Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D6.3

Design of Education and Professional Framework

Document Identification	
Due date	31 January 2021
Submission date	25 March 2021
Revision	2.0

Related WP	WPCO	Dissemination Level	CO
Lead Participant	VTT	Lead Author	Anni Karinsalo, Kimmo Halunen
Contributing Beneficiaries	ABILAB, ATOS, DTU, ICITA, POLITO, UM, UMU	Related Deliverables	D6.1, D6.2
Contributing Authors	Simon Coltellese, Gabriele Gamberi, Marco Rotoloni, Juan Carlos Pérez Baún, Susana Gonzalez Zarzosa,		

	Alberto Lluch Lafuente, Borislav Semstrinski, Alexander Zahariev, Andrea Atzeni, Daniel Canavese, Marko Höbl, Tamara Bubnjar, Marko Kompara, Antonio Skarmeta, Sara Nieves Matheu Garcia		

Abstract: This deliverable presents a short review of the most relevant European Cyber Security-related professional education frameworks, and establishes a framework for assessing skills and competences required for different Cyber Security roles in organizations. This relates to the Task description "*the initial review of existing programs at European Level and the final development of assessment mechanisms for the general Cyber Security capabilities of the workforce across all Demonstration cases*." Four use cases that include twelve scenarios are presented, with related profile descriptions. Using our framework, required skills in each of these scenarios are evaluated. Then, the profiles and what is their average Cyber Security skill level required in each of the scenarios are evaluated according to a four-step skill rating scale. Also, a customised framework targeted for lawyers is presented. In addition, a preliminary evaluation of all the skills required in all the framework profiles is presented.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

The need for Cyber Security education in a European context has been identified by many organisations. The lack of such an education will pose a grave risk for all stakeholders in the European society. There is also a need to identify what skills and competences, and at what level, are needed in the various Cyber Security roles. To achieve these goals, several taxonomies, frameworks and educational programs have been proposed. This document first reviews the most common Cyber Security-related professional frameworks and analyses challenges and needs for quality Cyber Security education for professionals. Then, this document establishes a framework for Cyber Security professional categories, and a scale for assessing the skills and skill levels for a category in the framework. The end goal was to have good educational resources for the people wanting to learn about Cyber Security and some form of criteria that people can present as evidence of their qualifications for positions relevant to Cyber Security.
The framework is based on the CS4E Task 6.1 framework and on other common frameworks that have been proposed in the field of Cyber Security. In order to enhance the framework applicability and build relevant and wide-ranging job profiles for the framework, four specific use cases with twelve scenarios are presented. The skills required in each of these scenarios is evaluated. Related job profiles are derived from these scenarios, and what is their average Cyber Security skill level required in each of the scenarios is evaluated according to a four-step skill rating scale. From the scenario evaluations, we can conclude, that the main needed skills in scenarios are Data Integrity and Authentication, Access Control, Secure Comminication Protocols and Usable Security and Privacy. Less required skills are related to Cryptanalysis, Design, Component Procurement and System Thinking. In general, most scenarios require rather broadly various Cyber Security skills.

Even though skill requirements related to the scenarios represent the scenario writer's point of view, we can draw some conclusions: because the variance of required skills can be vastly different depending on the role, general Cyber Security programs targeted to a certain work environment might be useful to some extent, but to efficiently bring value, there is a need for well-justified and customized skill education for a certain professional group. Also, analysis of a scenario of this kind, in the form of standard and easily comparable table framework, may help point the breadth of required skills. The framework can help visualize highly relevant Cyber Security skills that can be difficult to discover otherwise. For instance, when considering Cyber Security education offering in general for IT professionals, usability skills might often be overdriven by technical skills, but the skill *Usable Security and Privacy* is required in many of our scenarios on an advanced level. In addition, this kind of illustration reveals overlapping in education needs, and may help combine different target groups when arranging Cyber Security education.
After that, all the distinct profile descriptions' all required skills are rated according to a four-step skills rating scale via 6 internal to the project expert evaluations. From these ratings, an average figure is constructed for each of the profiles. As a special case, a customized framework targeted to lawyers is presented, representing how the framework could be easily applied in a certain profession context.
From the framework skill assessment we can conclude, that the most demanded skills are in a declining order Personal Data Protection and Privacy, Secure Communication Protocols, Data Integrity and Authentication, Data Privacy and Access Control. The most demanding profiles are

Digital Forensic Analyst, Chief Information Security Officer, Security Operations Centre Manager, Information Security Officer and Software Engineer, whereas the most demanded skill categories over all profiles are Human Security, Data Security, Societal Security, Connection Security and Organizational Security. It should be noted that since the number of evaluations is relatively low all the results are only indicative and may be slightly biased. To strengthen the result credibility, future work will improve the result validity with surveys and using relevant expertise to further validate the skill ratings with a larger audience. The evaluations via our framework presented here and strengthened at later phases help organizations resolve, what kind of skills education offerings mostly would benefit their professionals.

Document information

Contributors

Name	Partner
Anni Karinsalo	VTT
Kimmo Halunen	VTT

Reviewers

Name	Partner
Chan Nam Ngo	UNITN
Christos Douligeris	UNIPI
Marco Angelini	ENG
Natalia Kadenko	TUD
Fabio Massacci	UniTN
Pierantonia Sterlini	UniTN
Peter Hamm	M-CHAIR
Narges Arastouei	M-CHAIR

History

Version	Date	Authors	Comment
0.01	2019-03-28	Kimmo Halunen	1st Draft

0.1	2020-10-12	Kimmo Halunen, Anni Karinsalo	2nd Draft
0.2	2020-11-30	Kimmo Halunen, Anni Karinsalo	Internal Review
0.3	2020-12-14	Anni Karinsalo	1st Review
0.4	2021-01-15	Anni Karinsalo	2nd Review
1.0	2021-01-22	Anni Karinsalo	Updated version, 3rd review
1.1	2021-03-04	Anni Karinsalo	3rd Review
1.2	2021-03-24	Anni Karinsalo	4th Review
2.0	2021-03-25	Narges Arastouei	Final version and improve some minor points to be submitted

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**ACM**	Association for Computing Machinery
	AIS SIGSEC	Association for Information Systems Special Interest Group on Security
C	**CyBOK**	Cyber Security Body of Knowledge
E	**ECSO**	European Cyber Security Organisation
	ENISA	Acronym 3
I	**IFIP**	International Federation for Information Processing Technical Committee on Information Security Education
	IEEE CS	IEEE Computer Society
J	**JTF**	Joint Task Force on Cyber Security Education
	BCD	Acronym 3
K	**KA**	Knowledge Area (in CyBoK)
	KSAs	Knowledges, Skills and Abilities (in NIST NICE)
M	**MOOC**	European Cyber Security Organisation
N	**NICE**	National Initiative for Cyber Security Education
	NIST	National Institute for Standards and Technology

1 Introduction

The need for Cyber Security education, and the need for describing the required Cyber Security skills in work has been identified by many organisations both at a European and at a global context (ECSO2020, NICE2020). The shortage of skilled Cyber Security professionals will pose a risk for security, people, organizations, and society.

CyberSec4Europe (CS4E) is one of the 4 EU-funded pilot projects for the forthcoming European Cyber Security Network and Centre. In D6.2 of CyberSec4Europe, an analysis of the different Cyber Security-related skills and offerings from the university sector were provided. As D6.2 provided information about constructing framework for academia, we can use it as an example and information source when constructing a framework for professionals. However, the context and thus point-of-view is different between academia and professionals. In order to design a proper education framework for professionals, as defined in T6.2, we need to identify relevant profiles for Cyber Security professionals, the skills these profiles require, and the level of skill that these profiles require. After that we are able to know the relationship between the specialization and the (required) skill levels related to the specialization. Thus, we will know the needs of a certain specialization, and the right kind of education can be targeted to a certain specialization, or profile (profiles will be defined later in this document).

In this deliverable, we build a framework presenting the relevant specialization Cyber Security domains with the related capabilities and skills (in terms of knowledge areas and knowledge units) from an organizational point of view. We will validate the required level of the skills per profile by conducting an expert evaluation in organizations. As a basis for this, a categorization from the CS4E D6.2 is utilized. In addition, most of the used European and global frameworks in the field of Cyber Security professional categorization are studied and summarized. From this study, relevant structures for our point of view are gathered that lead to the construction of our proposed framework.

The results from the expert evaluation will be delivered to the European Commission and will help shaping the future of Cyber Security education in Europe. The results will also be used to form a Cyber Security skills framework as a part of the project.

1.1 Methodology

This study utilized the following structured phases:

- Analysis of relevant frameworks
- Analysis of the required framework structure
- Building of the profiles according to use cases and scenarios
- Analysis of the profile skill importance by collecting and summarizing expert evaluations according to a rating scale

1.2 Structure of this document

This document is structured as follows. Section two presents a brief overview of the most relevant existing frameworks and finds out challenges and needs for quality Cyber Security education for professionals. Section three presents use cases and related scenarios, of which the profile descriptions are derived from.

Section four describes our framework and section five analyses skills' importance based on the framework. Section six concludes the work.

1.3 Purpose of this document

This document presents the work of Task 6.2 until January 2021 in the Cyber Security for Europe project. The deliverable shortly reviews existing Cyber Security frameworks and identifies challenges and needs for quality Cyber Security education for professionals. In addition, we propose our own framework which is founded on the skills taxonomy that was presented in an earlier deliverable (D6.2, Education and Training Review). Through the different use cases and scenarios, we have identified a list of Cyber Security professionals specializations. For each specialization, different skills (from the taxonomy) levels has been evaluated and the results are reported in this deliverable and the corresponding Framework description.

2 Cyber Security Education: existing frameworks, training materials and needs

2.1 Frameworks

In the following we present relevant frameworks in the context of Cyber Security.

2.1.1 NIST NICE

The National Initiative for Cyber Security Education (NICE)[1] is a partnership between government, academia and industry into creating an ecosystem for education, training and workforce development of Cyber Security professionals. NICE is led by NIST. The main purpose of the NIST NICE framework (NICE2020) is to describe the work tasks of a Cyber Security professional. To achieve this, the framework uses a structure which consists of seven Categories divided in 32 Speciality Areas, that are further divided into Work Roles. Work Roles include Knowledge, Skills and Abilities (KSAs) and Tasks.

The NICE framework besides defining the task descriptions, offers a thorough approach into defining the Cyber Security workforce needs. First of all, it offers a lexicon that all stakeholders (educators, trainers/certifiers, employers and employees) can use to prevent misunderstandings. Also, the NICE framework helps defining KSAs and tasks that are relevant for each Work Role. In addition, it presents a proficiency analysis that will help define an organization's expectation of the level for positions (comprising often of more than one role). In the NIST NICE framework, the mapping between needs of professionals and education provided by different entities is extensive and the number of different skills is vast.

