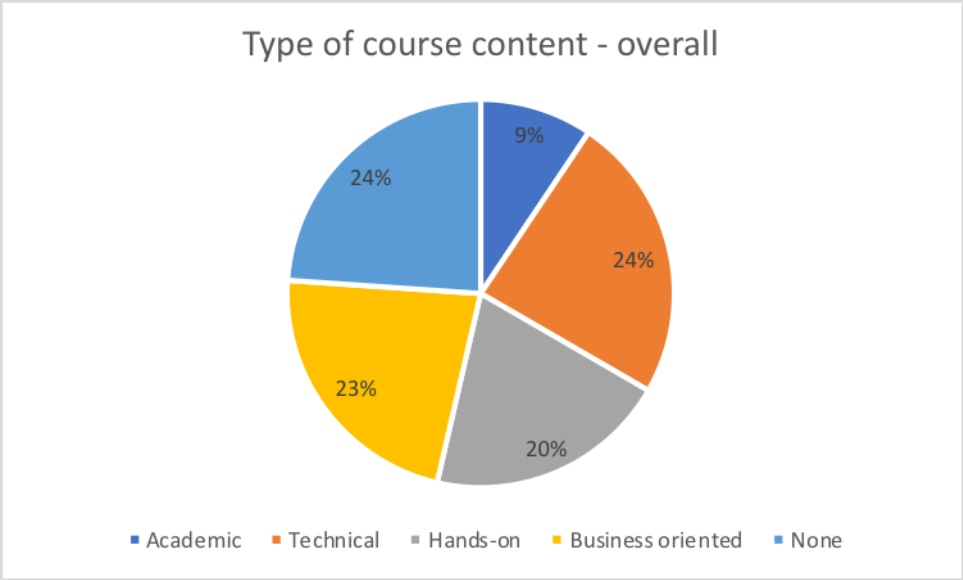


Figure A6. Type of course content - overall

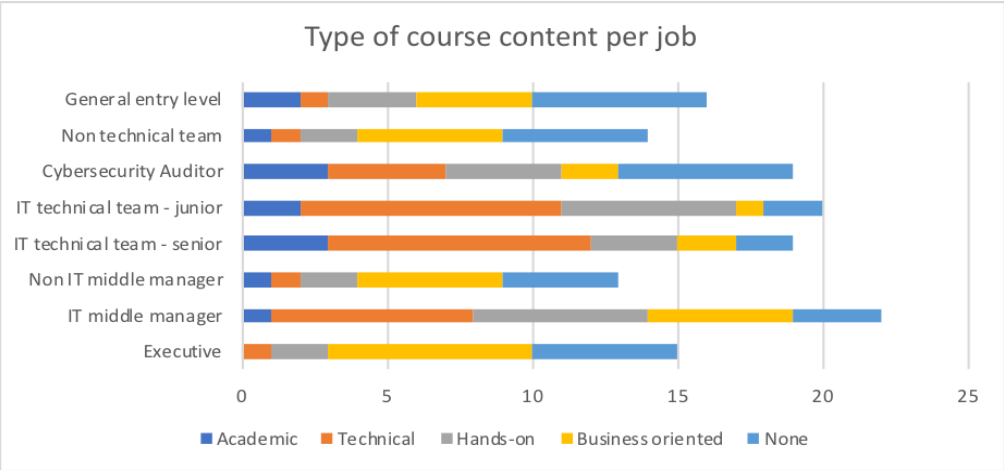


Figure A7. Type of course content per job

- Most of the companies surveyed are offering or would like to offer cybersecurity related courses to the different categories of their employees. Not surprisingly, the most targeted ones are the IT technical team seniors and juniors, but also the IT middle managers. The online format for courses is preferred by far while the blended format has the least traction.
- When it comes to the company normal practice with respect to the courses offered to their employees, apart of two companies declaring that they are offering the employees only courses developed inhouse, all the others are offering a mix of the following options: Develop and run in-house; Contract a course provider to tailor the content for the specific needs; Allow employees to find an online course that fits their needs; Buy off-the-shelf courses.
- The employees are offered the possibility to attend a course for updating their cyber related knowledge with different frequencies which vary from "as frequent as needed" listed by most of the companies to "once every 2 years", with a preferred length of 2-3 days in case of a Face-to-Face format.
- How important is the Certification option when buying a course for your employees? The in-house courses or baseline security courses offered to the employees are not necessarily selected because of the certification options. Yet the employer is interested in more than a certificate of attendance but of a Certificate issued by the training provider following a test/exam passed and/or Certificate offered by MOOC platforms as proof of the knowledge acquired. When it comes to the certifications based on standards, the following have been listed: CSX, CSX(P), OSCP, CEH, Cyber Essentials.

The CONCORDIA industry partners were also asked to list their top 3 immediate needs in terms of skills, considering the cybersecurity threats their organization is facing. The answers pointed mainly to traditional courses and varied from Security awareness and Security fundamentals to Solid understanding of mobile network security or Use of AI/Machine Learning; from Threat Intelligence analysis, Penetration testing and intrusion detection and Malware analysis, to Secure chip-design, Secure software-design and secure hardware-software co-design. Specific mentions were included on the importance of a hands-on, exercise-based approach including for the online format of delivery which should be as interactive and real life as possible.

Finally, the partners were asked to add any other comments linked to developing skills for cybersecurity professionals and which were not addressed by the previous questions. The most relevant of them are listed below and will be used in the development of the cybersecurity specific methodology for the creation of new courses and teaching materials.

“Need to easy to access and register courses, that are online, that are mobile device friendly, that cover concepts intuitively, and can provide links to more hands-on courses, if follow-ups are needed”

“We have a number of internal online courses which are obligatory for each employee and others that are obligatory for certain roles.”

“Coaching is an important part during the learning process. Could be on-line. “

"Cybersecurity professionals would benefit from the development of soft skills that could further support them works in a collaborative manner."

"Academic degrees, although interesting, appear to lack basic skills for the cybersecurity practitioners. When hiring a person with a degree in the subject, usually that only means that she/he have the potential to understand the subject provided specific theoretical and on-the-job training is provided. But even so, in some countries it is difficult to find even that. (e.g. Germany, Austria ...)"

"the semiconductor industry take a special place in the cyber security market; semiconductor companies stay at the beginning of the value chain for the security industry, which are focus on prevention of cyber-attacks; secure microcontroller, means develop, qualify and certify products along ISO 15408, EAL4+, 5+ or 6+"

CONCORDIA professional education landscape

CONCORDIA aims at establishing a European Education Ecosystem for Cybersecurity. The first step in this endeavor is to start collecting information on what CONCORDIA consortium offer in terms of skills development (university and industry partners). This data will be contrasted with the needs in terms of skills of different CONCORDIA partners (mainly the industry partners) and of the market as to identify the potential unmet needs in terms of skills development.

To this end we invited all the CONCORDIA partners to provide structured information on the courses/trainings they are organizing for Cybersecurity professionals.

Apart of a general description of the course, its location and the language taught, the following information aligned to the CONCORDIA scope and objectives were also collected:

- **Cybersecurity pillars** addressed – Device-centric // Network-centric // System/Software-centric // Application/Data-centric // User-centric security – see description of the pillars in **Annex A.3.**

- **Industry field** addressed - with a focus on CONCORDIA sector-specific pilots: Telecommunication // Finance // Transportation/e-Mobility // eHealth // Defence
- Main **target audience** – different categories of industry professionals
- **Type of course** (face-to-face, online, blended)
- **Entry requirements**
- **Type of Certification** offered

By end of year 2019, the CONCORDIA partners both from industry and academia, provided information on a total of 33 courses (**Annex A.4.**). The data is displayed on a dynamic map[1] on the CONCORDIA website for the use of the community at large. The map provides different filters as to help match easier the specific need for skills development with the offer.

Over the course of the CONCORDIA project, the map will be periodically updated with the new courses/trainings developed by the different university and industry partners. Besides, in our effort for establishing a European Education Ecosystem for Cybersecurity, the map is open for submission of courses/trainings for Cybersecurity professionals organized by other European organizations. To date the map displays already 27 courses organized in Europe by different organizations outside the Concordia consortium. The map will thus have the potential to become a marketplace for Cybersecurity skills for professionals.

General considerations

Most of the CONCORDIA courses were launched in 2018 or 2019. They are usually running once or twice a year with few exceptions such as the Cyber Incident Game planned for 4 sessions over a year, and SINA basic scheduled twice a month, with 15 sessions in total over a year. The short courses are between one day and one weeklong and are addressing groups of 10 to 20 people. The longer courses of the equivalent of one university semester (12-14 weeks) are bringing together larger groups of participants, namely between 80-120. Most of the courses are offered against a fee.

Cybersecurity pillars

A close look into the data collected with respect of the five CONCORDIA Cybersecurity pillars (**Annex A.3.**) addressed reveals the fact that almost 40% of the courses are specifically targeting one cybersecurity pillar, while another 40% are offering content valid for two or three pillars. Nevertheless, some courses are tailored to develop more general skills relevant for all the five pillars.

The most addressed pillars are the Network-centric, followed closely by the Data/Application-centric security and the Software/System-centric pillars. Interestingly, the least covered skills are in the area of Device-centric security which deals with data acquisition and the devices producing raw data such as embedded systems, sensors, IoT devices. The User-centric security pillar is also less addressed in the courses curricula although it deals with issues like privacy, social networks, fake

1 https://www.concordia-h2020.eu/map-courses-cyber-professionals/

news and identity management. This could be explained by the fact that CONCORDIA partners are mainly acting in the areas linked to the transportation and usage of data, and less in those dealing with data acquisition and devices producing raw data.