2.1.2 The Cyber Security Body of Knowledge

One of the most comprehensive frameworks on the Cyber Security discipline is the Cyber Security Body of Knowledge (CyBoK), which covers most aspects of Cyber Security in a very good level of abstraction. In addition to the report and document, the website[2] contains a lot of information and videos that explain the material. The CyBoK is also open for amendments and changes and is updated accordingly.

In CyBoK, Cyber Security is divided into 19 Knowledge Areas (KAs). These are grouped under five categories and are a very good summation of the different aspects of Cyber Security.

In the development of an education and professional framework, these KAs need to be addressed. The question is, how to choose the various needs of different professionals and how to map the education provided by different entities to these. Compared to NIST NICE, which has an extensive mapping, a similar effort is analysed in CyBoK with a mapping between common Cyber Security terms and the KAs (CyBoK 2020).

2.1.3 ACM/IEEE/AIS SIGSEC/IFIP (JTF) Cyber Security Education Framework

The Joint Task Force (JTF), consisting of ACM, IEEE, AIS SIGSEC and IFIP, concentrates via its framework (CSEC2017) on developing undergraduate degree programs in the computing disciplines of Computer Engineering, Computer Science, Information Systems, Information Technology and Software

[1] https://www.nist.gov/itl/applied-cybersecurity/nice
[2] https://www.cybok.org

Engineering. In addition to that, its education platform[3] offers education capabilities for professional computer technology-related learning.

The Cyber Security Education Framework recognizes 8 Cyber Security Knowledge Areas that are further divided into several Knowledge Units. The JTF Framework also presents Topics for each Knowledge Unit, as well as a description of the guidance, and Essentials and Learning Outcomes for each of the Knowledge Areas. The identified Knowledge Areas are the following:

1. Data security
2. Software security
3. Component security
4. Connection security
5. System security
6. Human security
7. Organizational security
8. Societal security

The JTF framework is targeted more towards academic students of post-secondary degree programs, and as such is not directly applicable to engineering professional Cyber Security education. However, the framework establishes interesting ideas to enable learning, such as *essential concepts*, which means basic skills for each Knowledge Area, as well as an initial concept of a *roadmap*. The JTF's components for coursework are described as the following process:

1. Provide a rationale for knowledge and its importance for the specific work role.
2. Identify and describe relevant courses and course modules.
3. Outline strategies for obtaining the knowledge when specific courses are not available or accessible within the institution.
4. Highlight challenges (and associated strategies to overcome them) to following the suggested course of study.

2.1.4 The CS4E D6.2 Framework

The development of the framework in D6.2 is based on a comparison between the ACM framework (see 2.1.3) and the NICE framework and finding any overlapping. Then, the decision was made to adhere slightly more to the ACM framework terminology, because of being more scientifically oriented, whereas the NICE framework is more focused/targeted on workforce skills. However, because of the similarities, the end result includes the key ideas of NICE as well. Despite the different target groups of the framework of D6.2 (education/academia reference group, whereas our reference group is professionals/workers), we conclude that we can use it as a base work in our framework as well. This is because the developed framework in D6.2 covers also key ideas used in NICE that would be relevant for our target groups.

2.1.5 Framework by ENISA

In its report (ENISA 2019), ENISA is recognizing the need for professional workforce development, by establishing as a recommendation the need to "design a comprehensive Cyber Security workforce development strategy". ENISA is acknowledging its role here as the "community builder" and "making sure all stakeholders needs are addressed". Also, as to balance the efforts targeted to offering higher education

[3] https://learning.acm.org/

of students, ENISA clearly implies that "more is needed to create a virtuous cycle that guarantees a good match between workers' supply and labour market demands. Hence, employers should be fully integrated in the development of a Cyber Security workforce and their role should be clarified". (ENISA 2019)

Also, ENISA will develop a European Cyber Security Skills Framework. In the meantime, ENISA has created the Cyber Security Higher Education Database, an interactive list of Cyber Security degrees in EEA countries and Switzerland. The Database aims to become the main point of reference for all European citizens looking to upskill their Cyber Security knowledge and skills through a higher education degree. With it, citizens should be able to make more informed decisions about Cyber Security education and training, choosing the degree that is most suitable to their needs.

To advance these goals, ENISA will also be establishing an Ad-hoc Working Group[4] on the European Cyber Security Skills Framework. The scope of the Working Group is to advise and aid ENISA in developing a European Cyber Security Skills Framework, enabling a common understanding of the roles, competencies, skills and knowledge used by individuals, employers and training providers across the EU Member States. Furthermore, it could also raise awareness by identifying the gaps in the Cyber Security landscape that can be bridged with the creation of the framework.

2.1.6 CONCORDIA European Cyber Security Competence Framework and Map

The CONCORDIA project aims to establish a Cyber Security Competence Network with leading research, technology, industrial and public competences by means of a user-centric EU-integrated Cyber Security ecosystem for digital sovereignty in Europe. It will be co-operating for example with ENISA, as implied in one of CONCORDIA project's main objectives[5] "Position the CONCORDIA ecosystem, a Cyber Security Competence Network with leading research, technology, industrial and public competences to build the European Secure, Resilient and Trusted Ecosystem, with the CODE research center[6] as coordinator and hub, and ENISA as secretary". CONCORDIA will be establishing a Cyber Security Maturity Assessment framework[7] for standardizing the evaluation of the Cyber Security posture of organizations and to facilitating Cyber Security assessment and audits according to different maturity levels.

2.2 Training materials

In this section, we discuss the training materials in the context of Cyber Security, and present a case depicting the need for training in banking sector.

2.2.1 MOOCs and other methods of education delivery

D6.1 draws a conclusion of European-level MOOCs available both from the academic and non-academic side. MOOCs are online courses, where the course material is publicly available for everyone to use. Conclusion is, that most of the online courses related to cyber range capabilities and continuous learning are offered by academic institutions, but they are not publicly available outside academic world, thus they are not classified as MOOCs. Especially MOOCs related to cyber range capabilities do not actually exist. It is clear, that there is still a great lack of cyber range MOOCs both in academic side and non-academic side.

[4] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls
[5] https://www.concordia-h2020.eu/home-2/objectives/
[6] https://www.concordia-h2020.eu/consortium/research-institute-code/
[7] https://www.concordia-h2020.eu/blog-post/a-novel-cybersecurity-maturity-assessment-framework-cmaf/

In the commercial side, there is a need to pay attention to the quality assurance criteria, with regard to course content being biased and course admission and evaluation being fair and transparent. One notable issue is that MOOCs platforms and channels are hardly ever European, which leads to issues regarding GDPR and privacy.

2.3 The need for quality education

In the following, we will analyse the need for quality education for Cyber Security professionals and present real life conclusions of training adequacy in a case from banking sector.

2.3.1 Challenges of and the needs for quality education for professionals

Cyber Security is a highly interdisciplinary field of study. Specific degree programs are often associated conceptually and practically with one of the established disciplines in a way that has a significant effect on the fundamental identity of the program. One of these degree programs, the Cyber Security Curricula 2017 report, known also as CSEC2017, became public in 2017. The report recommends security in eight areas to include data, software, component, connection, system, human, organizational, and societal. The CSEC2017 mission was to develop comprehensive and flexible curricular guidance in Cyber Security education that would support future program development. The aim was also to produce a curricular volume that structures the Cyber Security discipline and provides guidance to institutions seeking to develop or modify a broad range of programs.

The report explicitly states that there is a broad spectrum of Cyber Security jobs from technical (such as cryptography and network defense) to managerial (such as policy and regulatory compliance) positions. At the same time, it also recognizes that every graduate of a Cyber Security program requires both technical skills and business acumen, essentially a managerial understanding of the organizational actions needed to ensure system-level security. A degree in Cyber Security prepares graduates for a broad range of application areas, including public policy, procurement, management, research, software development, IT security operations, and enterprise architecture.

The need for specialized abilities, that Cyber Security graduates should have, is becoming apparent every day. Continuous challenges of various types face organizations around the world who must secure data regarding their customers. Solutions that secure organizational data are multidimensional ranging from highly technical to organizational policies and societal legal and regulatory responses, creating a significant need for professionals with a broad range of specialized security expertise combined with the generic individual foundational abilities (such as problem solving, critical thinking, oral and written communication, teamwork, negotiation) that all computing professionals need.

Gaps analysis in frameworks has been done by ECSO (ECSO2018, ECSO2020). Their analysis contends that there is a skills shortage and the short term fixes or “patches” are not going to work and produce the necessary results. The long term goals identified in the report are:

- Creating the foundations for a truly interdisciplinary understanding of the subject area;
- Universities need to ensure they do not lose academic values (such as critical thinking);
- Cyber Security aspects shall be integrated in educational curricula (not just IT related);
- Professionals shall be able to certify their knowledge.

The fourth part is somewhat problematic, although certifications do exist. One concern is that the globally acknowledged certifications are heavily US centred and do not reflect all the aspects that European professionals need. Many European certifications are only national and thus are not necessarily applicable in other states than the one awarding the certification.

Another findings from ECSO (ECSO2020) relate the need for improving Cyber Security education of professionals in several areas. First of all, there is a need for Cyber Security exercises and awareness, in terms of defining a common regulation for Cyber Security exercises across Europe. Second, competences and certifications should be in place, especially for Cyber Security professionals: common and recognized Cyber Security certifications should be a must-have for working in the sector and be globally acknowledged. Third, competence should be built by Cyber ranges. Cyber ranges should be an integrated part in the digital competence building programs within Europe, both in high level education and training sector, providing the hands-on knowledge base for the participants. Cyber ranges should help the targeted skills and competence development of the participants along with the extended thinking when approaching IT infrastructures and functions. Simulation based competence building should be easy to integrate into existing educational and training curricula. (ECSO2020)

In ECSO, WG5 has analysed the professional certification landscape (WG5ANALYSIS). They have similar findings as mentioned above. First of all, they propose an European-level market study regarding the age structure and career history, training paths and industry demand of Cyber Security professionals. Also, an European-level certification scheme with related baseline requirements should be developed, enabling the offering for accreditation services. In addition, an European-wide education framework for Cyber Security should be developed. In both the certification scheme and framework, representatives for existing initiatives at national level should be involved. Education framework should co-operate with related parties such as NIST, and be generally accepted on an international level.