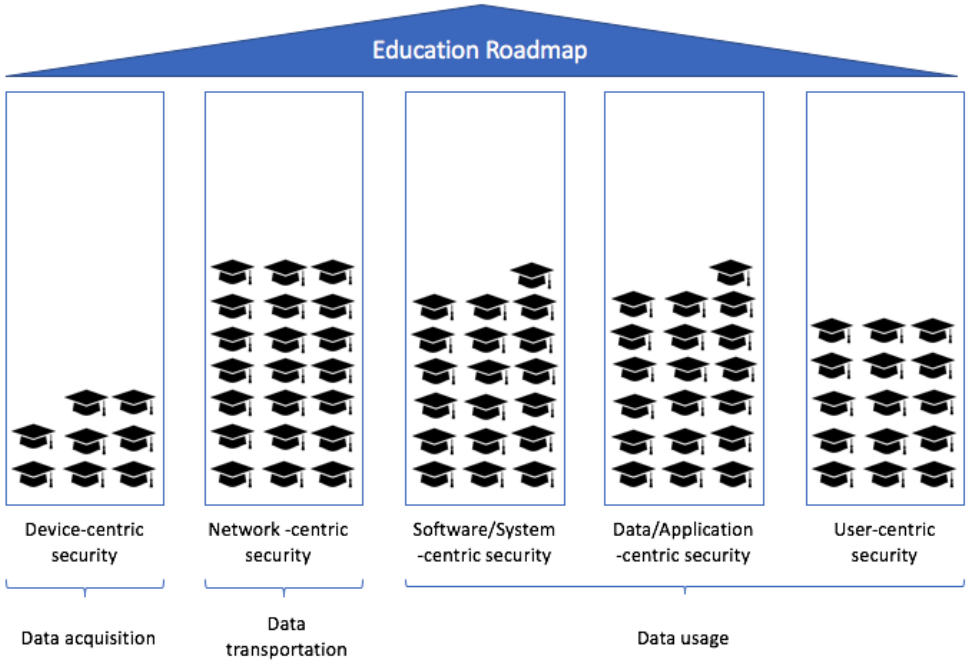


Figure A8: CONCORDIA courses – content vs. the cybersecurity pillars addressed

Industry fields

The five CONCORDIA sectors (Telecom, Finance, eHealth, Defence, Transportation / e-Mobility) are almost equally covered by the to-date CONCORDIA training portfolio with Telecom sector being the most addressed. The majority of the courses help develop skills applicable to at least 4 CONCORDIA industry sectors. Nevertheless, a number of other courses are targeting different other industries such as cloud, IoT, critical information infrastructure or operating systems, while almost a quarter of the courses are not related to any industry in particular.

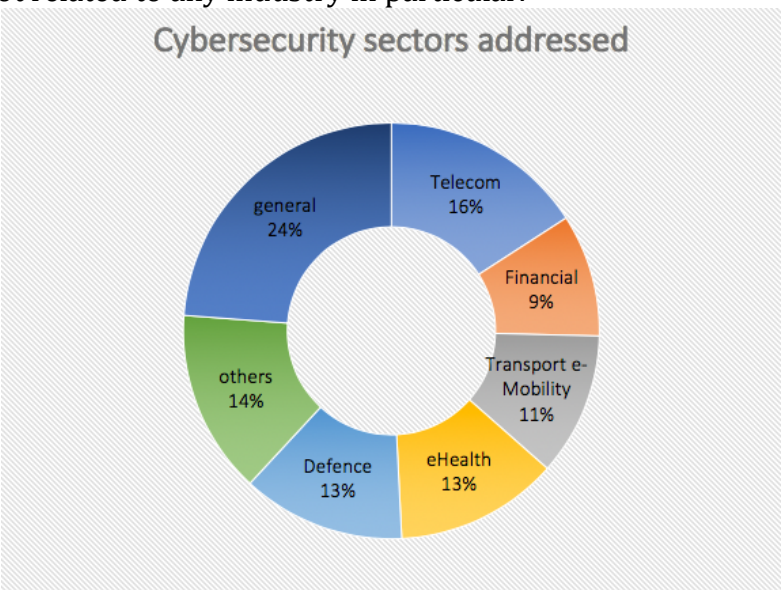


Figure A9: CONCORDIA courses – content vs. industries relevance

Target audience

The existing CONCORDIA courses are mainly addressing the technical people, and to a lesser extent the middle managers of non-IT departments and the executives of big and small companies.

Figure A10: CONCORDIA courses – distribution of the target audience

Delivery method - F2F, online or blended?

According to the (ISC)2 Cybersecurity Workforce Study 2018, the employers' main choice in offering skilling opportunities to employers is the online version as this is the most cost effective one from the management perspective. The face-to-face option ranks 5 in the list of options for professional development in the workplace, after conference attendance, personal study review and on the job with peers' alternatives. On the other hand, the same study reveals that the employees are more prone to attend the face-to-face (F2F) courses as these give them more opportunities to interact and network, to exchange experiences, and it is closely followed by the internet-based training.
When it comes to the CONCORDIA courses, the vast majority of them is offered exclusively in a face-to-face format while only two are fully online and three others are blended. Thus, they are very much aligned to the employees' appetite to consume this type of service.

Language taught

18 out of the 33 CONCORDIA courses are taught in English or offer this option as alternative to German or French. This already proves an openness to the European Cybersecurity skills market as language is not, in this case, a barrier. Nevertheless, 20% of the courses are exclusively taught on less common languages such as Czech, Dutch, Slovene or Italian.

Content

Content wise, the CONCORDIA courses are focusing on developing specific technical skills. This is reflected in the target audience those main group is the technical team, followed by academia and students' group. Nevertheless, some other courses take a broader approach to the topic and have low or no entry requirements thus are more accessible to a larger audience such as senior managers, managers of non-IT departments, startups.

Certification

To date, none of the courses organized by CONCORDIA partners are offering industry recognized certifications. Nevertheless, some of them are preparing the participants in view of applying for ISACA and (ISC)2 certifications. The vast majority of course providers are issuing certificates of participation, sometimes signed by a Cybersecurity expert. Others offer certificates of completion issued by a well-established online training platform such as Coursera.

Alumni

Although no consistent data was collected with respect to the participants to the courses organized by the CONCORDIA partners, the following information was considered to be a good estimate on the graduates so far:

- Total number of participants over the whole period the courses run: 5900+
- Gender distribution: 91% males and 9% females
- Age distribution: the majority of the attendees are in their early stages of their careers or in the growing stage as 62% of them are between 25-34 years old. 35% of the participants are between 35-54 years old and only 3% are between 55-64 years old
- Country of origin – most of the participants come from the countries in which the course is hosted (in case of the face-to-face courses). In case of longer duration courses (the equivalent of one university semester) the participants group is multinational like in case of a course organized in Germany which, apart from other EU participants, attracts people from China and India; or the case of the courses in Slovenia attracting also participants from Croatia, Spain, Portugal and Turkey.

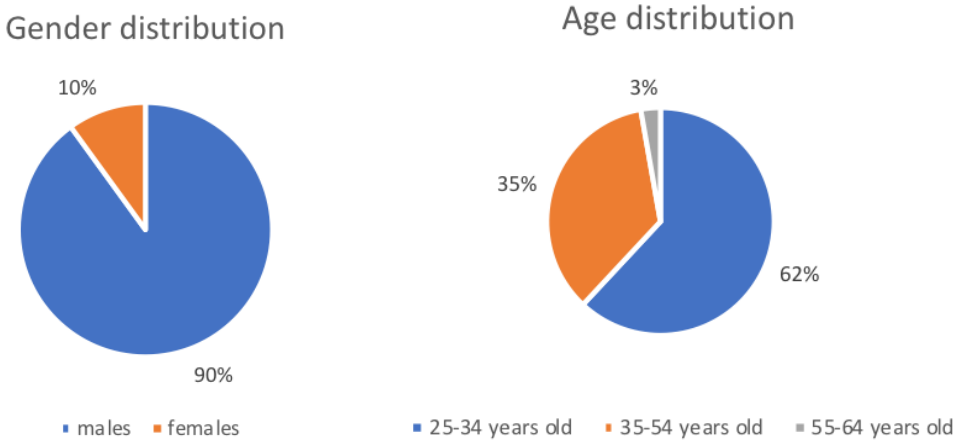


Figure A11: CONCORDIA courses – past participants distribution per gender and age

The external courses plotted on the CONCORDIA map

The CONCORDIA map was open for external submissions starting mid-July 2019. Over a period of 2 months there were submitted 27 courses via the Register your Course[1] form. This pool of external courses following to a certain extent the characteristics of the CONCORDIA courses and could be described as follows:

- Pillars: most of the courses address the Software/System-centric, Network-centric and Application/Data-centric pillars while the less targeted one is the User-centric pillar
- Industry: the vast majority of the courses are developing skills fit for the Telecom industry, followed by the Transport industry; some of the course providers reported also other areas of use of the skills acquired via their courses such as Energy.
- Target audience: most of the courses are targeting the corporate audience, mainly the technical team members but also the managers of the non-IT departments and the senior management group. Some of them are targeting the users - individuals using 5G technology or those interested to learn the approaches used by hackers, while one is specifically addressing the public administration
- Delivery method: face-to-face is the model used by 70% of the courses while only 4 are run online and only 1 is offered in a blended format.
- Language: the language used is, generally, country specific. Nevertheless, some of the course providers offer the course (also) in English, or provide the documentation in English
- Content: only 20% of the courses do not require any entry requirements as the content provided is considered introductory or close to introductory to the specific topic. All the other courses require basic to medium skills in the technical domains addressed by the course.
- Certification: 2 of the courses are offering official certificates recognizes by the national authorities while the others are offering certificates of attendance.

Chapter 3. Conclusions

The findings so far proofed heterogeneity both of the cybersecurity jobs market and of the cybersecurity courses offer. Besides, the lack of an agreed terminology cross domains and industries related to competencies needed for a specific job makes difficult for the companies to fill in the open positions, but also for course providers to design their curricula as to answer to the market needs, and for the individuals to identify the skills they need to possess or develop as to match the job opened on the market.

Pillars

In an attempt to create a high-level structure of the courses offered in Europe, we used the data driven approach and its five pillars advocated by CONCORDIA. We thus

[1] https://docs.google.com/forms/d/e/1FAIpQLScg5QrSQEOikUAJguXL3OrBhIPh3FzZzSvBk2RhGmh6ZRIMtQ/viewform

invited the course providers to register their courses on the CONCORDIA map by mentioning, between other elements, the cybersecurity pillars the skills developed under the specific course could be used. The findings gathered from 60 courses (33 from CONCORDIA partners and 27 from external course providers) shows that the least covered pillars in CONCORDIA are the Device-centric security pillar dealing with data acquisition and the devices producing raw data such as embedded systems, sensors, IoT devices, and the User-centric security pillar dealing with issues like privacy, social networks, fake news and identity management. These findings, although not necessarily representative for the whole European market, match the threats identified in the first chapter, especially those linked to the user-centric security pillar.

Target

More general cybersecurity awareness needs to be offered across different industries, not necessarily technical ones, thus targeting non-traditional cyber audience. Although there are quite a few online courses addressing this general need, there is little or none tailored to some specific non-technical audience yet targeted and impacted by cyberattacks. In this respect the following topics could be envisaged: Economics of Cybersecurity within an organization, Cybersecurity for lawyers, Cybersecurity for physicians, Cybersecurity for investors. The Cybersecurity for Investors course for instance, could answer to problems identified in the ENISA analysis on Challenges and opportunities for EU Cybersecurity startups[1]) and could be co-organized in collaboration with Invest Europe[2] . The knowledge acquired by the investors will help them not only when looking for investing in Cybersecurity companies but also when assessing the viability of any of the companies as cybersecurity should be treated as a business risk.

The industry survey reveals an increased interest in Cybersecurity awareness courses as untrained staff is the greatest cyber risk to the business.