What can be the expected as a benefit and/or impact and what can be achieved is first of all increased awareness and increasing number of Cyber Security professionals. Second, increasing awareness can reduce cyberattacks and their impact both in economic terms and consumers' trust, thus the outcome will be a more secure and reliable European ecosystem. Third, ensuring a new and prepared generation of cyber specialists is necessary for maintaining and increasing the Cyber Security maturity level of the sector. Fourth, a regulatory Cyber Security framework applied to all players (EU and non-EU working in EU) reduces uncertainty, ensures comparability and allows competitive solutions on a global basis. (ECSO2020)

2.3.2 Training adequacy: real life results in banking sector

As an example of training adequacy, a case regarding banking sector is discussed. In this case description, based on the results of the annual survey realized in 2020 by CERTFin, we depict the way banks are performing regular and adequate training sessions towards customers and personnel. The Fraud Report, addressed to members of the CERTFin's Constituency, aims to broadly analyze the landscape of fraudulent activities which have affected the Italian Banking Sector in the past year. The analysis is not limited to show how threats are evolving but also investigate the related impacts on customers, as well as technical and organizational attack aspects inherent to the organizations involved directly or indirectly.

2.3.2.1 Actions towards Retail and Corporate segment customers

The correct and conscious use of banking tools requires communication with their own customers to share updates and recommendations on the correct use of the devices and on good behavioral practices in credentials management and payment tools.

Customers are periodically informed about various issues, ranging from the correct use of devices to carry out remote banking transactions, to good practices in managing credentials and passwords.

Among the various topics examined (Figure 1), the most shared with customers remain the management of identity and the security tools to protect banking services (95%), security in the use of payment instruments (74%), e-mail (68%) and devices when connected to the Internet (63%). Additional information areas

concern the safe use of mobile devices (58%), the risks associated with e-commerce (47%), money muling and social networks (both reported by 26% of respondents).

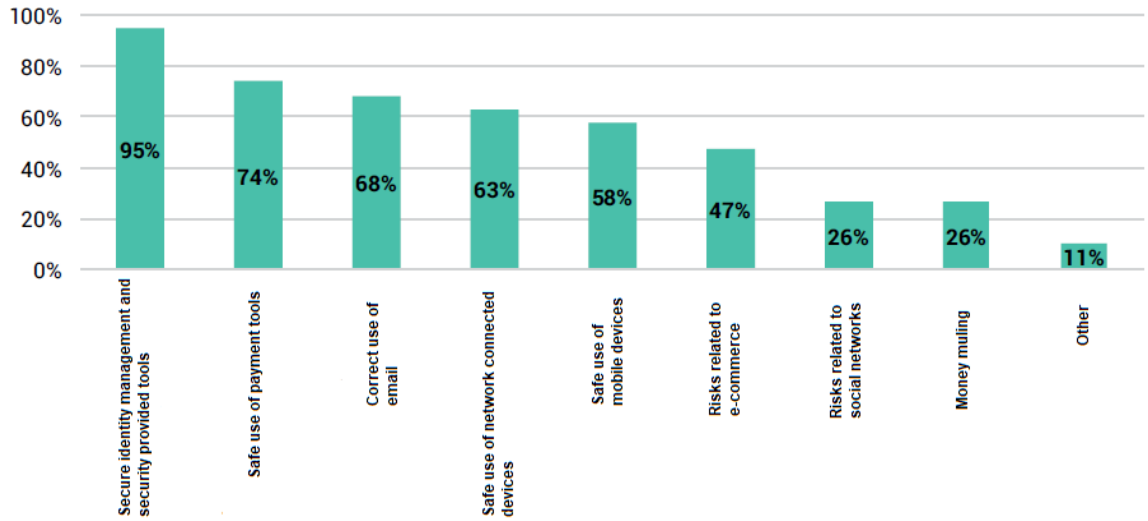

Figure 1: Cyber Security and fraud issues faced with Retail customers

As for **Corporate customers**, the topics covered do not show particular differences regarding the awareness Retail and Corporate (Figure 2): the most discussed are issues of secure identity management (87%), security in the use of devices connected to the network (73%), the secure use of payment instruments (67%) and the correct use of e-mail (60%). The information offer is completed with topics related to the risks associated with e-commerce (53%), the safe use of mobile devices (47%) and social networks (33%).

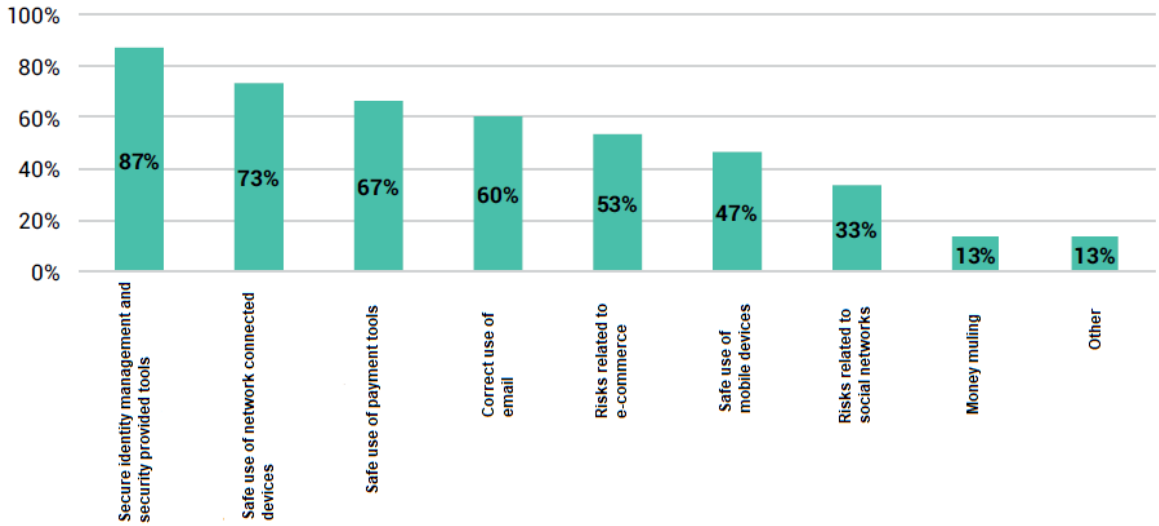

Figure 2: Cyber Security and fraud issues faced with Corporate customers

2.3.2.2 The bank's internal law enforcement actions

Many attack mechanisms rely on the human factor as an element of vulnerability through which useful information are collected for the implementation of malicious operations or intrusions in computer systems, using increasingly advanced and sophisticated procedures combined with **social engineering** techniques. For this reason it is essential to implement **training and awareness initiatives** not only for customers, but also for internal staff.

The data collected show a **growth in training activities for bank employees** (Figure 3), which involved all professional families. In particular, in 2019 the actions were spread to the entire organization, albeit with greater attention to specialist security personnel (89%), Top Management and Contact Center personnel (both 83%), which have grown significantly compared to the previous survey. Then follows the training of the Back Office (78%) and branch personnel. Other Help Desk functions continue to be involved in training in percentages that are always higher than 50% of respondents.

The **main topics covered** in the training courses include the following topics:

- Cyber Security
- Fraud and risks associated with electronic payments
- Correct use of company tools
- Security Awareness
- Correct online behavior and incident management

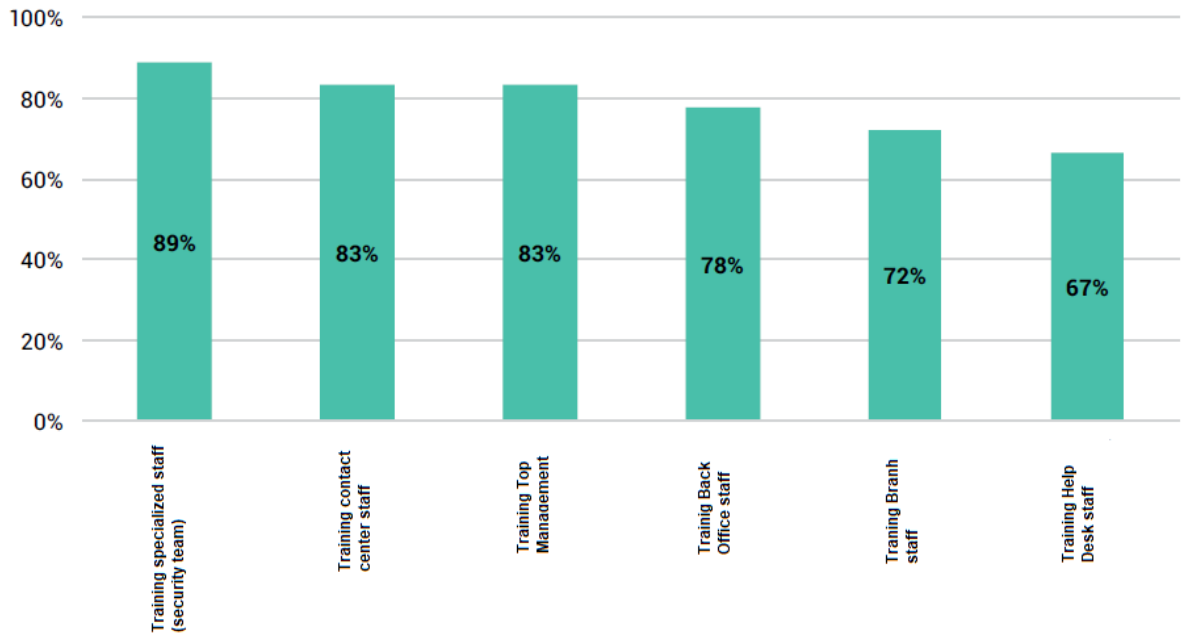

Figure 3: Internal training activities on Cyber Security and fraud issues

As usual, **in-house training**, in addition to **classroom sessions and in-depth courses**, was **also conveyed through** the publication on the company intranet of **bulletins and news** relating to the main general safety phenomena and topics, precisely with a view to raising awareness in a widespread manner all banking staff.

2.3.2.3 Considerations

In conclusion, the training mentioned above is **not to be considered inadequate**, as such training sessions are being held periodically by the banks. Cyber exercises and Red Teaming sessions should be organized in order to support the banking environment resiliency.

3 Use cases and scenarios

Identifying Cyber Security needs and requirements of a certain work profile will be an easier process when we describe the narrative of typical functions and events occurring related to the profile. Another way to describe the work characteristics is or recognize the challenges of the environment, namely Cyber Security threats typically faced in this environment, thereby understanding the level of Cyber Security knowledge that is required to overcome these threats. In the following, four specific use cases that include distinct scenarios are described by CS4E partners. The structure of the use cases and scenarios is illustrated in Table 1. The abbreviation between the parentheses is used further in the Tables 2 and 3 for the sake of readability to describe these scenarios when applying them with our framework. The purpose of the scenarios is to describe typical schemes of different professions, where focal actors, functions, needs and requirements in the field of Cyber Security professional education can be derived. From these scenarios, we construct the profile descriptions, that shall be representing the essential work profiles in the framework, and assessed according to their required skill level in each skill category.