When it comes to the technical area, in a data-driven environment and data-driven economy, a Cybersecurity professional must have competences in the area of data analysis. Thus, a specific curriculum for data scientist positions would be beneficial to be developed. Some other topics could be further identified based on the analysis to be done in the Deliverables linked to the Threat landscape, legal environment and economic perspectives.

Content

Content wise, the courses would need to be developed in relation with an agreed EU competence framework. They should not stay at a general level as to ensure their relevance for a broad cross industry audience but should be industry specific and built starting from clear learning objectives defined in direct collaboration with the targeted industry representatives. No matter the target audience, a broad approach to the topic would be advisable, as to cover both technical knowledge and soft skills,

1 https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups

2 https://www.investeurope.eu/

but also some managerial skills[1]. The weights of the different subjects should be balanced though, according to the profile of the target audience. The hands-on approach and real case scenarios adapted to the specific audience should be favored.

Language

EU is a multi-cultural continent and local language skills are important to communicate. Yet, the free movement of people comes with free movement of skills and the language should not be a barrier. Thus, in an attempt to build an international network of Cybersecurity experts looking into exchanging information in support of better protecting Europe against cyberattacks, the trainings should, at least partially be taught in English, the language of the computer (most programming languages use English language keywords). Choosing English as a main language would increase also the participation in the different MOOCs which are in their vast majority taught in English, still a barrier for non-English speakers[2]. It will also support the mobility of the Cybersecurity professionals from countries with a big offer of courses, thus presumably more Cybersecurity skilled people to countries with big demand on job market.

Certification

Undoubtedly, certifications are important in the process of recruitment of the cyber professionals. And at the international level there are quite a few very specific certifications for the IT professionals. In Europe though, as revealed in the ECSO study, the industry is still very dependent on US-centric certificates which are not based on formal training. And, even if in some European countries first steps have been taken to set up a certification scheme, the uptake of these schemes is very limited. There is thus room and a need for a European Cybersecurity certification scheme. During the duration of the project we will be looking into developing a framework of a certificate.

The analysis helped identifying some topics and some good-to-have courses' characteristics. These findings will be further considered when developing the cybersecurity specific methodology for the creation of new content and teaching materials. Besides, the course content development and deployment are intended to be designed in such a way as to be aligned to the CONCORDIA certification framework.

The paper will be periodically updated as to capture the new trends, challenges and offers in the cybersecurity education and will contribute to the definition of the education pillar of the Cybersecurity Roadmap for Europe.

1 https://insights.dice.com/cybersecurity-skills/

2 https://www.academia.edu/23952938/Planning_to_Design_MOOC_Think_First_?email_work_card=title

Annexes

A.1. Cybersecurity Career Pathway - example

Source: https://www.cyberseek.org/pathway.html (data collected from September 2017 through August 2018)