Table 1. Use cases and related scenarios for the framework

Use case	Scenarios				
1. *Federated IdM scenarios on Public Sector*	Data Protection Lawyer in University (DP)	Security Certification Agent in University (SC)	Security Trainer in University (ST)	Network Administrator in University (NA)	IoT Security Manager in University (IS)
2. *Open Banking and Revised Payment Service Directive*	Ensuring Integrity and Confidentiality 1 (IA)	Ensuring Integrity and Confidentiality 2 (UI)	Ensuring Integrity and Confidentiality 3 (UE)	Ensuring Legitimate Access (CL)	
3. *Security-enhancing Platforms*	Security Intelligence (SI)	Cross-Border Authentication (CB)			
4. *Assessment mechanisms for non-ICT workforce (lawyers)*	Cyber Security for Lawyers (CS)				

3.1 Use Case 1: Federated IdM scenarios on Public Sector

The scenarios related to Use Case 1 describe professionals in the context of working in University. It must be noted, that while the working environment is academic, the profiles represent professional point-of -view, such as “network administrator”, not academic point-of-view, such as “student” or “lecturer”.

3.1.1 Background: Current professional training of the selected profiles at the University

The University of Murcia selected five specific profiles (scenarios) that are considered especially important for the security of an organization: data protection lawyer or consultant, security certification agent, security trainer, network administrator and IoT security manager. While each profile may come from different studies, for example the data protection consultant can be a lawyer with a data protection specialization or a computer scientist with a lawyer specialization, they all share a common need for Cyber Security knowledge to correctly develop their role.

The current curricula at the Computer Science faculty of the University of Murcia includes in the first course of the Bachelor degree, a subject of Management of Organizations and Professional Skills, where especially the external profiles (consultant, certification agent and security trainer) will be able to acquire valuable knowledge and basic skills for their development in a company, to acquire social abilities, and where they will be able to understand its operation. In this first course, the profiles also learn the basic internal operation of the computer, crucial to understanding certain types of attacks such as buffer overflow. In the second course, the profiles start to learn how the network works, its basic functioning, and the protocols TCP/IP. They also study how to manage an operative system in a semi-advanced way. The third course goes beyond, and it has a high degree of subjects related to networks and security. The previous subject of networks is further developed in this course, so that the profiles can study advanced network management, router configuration and routing protocols, which is really valuable for the network administrator profile and even for the IoT security manager. This knowledge is also expanded with the study of the main telematics services at the application level and the introduction to security in systems (mechanisms such as certificates, digital signature, secure protocols, etc.). In relation to the quality of the software and its development, some subjects include methodologies to correctly design software and avoid vulnerabilities, as well as tools for managing the functional and security requirements. Finally, the fourth course is divided into several specializations, in which, depending on the chosen specialization, the students can learn concepts related to embedded systems and wireless networks, useful for the IoT security manager profile, virtualization and advanced network administration, for the network manager profile and software quality, quality standards and testing for the certification agent profile. Furthermore, one of the specializations includes a subject totally dedicated to security, integrating concepts such as firewall, malware, pentesting, most common attacks, intrusion detection, data security and risk management. This subject is especially useful for all the profiles considered, as it addresses a wide variety of basic security concepts.

The Computer Science faculty also offers a Master degree in new technologies of computer science, in which the students can deepen their knowledge, as well as acquire new one related, for example, to the security of distributed systems, new generation networks, IoT, cryptography and system modeling, from the mathematical point of view. In this case, the consideration of closed specialties limits the student's choice to a particular branch of the computer science education.

In general, the teaching covers certain profiles such as network administrator very well, while others such as IoT security manager or data protection lawyer are not fully developed. This fact, together with the closed specializations of the master and the fourth year and the fact that in joint degrees such as mathematics and computer science, it is not possible to study optative topics, further undermines the fundamental knowledge of Cyber Security of these profiles and the possibility of developing specific professionals. The knowledge that students can acquire is limited by these specializations, limiting the creation of more heterogeneous and interdisciplinary profiles.

The first profile, data protection lawyer or consultant, ends with a basis about what is privacy and some mechanisms to guarantee it, but this profile does not learn anything about regulation, policies, intellectual property, ethical norms and laws. Moreover, human and societal security is, in general, a topic that is not discussed in any subject. This profile can come from a wide array of educational backgrounds, and the experience suggests that much of this knowledge area’s content will be novel to those whose education is based in science, technology, engineering, mathematics, many social sciences, and many of the humanities.

The second profile, security certification agent, which is quite related to the first one, experiences the same problem. There is no training on regulation and standards, so this profile will see such topics for the first time when studying a specialization. Although in the bachelor degree some subjects of project management and organization management are taught, they do not delve into organizational security. Another deficiency in this profile is the fact that nothing related to risk assessment is studied, beyond software testing and requirements elicitation, limited at software level. The use of advanced testing tools or risk estimation tools and evaluation methodologies is not studied. With the third profile, the same happens: a security trainer needs a basis of Cyber Security, which is more or less covered, but some important aspects such as the human security are not even mentioned (e.g., social engineering, human errors or usable security). How to catch people's attention and convince them security is worth the engagement and how to support the acquisition of skills by letting people practice the skills in a setting where they can 'experiment' with security decision-making and reflect on their perceptions and biases are social abilities that are not developed in the bachelor degree. In general, this profile requires a set of skills that have traditionally not been part of the training provided for security experts and practitioners. The fourth profile, network administrator, is quite aligned with the objectives of the Bachelor of Science in Computer science. The main concepts are taught in the second and third year, and the student can do the specialization in networks. However, there is still some lacks on risk and incident management, as well as on IoT security, as they are the most common devices that are connected to the network, and the weakest point of entry to the network. Finally, the fifth profile, IoT security manager, as a relatively novel profile is quite forgotten. The subjects related to the security of IoT devices are practically non-existent. Thus, this profile will need to learn through other specializations knowledge about Cyber Physical Systems (CPS), its characteristics, crosscutting security, the different application domains, programming of IoT devices, main attacks associated to IoT, security mechanisms to prevent them, etc. Moreover these devices usually operated with personal data, so an education in privacy and data protection mechanisms is also important to complete this profile.

In conclusion, these profiles manifest a profound lack of education in standards and regulation, as well as in societal and human security. In addition, certain aspects such as security in IoT are not sufficiently developed as it is a relatively new paradigm that has gained importance with the arrival of 5G. Risk management, its evaluation and the different testing mechanisms are only seen at the software level, so aspects as important as dependencies between components and their implication in risk estimation go unnoticed. Finally, although basic Cyber Security concepts are taught, all profiles will need to deepen this knowledge to achieve adequate training for their work.

3.1.2 Scenarios for the roles in University: detailed description and importance of the roles

On the one hand, the first and second profiles and possibly third profile are considered externals to the organization, and they are meant to be consulted when an organization needs support about a specific topic (e.g., GDPR, standards, regulation, etc.) and when an organization needs an accreditation of its security. On the other hand, the rest of the profiles are intended to be internally in the organization, working directly to support and manage the security of the different systems, as well as the education of the personnel. In combination, these profiles provides a clear vision that the security of an organization depends on many professionals, both internal and external, that are focused on many different aspects, not only in systems but also in people.

First scenario: A data protection lawyer is defined as a person (or team) in charge of assess a client (e.g., manufacturer, organization) about the compliance of the General Data Protection Regulation (GDPR), in order to ensure that the products are in line with it. This role is especially important with constantly evolving regulations and allows an organization to forget about being up to date with these changes and to focus on the development of its activities. However, an organization cannot directly ignore the different regulations

existing in the countries where it is going to carry out such activities or in which it is going to sell or develop its products. A lack of knowledge on its part can lead to heavy fines and a damaged reputation, at the very least. That is why this role becomes even more important, not only to avoid major problems in a company, but also to ensure that the law is fulfilled and that the privacy of each individual is preserved.

Second scenario: The second role, **security certification agent**, is quite related with the previous one. A security certification agent is meant to be a person, team or entity in charge of evaluating the security of a system according to a specific certification scheme, processes and standards. In this case, the company does not have the obligation to follow a certain standard, since it is not a regulation, but the fact of certifying that its processes and the products developed meet certain quality criteria directly impacts its reputation. A customer will have a better opinion of a product that has been certified, for example, to accredit an adequate level of security, which will increase the value of that product. Although a company can self-certify, understanding the processes, standards and being able to be critical with its own activities and its management is complicated and requires a high amount of time. At this point, the role of the certification agent is essential to ensure that all processes are carried out correctly, the products have the appropriate quality and to detect deficiencies and vulnerabilities that could be overcome. In addition, it is important to mention that an external certification, although more expensive, will always be more reliable at the eyes of the buyer than a self-certification.

Third scenario: The third role, **security trainer**, can be understood as an external or internal role. This role is defined as a person in charge of training personnel of an organization to be aware of the security concerns and to train them on how to avoid security issues. The security of an organization heavily depends on the security education of the personnel. The majority of the attacks performed in big organizations start with social engineering: a malicious mail, phishing webpages, impersonation, etc. It is critical that the staff of a company is aware of the risks to which they are exposed to, that they know how to recognize them and act against them, so as not to compromise the security of the entire system. The mission of this profile is important, but at the same time complicated, since it must transmit knowledge in an appropriate way to people without Cyber Security knowledge. These people often resort to tools such as group sessions, presentations, cyber ranges, flagships and other techniques, depending on the organization domain, in order to liven up education while practicing the required skills.

Fourth scenario: The fourth role is considered internal to an organization. **A network administrator** is a person in charge of configure and manage the network components in an organization (security, identity, configuration, application of countermeasures). This person is also in charge of updating the firmware of the components. Therefore, this person has a fundamental role in ensuring the security of an organization's services. The task of a network administrator is based on guaranteeing the operation of all resources at the network level, providing and configuring the components and communications necessary for said operation while maintaining an adequate level of security. Of course, this role requires very technical knowledge that allows them to carry out their work, but it also requires communicating with staff, adapting the network services to emerging needs, solving technical problems and doubts, and being able to understand and be understood. Another fundamental aspect of this role is the management of the network resources and services throughout the entire life cycle. He must not only adapt the network to new needs, but also ensure that all components and systems are kept up to date to avoid possible threats.

Fifth scenario: Finally, the **IoT security administrator** has been considered an emerging role due to the proliferation of this type of devices in organizations, and moreover after the arrival of the 5G. These devices have special needs and cannot be treated in the same way as the other components of the system. Thus, the IoT security administrator is the person in charge of managing the security of the IoT devices that are part of the system (configuration, protocols, security changes, communications, information shared, reassessment, vulnerability database consultation, etc.). These devices, usually considered constrained and cheap, do not usually have a high security associated, since manufacturers tend to save costs in this regard. Some of the most famous and shocking attacks, such as the Mirai IoT botnet, used this type of devices as

the entry point to the system. It is absolutely essential that there is a professional dedicated to protecting these devices while protecting the network where they are going to enter, limiting their communications, for example, establishing access control security policies, but also guaranteeing updates and managing threats that may arise during their operation.

3.2 Use case 2: Open Banking and Revised Payment Service Directive (PSD2)

Use case 2 includes scenarios related to Open Banking and Revised Payment Service Directive.

3.2.1 Introduction

The Revised Payment Services Directive (PSD2) is a EU Directive (2015/2366) to regulate payment services and payment service providers throughout the European Union (EU) and the European Economic Area (EEA)[8].

PSD2 revises the original Payment Service Directive, the EU directive (Directive 2007/64/EC) that provides the legal framework within which all payment service providers must operate, with the aim of promoting financial service competition through the participation of non-bank entities in the payment industry, enriching the European open banking field.

3.2.1.1 Open Banking

Open banking (or 'open bank data') is a practice that provides third-party financial service providers open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions through the use of application programming interfaces (APIs).

It is part of a general movement related to the changes of attitudes in the data ownership, which involves regulations such as GDPR and concepts such as the open data movement. In this light, banks are substituted by a more abstract concept of financial service platforms, which can involve banks but also different entities. Banking itself becomes a service, not necessarily instantiated through a bank entity.

3.2.1.2 PSD1 framework

The original PSD contains two set of rules

1. **Market rules** section indicates possible actors like credit institutions (banks), financial authorities (e.g. central banks, government bodies), electronic money institutions (EMI -E-Money Directive in 2000), and Payment Institutions (PI). Particular attention to the latter, which is specifically introduced by the directive. The role of PI can be impersonated by third party organizations, i.e. neither credit institutions nor EMIs. PSD states necessary PIs capital and risk management requirements and possible scope of action; a PI can be established in any EU country and then pass (passport in PSD terms) their payment services into all other EU member states without additional specific PI requirements.
2. **Business conduct rules** dictate payment service institutions requirements in terms of information on service parameters and costs. For example, they must make available any charges, exchange

[8] https://en.wikipedia.org/wiki/Payment_Services_Directive

rates, transaction references, maximum execution time. This section also explains PIs, users rights and obligations (e.g. refunds on payments).

Each country had to designate a supervision authority to monitor compliance with business conduct rules, according to national legislation.

3.2.1.3 PSD2 framework

The European Parliament adopted the revised Payment Services Directive (PSD2), in October 2015. PSD2 went into effect on 14 September 2019, but EBA allowed for a time extension of the strong customer authentication (SCA) until 31 December 2020 due to non-ready implementations.

The new rules aim to promote the development and use of innovative online and mobile payments through open banking. The revised directive aims for harmonization of the rights and obligations for payment providers and user, as well as increase consumer security, for example by emphasizing strong authentication.

3.2.2 PSD2 Technical overview

From a technical perspective, the most relevant parts of PSD2 are related to the provisions on Strong Customer Authentication (SCA) for online payments[9], supported by more stringent common and secure communication (CSC) requirements.

Strong customer authentication indicates authentications based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses), and inherence (something only the user is). The adopted elements must use different channels, so the breach of one does not affect the others, and they must protect the confidentiality of the authentication data.

PSD2 demands eIDAS-defined qualified certificates for website authentication and electronic seals for communication between financial services players. The technical details are defined in the standard ETSI TS 119 495 which implements these requirements, also in accord to the EBA RTS[10], which details the security measures related to Third Party Payment Service Providers (TPP) account access and to SCA.

PSD2 defines new services to be operated by TPP on behalf of a Payment Service User (PSU). These new services are:

1. confirmation on the Availability of Funds Service (FCS) to be used by a Payment Instrument Issuing Service Provider (PIISP) TPP as defined by article 65;
2. Payment Initiation Service (PIS) to be operated by a Payment Initiation Service Provider (PISP) TPP as defined by article 66 ;
3. Account Information Service (AIS) to be operated by an Account Information Service Provider (AISP) TPP as defined by article 67.

To implement the new PSD2 services (subject to PSU consent) a TPP needs to access the account of the PSU. The account is usually managed by another PSP called the Account Servicing Payment Service

[9]https://www.berlin-group.org/psd2-access-to-bank-accounts

[10]European Banking Authority Regulatory Technical Standards, emitted in the final draft on 23 February 2017 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

Provider (ASPSP). To support the TPP in accessing the accounts managed by an ASPSP, each ASPSP has to provide an "access to account interface" (XS2A interface).

PSD2 defines responsibilities and rights of TPP and ASPSP concerning the interaction at the XS2A interface, while technical details and requirements for the implementation and operation of the XS2A interface are defined in EBA RTS, and, finally, for the implementation of the XS2A interface also the interpretation by the EBA[11] has to be respected.

3.2.2.1 TPP possible scenarios

For a TPP as an actor at the XS2A interface, it has to be distinguished between the following roles:

1. PIISP: Payment Instrument Issuing Service Provider: use of the XS2A interface of an ASPSP while executing a fund confirmation service (FCS) (article 65).
2. PISP: Payment Initiation Service Provider: use of the XS2A interface of an ASPSP while executing a payment initiation service (PIS) (article 66).
3. AISP: Account Information Service Provider: use of the XS2A interface of an ASPSP while executing an account information service (AIS) (article 67).

Even if a TPP may be authorized for different roles, it shall only execute one per transaction at the XS2A Interface, i.e. all requests are for a single service.

3.2.2.2 XS2A security

In Europe, multiple competing standards for XS2A interface exists (and some open API from a list of banks even before the PSD2 creation). There are also ongoing standardization efforts, aligned with the goals of the Euro Retail Payments Board, implemented by the Berlin group.

In particular, the Berlin group framework is a complex effort in standardizing PSD2 XS2A with specific technical measures, so it is suitable to depict the common baseline of security solution.

In details it proposes (from the Berlin Group specification):

1. “RESTful” API set using HTTP/1.1 with TLS 1.2 (or higher) as transport protocol;
2. TPP identification by ETSI-defined eIDAS certificates: QWACS mandated (easy measure to protect e.g. against DDOS attacks), QSEALS optional for banks (TPP follows instruction by bank);
3. supporting all PSD2 required payment initiation, account information and confirmation of funds use cases, with future-dated, multiple/bulk, and recurring payments optional (depending on support in online banking or in national legislation);
4. full multicurrency support of accounts;
5. four architecture models for Strong Customer Authentication (SCA): redirect, OAuth2, decoupled and embedded, with influence of the TPP on redirect preference;
6. multilevel SCA approach for corporates, e.g. to support a 4-eyes principle;
7. support of card transactions reconciliation accounts;

[11] EBA publishes an “opinion” on the implementation of the RTS on strong customer authentication and common and secure communication https://eba.europa.eu/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication, published on 13 June 2018.

8. signing baskets as signing vehicles for grouped transactions (instead of multiple payments functions);
9. transparent resource structures (allowing TPPs to keep an overview also in complex business processes);
10. dedicated consent API separating consent handling from account access, obeying both PSD2 and GDPR requirements;
11. optional session support (set of consecutively executed transactions), subject to appropriate customer consent;
12. data structures either as
    a. JSON with data model based on ISO 20022, or
    b. XML with pain.001 for PISPs and camt.05x for AISPs;
13. integrated formal and transparent change management process and versioning;
14. extensible with additional extensions for (non-core PSD2) value add services.

These requirements may contribute to understand the security competencies required in a PSD2 scenario.

3.2.3 Generic Threat Scenarios within Open Banking

The demonstration use case "Open Banking API Architecture" features three similar but distinct scenarios. In these scenarios, we describe the threats and derive how to ensure properties violated in them with skills and education requirements. The three scenarios are:

(1) Ensuring Integrity and Confidentiality 1
(2) Ensuring Integrity and Confidentiality 2
(3) Ensuring Integrity and Confidentiality 3

and we add another threat scenario Ensuring Legitimate Access, peculiar to PSD2.

We first provide a high-level overview of the demonstration use case along with a basic flow diagram and related post conditions.

3.2.3.1 **Scenario:** Ensuring Integrity and Confidentiality 1

Figure 4 provides an overview about the possible real cases related to an attacker performing a *spoofing attack*. In this type of attack, the attacker impersonates another user or device on a network in order to perform malicious activities (e.g. to steal data). The primary victims of the attackers in this scenario are banks and users, although ICT and service providers are also impacted.

The attacker obtains an authentication token to bypass the bank authentication system.

When the system allows access to the attacker, he performs a *man-in-the-middle attack* (MITM) which results in the theft of the users data information from the bank.

Another approach shows the hacker tricking the user into clicking on something different or compiling a form which reveals confidential information.

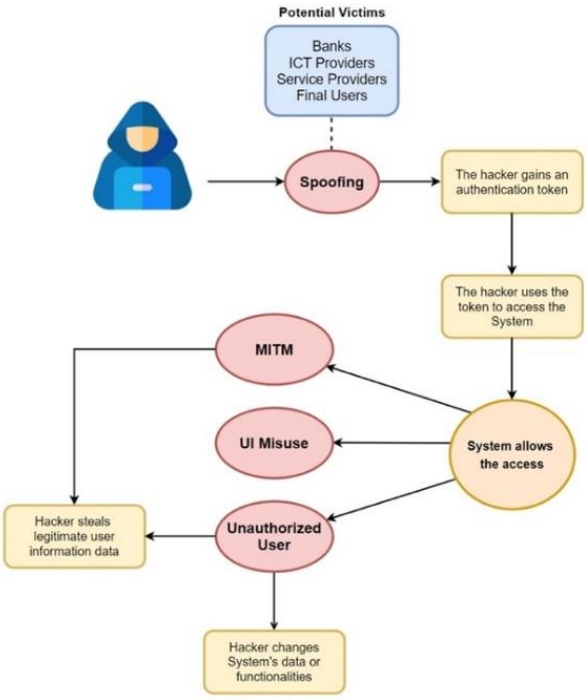

Figure 4: A spoofing attack and its consequences for the victims.

Finally the attacker accesses the system directly and changes some of the functionalities of the system.