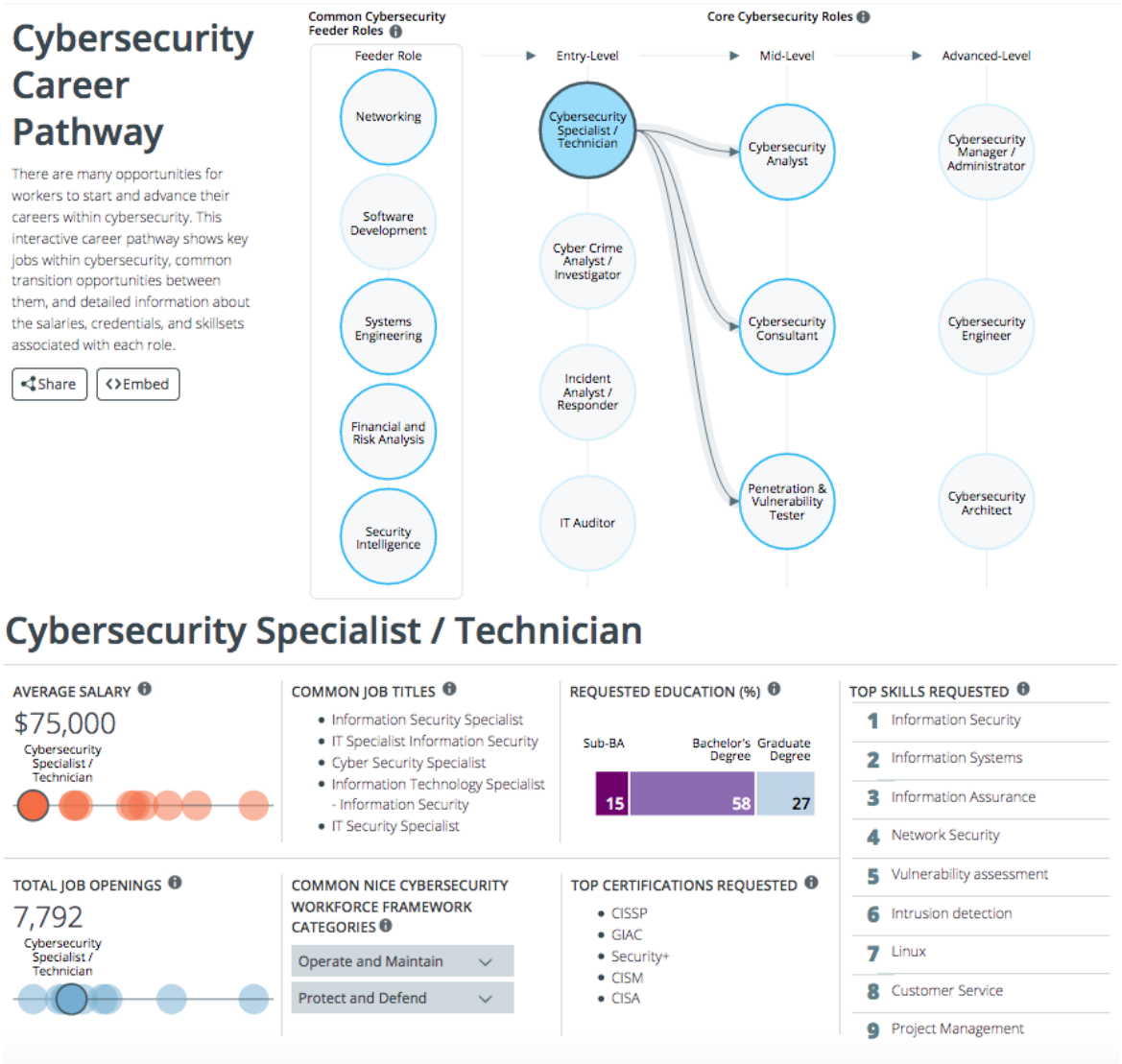
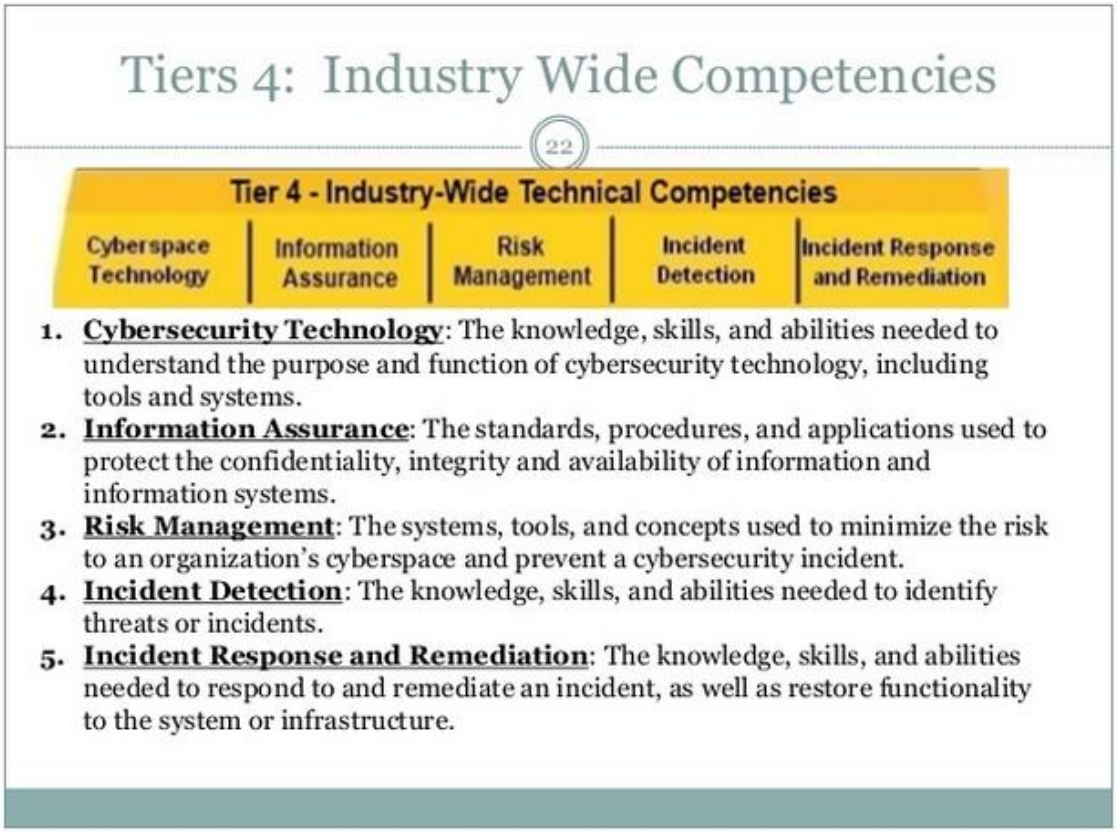


Figure A12. Cybersecurity Career Pathway – example for Cybersecurity Specialist/Technician