Basic Flow

A hacker finds a JSON web token vulnerability to access the bank system through the use of spoofing and steals information from a bank customer:

1. Hacker uses the vulnerability to create a new authentication token
2. Bank system accepts authentication token
3. Hacker creates a MITM (man-in-the-middle) connection
4. Hacker extracts information from the bank customer

Alternate Flow

Malicious user finds a JSON web token vulnerability to access the bank system through the use of spoofing:

1. Hacker uses the vulnerability to create a new authentication token
2. Bank system accepts authentication token
3. Hacker changes functionalities of the bank

Post Conditions

Information in the bank system is changed after the execution of this scenario. In particular, the hacker has:

- added new authorised users to the system for creating a new attack pattern;
- injected in the API system new API functions to view and change information of legitimate users;
- changed the user interface of the API system or of the bank itself to create new forms to be used for a future phishing campaign.

3.2.3.2 **Scenario:** Ensuring Integrity and Confidentiality 2

Figure 5 provides an overview about the possible real cases related to an attacker performing a *tampering attack*. In this type of attack the attacker changes or deletes a resource without authorization. If the attacker is able to tamper with it, it can have some consequences on the usage of the system itself (e.g. the attacker can add or remove some functional elements). The victims of the attacks in this scenario are banks, users and Service Providers.

In the scenario is supposed that the attacker is able to access to the bank system and compromise it. In particular the attacker modifies or creates new API functions that will be used to perform malicious activities. The attacker's goal is to make the user use the malicious APIs. As consequence, when the user invokes the crafted APIs, the system could suffer of two types of compromissions: *Integrity compromission* and *Confidentiality compromission.*

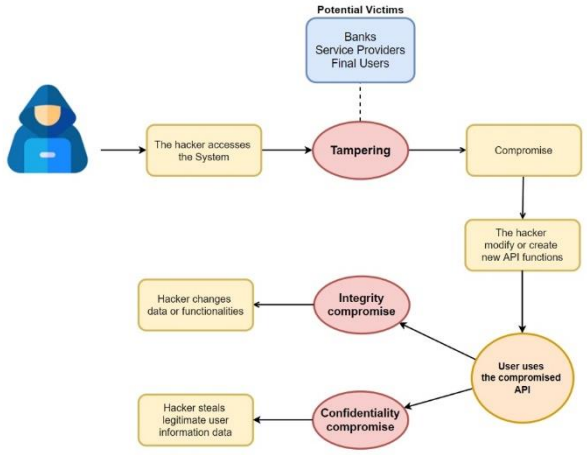

Figure 5: A tampering attack and its consequences for the victims

Integrity compromission implies that the attacker is able to change data of functionality so that the system will be transformed to work in a manner from the way in which the service was designed. *Confidentiality compromise* implies that the attacker is able to access to data that he is not authorized to view.

Basic Flow

A hacker finds an XSS vulnerability to tamper with the bank system:

1. Hacker uses the vulnerability to access the bank system
2. Hacker tampers with the bank system
3. Hacker creates a new API function
4. Bank customer connects and uses new API function
5. Hacker changes information in the bank system

Post Conditions

Information in the bank system is changed after the execution of this scenario. In particular, the hacker has:

- changed user information (e.g. name, surname, telephone numbers) for new and existing bank customers;
- changed the API system with new API functions to change information of legitimate users;
- added new API components to redirect function calls.

3.2.3.3 **Scenario:** Ensuring Integrity and Confidentiality 3

Figure 6 provides an overview of the possible real cases related to an attacker exploiting a vulnerability to perform a privilege escalation. Privilege escalation is frequently used in preparation for a more specific attack, allowing intruders to deploy a malicious payload or execute malicious code in the targeted system. However, the attacker could simply extract data or change the functionalities of the system. Potential victims of the attackers in this scenario are banks, service providers and Open Banking pure players.

The actors actively involved are the attacker and the bank.

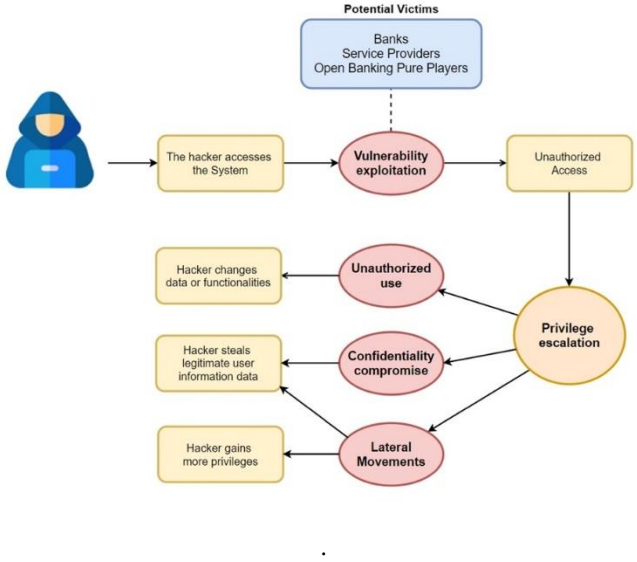

Figure 6: Schema representing an attacker exploiting a vulnerability to realize a privilege escalation with the relative consequences for the victims.

Basic Flow

1. The attacker accesses the bank system
2. The attacker makes changes to data or system functionalities through an unauthorised use of privileges
3. Then the attacker steals legitimate user data
4. Finally the attacker gains more privileges to do more damage

Post Conditions

Hacker has new permissions in the system. With these new privileges the hacker has:

- changed the data or functionalities of bank system;
- stolen legitimate information data;
- gained new privileges to access new system functions (e.g. add /delete /edit bank users).

3.2.3.4 **Scenario:** Ensuring Legitimate Access

PSD2 introduction from one side takes in greatest care the required security, but from the other it enlarges the attack surface. Companies with different size (often small) and different security postures (e.g. not subject to the restrictive bank regulations) can now access and manipulates banking data.

In addition, these new companies may not be subject to the same stringent regulations of the banks themselves. Amongst the others, "public" APIs (banks and FinTech), new mobile apps, and new interactions of legacy data sharing techniques, concurs to form the enlarged attack surface.

Since PSD2 allows FinTech company to develop API to access banking services, in the absence of appropriate access control to sensitive information, an attacker can exploit vulnerabilities to acquire user credential. The consequences for credential leakage threat is illustrated in Figure 7. If a FinTech company publishes its API documentation online, a hacker can analyse the documentation finding out weaknesses, e.g that suitable information like customer's email address, password, client secret authentication, the client ID may be visible in the path of the API URL

Basic Flow

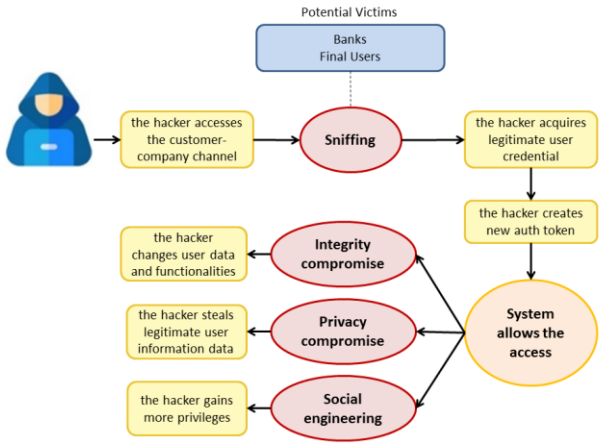

Figure 7: Credential leakage threat and consequences for the victim

1. The attacker manages to put him/herself as a passive MITM between the customer and the FinTech company
2. The attacker acquires the user credentials of a legitimate customer
3. The attacker creates a new authentication token
4. The attacker connects to the bank system through the FinTech API using the stolen credentials
5. The attacker extracts further information of the bank customer

Post Conditions

The attacker gained a new access to the system. With that, might possibly steal sensible data of the customer from the bank system, make operations on illegitimate behalf of the customer, use these new permission as starting point for new attacks (e.g. social engineering ones).

Successful attacks can be prevented adopting organisation-wide security policies and procedures. The FinTech must have an adequate identity management system to avoid easy circumvention of the access control mechanisms, must adopt Privacy by Design and by Default development to avoid sensible information leakage, Security communication protocols and adequate security management (e.g. key distribution and certificate management) must be applied to avoid MITM attacks, Effort on security awareness and usable security must be considered in the risk management and security governance posture to avoid the many non-security savvy users involved in a transaction may become pray of social engineering.

Security requirements to counter the described threats are summarsed in the next sections, as well as countermeasures at technical and organisational level to avoid them.

3.2.3.5 PSD2 security requirements

PSD2 security requirements (from the directive itself, the RTS and the Berlin group framework) are:

1. **logging** since payment service providers must log all the (succeeded and failed) transactions;
2. **privacy** since payment service providers can access, retain and process personal data (e.g. to detect and investigate frauds), but only with the explicit consent of the payment service user;
3. **incident management** since payment service providers must have effective incident management procedures for the detecting and classifying of operational and security incidents;
4. **reporting** since payment service providers must produce a report on the operational and security risks and the implemented mitigations to the competent authority on an annual basis and since payment service providers must produce statistical data on frauds to the competent authority at least on an annual basis;
5. **cryptography** since payment service providers must provide adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials;

6. **authentication** since payment service provider must apply strong customer authentication for electronic payments strong customer authentication must link the transaction to a specific amount and a specific payee.

3.2.3.6 Prevention measures and best practices

The following are the measures and best practices that the actors involved in the previous scenarios should enforce in order to prevent the described attacks:

- Vulnerability research;
- Vulnerability assessment;
- API Calls Monitoring.

3.2.3.6.1 Vulnerability research

The process of discovering vulnerabilities and design flaws that will open a network, operating system, or applications to attack or misuse is known as **Vulnerability research**. Actors involved into prevent the attacks described in the previous scenarios must perform vulnerability research on their products and resources to identify and eradicate all security flaws.

An IT administrator needs vulnerability research:

- To gather information about security trends, threats, and attacks;
- To find weaknesses and alert the network administrator before a network attack;
- To get information that helps prevent security problems;
- To know how to recover from a network attack.

An incident management team member needs to keep up with the most recently discovered vulnerabilities and exploits in order to stay one step ahead of attackers. This is done through vulnerability research, which includes:

- Discovering system design faults and weaknesses that might allow attackers to compromise a system;
- Being informed about new products and technologies in order to find news related to current exploits;
- Checking underground hacking websites for newly discovered vulnerabilities and exploits;
- Checking newly released alerts regarding relevant innovations and product improvements for security systems.

Security experts within the aforementioned team and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, or high);
- Exploit range (local or remote).

Incident handlers can research vulnerabilities online by using details of the resources in question, such as build, version, or operating system.

3.2.3.6.2 Vulnerability Assessment

The examination of the ability of a system or application, including its current security procedures and controls, to withstand assault is known as **Vulnerability assessment**. Such activity aims to scan networks to find known security weaknesses, and recognize, measure, and classifie security vulnerabilities in computer systems, networks, and communication channels. It also assists network administrators or incident handlers to secure the network by determining security loopholes or vulnerabilities in the current security mechanism before the attackers can exploit them.

A vulnerability assessment may be used to:

- Identify weaknesses that can be exploited;
- Predict the effectiveness of additional security measures in protecting information resources from attack.

3.2.3.6.3 API Calls Monitoring

In the new context of the banking industry, with particular reference to the PSD2 regulation, European banks are obliged to open their APIs (Application Program Interface) to fintech companies (technology applied to finance) and other companies that deal with products and financial services. Many times, software programmers in a rush to develop new features can make mistakes that lead to data exposure and data loss. What makes these errors so dangerous is mainly the nature of the API. The following are some reasons to support this:

- API security is underestimated;
- Many times more data is exposed than needed via API;
- Developers and security professionals don't work together to publish secure APIs and manage their entire lifecycles.

A best practice to prevent the aforementioned scenarios is to continuously monitor and assess the security risk of organization APIs. It is necessary to define a model for continuous monitoring rather than a simple periodic assessment.

It also needed to prioritize the reduction of risks within the development team. In order to properly inform the development team about the risks into their code and identify remediation, a best practice should be streamline the rolling out processes.

Finally, security experts should implement strong controls and protections to avoid that bad actors exploit and misuse organizations APIs.

3.3 Use case 3: Security and privacy-enhancing platforms

Use case 3 includes scenarios related to Security Intelligence and Cross-Border Authentication.

3.3.1 Security Intelligence scenario

One of the current challenges that faces the financial institutions related not only to incident reporting but also to fight against the increasing cyber-threats and cyber-attacks affecting this sector, as it was identified by the stakeholders in the analysis done in the CS4E deliverable D4.1[12], it is to promote a collaborative approach in the access to the information about security incidents that fosters the cooperation between public

[12] D4.1 Requirements Analysis from Vertical Stakeholders

and private entities for the achievement of a common interest and helps to improve the overall cyber-resilience across the European Union.

This need translates into the deployment of a threat intelligence platform for sharing data among the different stakeholders affected. But some features are key to be considered if we want to achieve the final goal of increasing the usage of this platform and, what is more important, reducing the rejection to share relevant information from the cyber-security point of view because it is considered compromising, sensitive or a risk for their reputation. In particular, it is required to improve trustworthiness for threat intelligence sharing and prioritize quality versus quantity, offering reliable and automated threat analysis of the data shared.

In the context of the Incident Reporting in the Financial Sector demonstrator, it is foreseen that part of the information collected through the platform by the Incident Management Team of a financial institution about the security incidents detected in their financial institution will be shared to a common financial data sharing platform using MISP[13]. This information, that could be shared at different levels or creating trusted groups based on access policies to maintain the control on who access to which sensitive information, will support the entities regarding the identification of what actually happened, how it happened or how to provide response against potential threats and detected security incidents, as well as enriching the information required for mandatory incident reporting. Trustworthy APIs for threat intelligence sharing and distributed security framework developed in the context of the CS4E WP3 would be used as mechanisms to improve trustworthiness and reliability. Additionally, Security Intelligence data shared in that common financial data sharing platform (shared by other entities or received from public threat intelligence feeds) would be qualified to help the users to properly and effectively identify which are more relevant or priority for its infrastructure. Multi-dimensional trust model for reliable CTI-sharing and heuristic analysis considering inventory information about the infrastructure and information about ongoing or past security incidents detected, also developed in the context of the CS4E WP3, is envisaged to be used with this purpose.

Figure 8 drafts the foreseen Security Intelligence Scenario where we assume a financial institution B is under a cyber-attack (e.g. it could be a phishing or malware campaign) that has also affected to other institutions (e.g. financial institution A). The Incident Management Team in the financial institution B is working on collecting all the information about the security incident detected in one of their offices, analysing it and preparing the mandatory incident report that need to be sent to the competent supervisory authorities depending on the applicable regulations. To understand better the security incident and what could be the origin of the attack, its impact and consequences, they would check additional information coming from the threat intelligence sharing platform. The data received from the sharing platform would be previously qualified and enriched by the CS4E threat intelligence assets included in the demonstrator. In this way, the Incident Management Team would know which of the incoming data are more reliable and more relevant for the ongoing investigation on a specific security incident and for their specific infrastructure. For example, if the same type of attack has been already performed in another entity, they could have already determined and shared the vulnerabilities involved, the next steps followed by the attacker or the mitigation measures they have applied. Additionally, once the investigation has been completed, they could also share data about the detected cyber-attack to the platform using the trustworthy APIs, so other entities in the common financial data sharing platform can be aware of it and benefit themselves from the shared Security Intelligence.

[13] MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Intelligence Information Sharing (https://www.misp-project.org/)

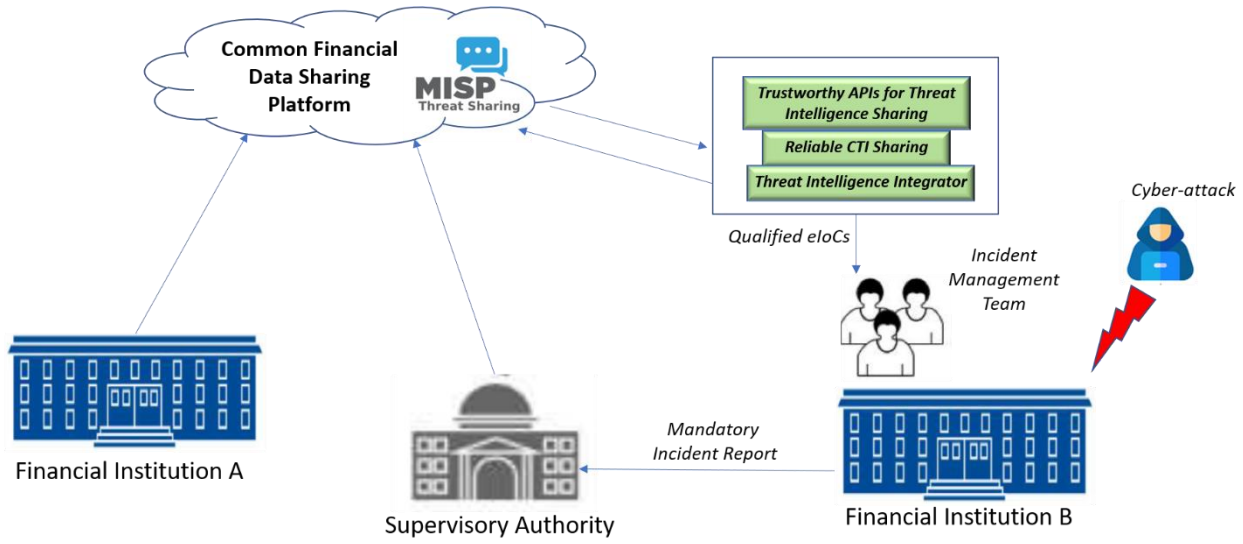

Figure 8: Security Intelligence Scenario

3.3.2 Cross-Border Authentication scenario

The European digital transformation is one of the main objectives of the European Commission developing a European digital strategy in order to facilitate citizens and businesses the access to the digital services provided by the public administrations and private companies. According to the European digital strategy[14], supporting new technologies not only the European citizens can improve her/his daily life, but businesses can benefit in terms of growth, innovation and competitiveness, and also the planet benefits from these digital technologies as they cause lesser impact on the environment and are more sustainable.

The increasing of seamless digital services across Europe and the freedom of movement to citizens, allowed by the EU, implies the performance of cross-border transactions. The development of mechanisms assuring these transactions are secure, create a trusted environment and guarantee the user privacy is necessary. For facilitating these cross-border transactions the EC developed the eIDAS Regulation[15] and build the eIDAS network[16] which allows the cross-border transactions in a secure and trusted environment by using eID[17] means issued by the EU Member States.

A simple eIDAS authentication flow is depicted in Figure 9, where a European citizen (e.g. Spanish citizen) try to log in to an online service in the country A. The Spanish citizen is redirected to the Spanish IdP through the eIDAS country nodes belonging to the eIDAS network. The Spanish IdP authenticates the Spanish citizen and provides the citizen personal identity data. This identity data reaches the digital service. Once the system confirms the validity of the user credentials, the Spanish citizen is allowed to access the requested service.

[14] https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[16] https://ec.europa.eu/digital-single-market/en/blog/eidas-cooperation-network-eid-few-impressions-after-first-meeting-0
[17] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

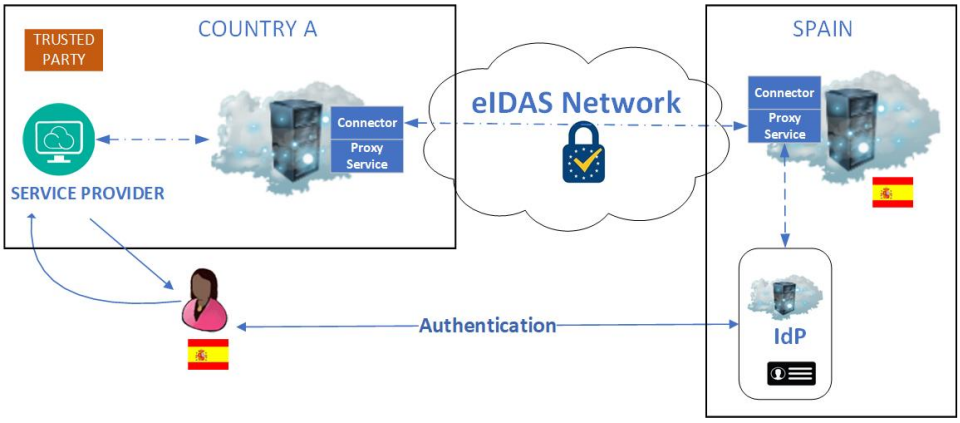

Figure 9: eIDAS authentication flow

In the context of Medical Data Exchange demonstrator, the eIDAS authentication process is integrated with the Covid-19 Data Exchange platform for providing a strong authentication mechanism when users such as data providers and data consumers accessing the sharing platform.

Figure 10 shows authentication process for accessing the platform and the actors involved.