A.2. Cybersecurity competencies

Source: https://www.slideshare.net/colleenlarose7/competency-model-clearinghouse



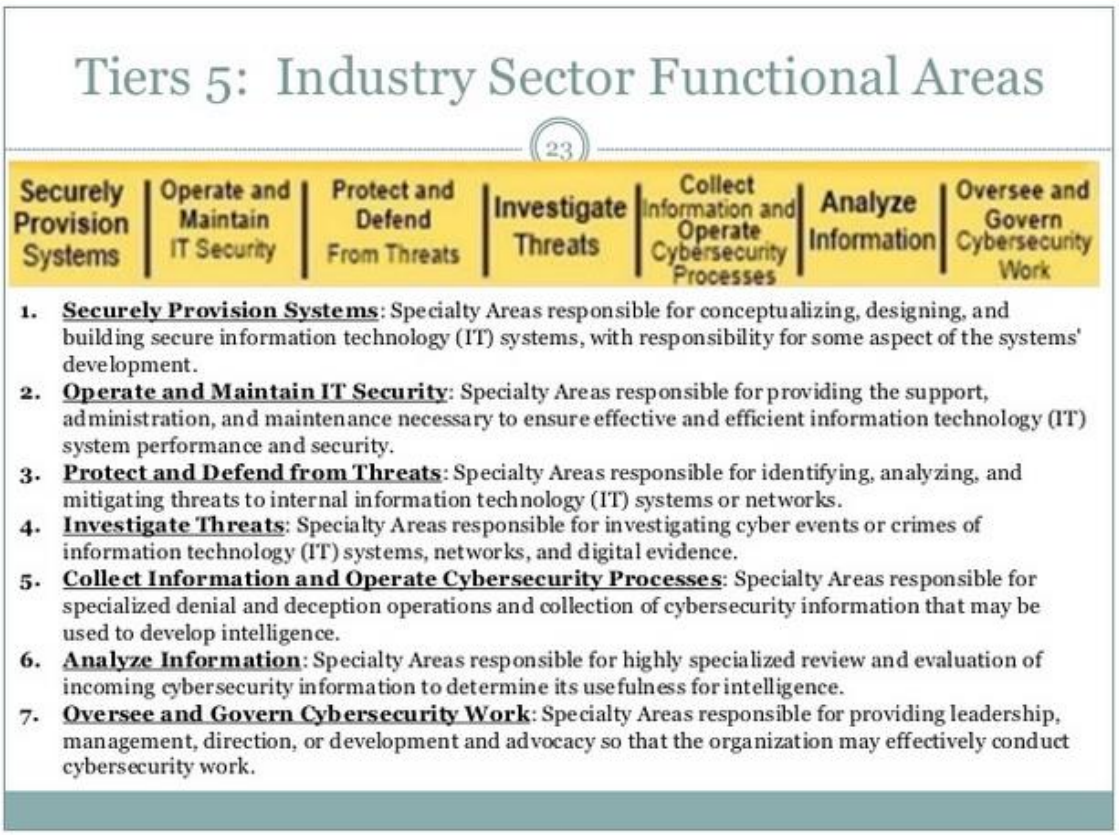


Figure A13: Cybersecurity Competencies – Tiers 4 and 5

A.3. The 5 pillars of the research and technology

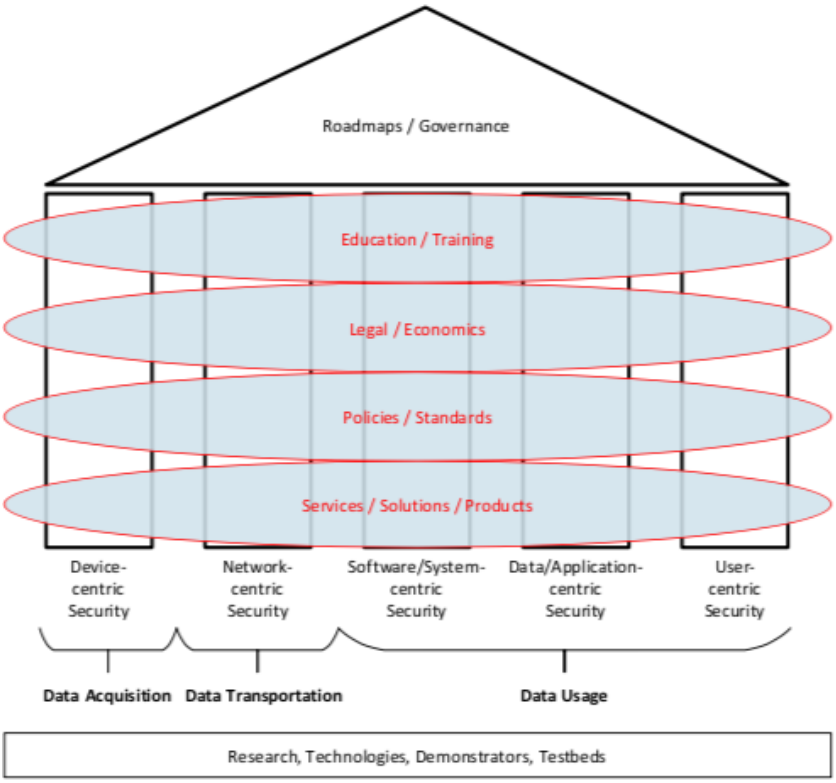


Figure A14: CONCORDIA - The five pillars of the research and technology

CONCORDIA has a data-driven approach to security and addresses it via the five pillars of research and technology as illustrated in the figure above. The individual pillars are described as follows:

• **Device-centric Security**: DCS addresses the *data acquisition* and the devices that produce *raw data*, such as embedded systems, sensors, IoT devices, drones, and the associated security-centric issues, such as IoT security.

• **Network-centric Security**: NCS refers to the *transportation of data* as well as with the networking and the security issues associated with this. Topics range from DDoS protection, Software-Defined Networking (SDN) to encrypted traffic analysis.

• **Software/System-centric Security**: SSCS centers around topics such as middleware, secure OS, and security by design. malware analysis, systems security validation, detection of Zero-days, and recognizing service dependencies are specifically addressed.

• **Data/Application-centric Security**: DACS addresses issues such as data visualization and the security of applications like cloud services.

• **User-centric Security**: UCS addresses issues like privacy, social networks, fake news and identity management.

A.4. The CONCORDIA courses (November 2019)

Title	WHO	WHAT
CyberRange: IT Ethical Hacking	Airbus Cybersecurity	Hands-on Labs on different topics and countermeasures in a simulated network.
ICS-Ethical Hacking	Airbus Cybersecurity	Hands-on Labs on different topics of threats scenarios and countermeasures in a simulated industrial environment.
Cyber Incident Handling Workshop	Airbus Cybersecurity	Table-top game to learn how to deal with cyber incidents from different perspectives.
CyberRange: Advanced Persistent Threats and Targeted Attacks	Airbus Cybersecurity	Hands-on labs to learn current techniques of APTs and Targeted Attacks.
Cyber Incident Game	Airbus Cybersecurity	Play the hacker role: plan a cyber-attack on an classical network or an industrial network infrastructure.
Cybersecurity for business	EIT Digital	An innovative training to empower and train in improving and championing Cybersecurity for the future
Security and Privacy for Big Data	EIT Digital	Learn how to identify key security and data protection issues and how to apply privacy preserving methodologies in compliance with the current regulations
ENISA Summer School (assisting the organization)	FORTH	Network and Information security: policy, economic, legal and research matters
CSIRT Cyber Training	Masaryk University	Hands-on tailor-made Cybersecurity training for IT administrators and CSIRT/CERT members. Everything from servers hardening to network monitoring & analysis
Capture the Flag by Team Localos	Research Institute CODE	Learn and evolve your Cybersecurity capabilities. And have fun at our Cybersecurity competition!
IT Competence Education and Training	Research Institute CODE	In our flexible Cyber Range, participants are provided with self-learning modules, individual exercises as well as

		defensive/offensive hands-on scenarios.
SINA Basics	Secunet	Basics and functions of the Secure Inter-Network Architecture (SINA)
TRANSITS I/II	SURFnet	Training for new and experienced computer security incident response team (CSIRT) personnel, and individuals interested in establishing a CSIRT.
Reliable Software and Operating Systems	Technical University Darmstadt	Dependability and Security Issues for SW systems
Security and the Cloud: The Issue of Metrics	Technical University Darmstadt	SW and Distributed Systems Security
ICT Security	University of Mariboru	Basics; Physical security and biometrics; Cryptography basics; Secure e-commerce; Protection of communication technologies; Standards, security policies and security planning; Software security; User aspects of security and privacy
Data protection	University of Mariboru	Introduction to the topic; Advanced cryptography; Usability and related standards; Practical aspects of data protection
ADVANCED INFORMATION SECURITY	University of Mariboru	Provide in-depth knowledge on techniques for securing and protecting information, computer systems and computer networks
Data security and privacy	University of Insubria	Models, tools and languages for managing access control and privacy policies/ preferences in a data management system
DATA SECURITY FUNDAMENTALS	University of Insubria	Basic knowledge for the design and verification of mechanisms for data protection in information systems and networks
Internet Security Protocols	University of Twente	MOOC to discuss the details of Internet security protocols, such as HTTPS, SSH, DNSSEC, IPSec and WPA

Internet attacks and defence	University of Twente	MOOC to discuss how to detect and mitigate Internet attacks. Topics include DDoS, IDS and Firewalls
Certified Information Systems Auditor CISA - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CISA certification. The Certified Information Systems Auditor (CISA) is a globally recognized certification for professionals in the areas of auditing, control and information security.
Certified Information Security Manager CISM - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CISM certification. The Certified Information Security Manager (CISM) is a globally recognized certification for experts in the field of information security management in companies.
Certified Information Systems Security Professional CISSP - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CISSP certification. The CISSP examination covers 8 areas of security which are necessary for the essential protection of information systems, companies and national infrastructures.
Certified Secure Software Lifecycle Professional CSSLP - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CSSLP certification. The CSSLP certification guarantees that you have comprehensive knowledge in all areas of the secure development lifecycle.
CyberSecurity Essentials	SBA Research	The aim of the course is to provide participants with an introduction to the topics of cyber security as well as IT and information security. The course provides participants with sound basic knowledge and essential threat scenarios as well as modern solutions and methods for coping with cyber risks.
Incident Response	SBA Research	The aim is to learn tools and techniques for clarifying an APT incident. The course

		participants will also have the practical opportunity to investigate a simulated APT attack using hard disks and memory images.
Windows Hacking	SBA Research	The aim is to convey the most frequent and dangerous gaps in Windows networks and thus provide the necessary knowledge for securing security-relevant networks and servers.
Secure Coding in C/C++	SBA Research	This training is especially designed for C/C++ developers. It covers secure software development practices and attacks.
Web Application Security	SBA Research	The course teaches developers the most common and dangerous bugs in web application development. Testers learn how to test security aspects.
IoT Security Essentials	SBA Research	The course teaches the typical and dangerous security vulnerabilities of Internet-enabled hardware, including the OWASP Internet Of Things Top 10.

A.5. Courses offer on NIS map vs. Jobs opened on LinkedIn

EU Country	Academic Courses offer ENISA map	Jobs opened - Entry &Associate levels - Oct'19	Jobs opened - Total - Oct'19
Germany	148	511	762
United Kingdom	97	1,068	1,459
Czech Republic	46	18	30
France	33	150	229
Belgium	31	54	98
Netherlands	22	375	559
Spain	22	63	124
Finland	18	9	18
Portugal	16	313	347
Italy	15	134	192
Cyprus	12	0	1
Slovenia	12	0	0
Sweden	10	24	68
Ireland	7	58	120
Austria	6	15	29
Greece	5	4	7
Romania	4	35	78
Estonia	3	5	11
Latvia	2	3	5
Denmark	1	20	41
Hungary	1	9	21
Luxembourg	1	19	31
Bulgaria	1	15	27
Croatia	1	0	0
Malta	1	0	0
Poland	0	96	145
Lithuania	0	5	8
Slovak Republic	0	5	11