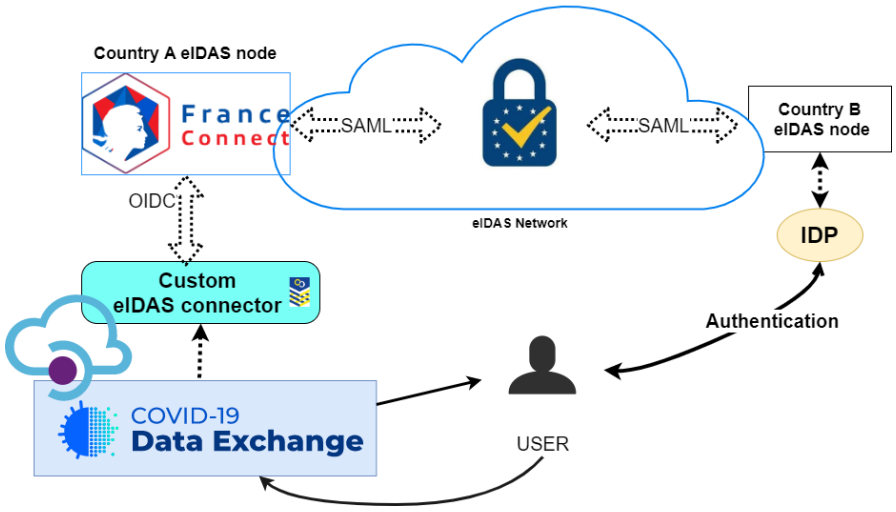

Figure 10: Covid-19-eIDAS authentication flow

In this case additional details are provided regarding adopted standard protocols such as OpenID Connect[18] (OIDC) and SAML 2.0[19] adopted for performing the user authentication process. The EC through the CEF programme[20] released the eID building block[21] which facilitates the development of the country eIDAS node and the way to integrate the node with digital services by using the SAML 2.0 protocol. Recently the EC

[18] https://openid.net/connect/
[19] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
[20] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom
[21] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eID

just pre-release the CEF eIDAS-Node version 2.5[22] for the Java platform. Java[23] programming language was chosen for these implementations. Also, eIDAS technical specifications[24] are provided by the EC. Two identification schemes[25] are provided for the eIDAS node development:

- eIDAS Proxy service, followed by most of the countries;
- eIDAS Middleware service, followed by e.g. Germany.

The skills for developing the components allowing the connection to each country eIDAS node are mainly constrained by the delivered building block. Therefore, medium and advanced skills on Java programming language are needed. Additionally, skills and knowledge to avoid vulnerabilities on these protocols are highly important[26] preventing from attacks and data disclosure.

For the integration of the eIDAS node with the digital services the Member States has the freedom to use their own mechanism, even based on SAML 2.0 protocol specifications or others such as Open OIDC protocol. Nevertheless, as the exchanged user identity data are personal data, the developers and the system managers must have a good knowledge on secure protocols and privacy-preserving techniques and tools to be applied on these developments and deployments. The user data protection rights must be assured at any moment as GDPR stablish. In the case of medical data exchange scenario, as the health records are considered as sensitive data, additional constrains apply in order to accomplish with the GDPR. In this case anonymization or pseudonymization mechanisms must be applied and known by the developers and system managers. In this particular case where data are anonymized the participation of a data privacy expert or a data protection officer is a must. These actors must assure that the user data are protected at any moment and the user data are anonymized properly avoiding any kind of de-anonymization could deliver the identity of the user (as the GDPR doesn't apply on anonymized data).

When the data are stored in some infrastructure the data processor must be assure that the data are protected properly by using hardware (e.g. Trusted Execution Environment) and software protecting mechanisms (e.g. cryptography tools). In this regard, experts on these fields are necessary.

When this kind of personal or sensitive data are shared, the use and knowledge of data sharing techniques[27] are compulsory. Also, the involvement of privacy experts and the execution of data privacy and security impact assessment conducted by experts must be performed.

3.4 Use case 4: Assessment Mechanisms for non-ICT Workforce (lawyers)

The main focus of this deliverable is aimed at information and communications technology (ICT) personnel. However, there are many other professions where Cyber Security knowledge is important or even essential to perform the required work. The official education curriculum for such professions often does not include the Cyber Security topics, or they are discussed very superficially. This is also a reason why professional training in Cyber Security is especially important for such professions. Of course, to identify and collect all

[22]https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2020/10/02/Pre-Release+of+CEF+eIDAS-Node+software+v2.5?pk_campaign=XSELL-Bulletin58-202010&pk_source=email&pk_medium=CEFbulletin&pk_content=technical

[23] https://docs.oracle.com/javase/specs/jls/se8/html/index.html

[24] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile

[25]https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile?preview=/82773108/148898845/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf

[26] https://sec-consult.com/en/blog/2019/10/vulnerability-in-eu-cross-border-authentication-software-eidas-node/

[27]https://www.researchgate.net/profile/Daniel_Smullen/publication/310823188_Privacy_Risk_in_Cybersecurity_Data_Sharing/links/5e6d1764a6fdccf994ca03d6/Privacy-Risk-in-Cybersecurity-Data-Sharing.pdf

the existing training/courses aimed at all non-ICT professions is a very big job, well out of the scope of this section. We have rather directed our focus at one such important profile. The work done here can be used as a template to gather the same data for other professions.

From all of the non-ICT professions that require some Cyber Security knowledge, we have decided to focus on the lawyers and Cyber Security knowledge they require in their line of work. Arguably, lawyers are not provided with sufficient Cyber Security training during their education, given the advanced technological developments. Cyber Security is not a static matter, but it is a constantly changing and developing activity in different fields of law as well. It represents the protection of data and information systems against unauthorised access, use, disclosure, alteration or destruction. When practising their profession, lawyers and attorneys must ensure the protection and confidentiality of their clients' data and ensure that the obtained data is not misused. To perform the best work possible, interdisciplinary is extremely important for lawyers and other professionals working in the field of law, this includes relevant knowledge of Cyber Security.

3.4.1 Scenario: Cyber Security for Lawyers

Due to technological advances, the vast majority of data is nowadays stored electronically, and most of those are in some way connected to the internet. As a result, the risks associated with their disclosure increase. Article 5 of the General Data Protection Regulation (GDPR) stipulates that personal data must be processed in a manner that ensures adequate security of personal data with appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Therefore, the consequences of the invasion of privacy for individuals, businesses and others can be very severe - both in terms of direct damage caused by data theft and potentially by the liability of new regulations such as the GDPR in the EU. Similar to other professions, lawyers and attorneys follow this trend and perform their activities, mainly in digital forms. The work of lawyers and attorneys differs from other professions primarily in the amount of personal and confidential data (e.g. trade secrets, personal and other (legal) sensitive data) they encounter in the exercise of their profession. Taking this into account, lawyers and attorneys conduct counselling via videoconferencing, communicate with clients via e-mail, which often also contains confidential information, etc. At the same time, in the information age, many legal issues, proposals and problems are directly related to digital content and its safe and private management. Taking into account everything mentioned, it is vital for a lawyer or an attorney to have a certain level of knowledge in the field of Cyber Security, so that they will be able to provide security and privacy to the clients and be able to advise them when problems occur.

A simple search for existing professional training on Cyber Security aspects aimed at giving the lawyers, and related law professionals, the knowledge they require in their work has shown that there are very few existing courses or other training possibilities on the market in the EU, that are readily available (possibly there are more one-time courses; however, those are hard to find, as any information about them tends to disappear after they have finished). Courses like the SANS' LEG523: Law of Data Security and Investigations[28] and associated certification GIAC Law of Data Security & Investigations (GLEG)[29], provide professional training, including skills in the analysis and use of contracts, policies, and insurance security questionnaires. The course also covers the law of crime, policy, contracts, liability, compliance, Cyber Security, and active defence - all with a focus on electronically stored and transmitted records. However, while courses like these are useful to lawyers, they are not really designed for them or at least not

[28] https://www.sans.org/cyber-security-courses/cybersecurity-law-data-security/
[29] https://www.giac.org/certification/law-data-security-investigations-gleg

for the majority who do not actively work in the field where Cyber Security is directly applicable (i.e. cybercrime). Given the apparent scarcity of training for these professionals, we are interested in finding out which Cyber Security knowledge would be the most important for them to have the knowledge about.

When thinking about Cyber Security and law professionals, the first and often only connection that comes to mind is the cybercrime. However, there are other examples when knowledge on Cyber Security is useful in the field of law. Here are just a few examples.

The requirement for knowledge of Cyber Security is especially evident in the field of criminal law. According to the Convention on Cybercrime[30], criminal offences committed with the help of modern information technology or against a computer can be divided into three groups. Firstly, offences that can be committed using a computer, but do not involve a direct misuse of information technology. In other words, the computer is the mere means of execution in the case of these crimes. Considering we live in the information age, this group of crimes is very extensive - this includes crimes against honour and reputation, crimes in which individuals who have authorised access to computer-controlled databases unjustifiably change the data in these databases. Secondly, crimes that can be committed using a computer and involve direct misuse of information technology. These include, in particular, infringement of copyright and related rights, misuse of intellectual property, display, production, possession and distribution of pornographic material, as well as the manufacture and acquisition of weapons and accessories. Thirdly, crimes that can only be committed using a computer and involve direct misuse of information technology. This group includes unauthorised entry and intrusion into the information system. During criminal proceedings, knowledge of Cyber Security is extremely important, especially in the field of digital forensics. The evidence during the proceedings is useless if it was obtained, e.g. by breaking into the information system. Because digital evidence is "unstable", its probative value could be compromised.

In the field of civil law, lawyers and attorneys need a certain basic knowledge of Cyber Security. As a result of technological progress, a lot of data is transferred and transmitted over the internet, wherein lawyers and attorneys must ensure the confidentiality and privacy of the data. They must be familiar with the Cyber Security basics in order to be able to advise and help the client. For example, in the field of family law, parents, as holders of parental responsibility, control their children within certain limits and sometimes have to access the child's personal data (social network profile). In order to be able to advise a parent, a lawyer or an attorney must, of course, be familiar with Cyber Security. Otherwise, they cannot help the client due to the lack of knowledge in the field of Cyber Security.

Constitutional law primarily guarantees the protection of fundamental human rights and freedoms. The internet, on the other hand, represents a new space for political participation, active citizenship and the development of democracy in general, while at the same time offering space for the spread of traditional forms of social exclusion, intolerance and discrimination. The internet, as a specific technological and communication tool, requires a strong involvement of a range of stakeholders (both nationally and internationally) who can influence on the restriction of hate speech and other unacceptable human rights abuses on the internet. Every individual must be able to use information technology as safely as possible while respecting human rights. With the appropriate knowledge in the field of Cyber Security lawyers and attorneys can introduce the risks and the ways to reduce them as well as the responsibilities of each individual for their own safety in the global communication network.

Lawyers and attorneys, in the field of administrative law, represent clients in administrative, taxes and inspection procedures and other proceedings. The basic knowledge of Cyber Security is very significant especially due to the increasingly large number of applications that clients submit to different state

[30] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

authorities via e-mail or e-application. All those applications contain confidential and private data. In case of an attack or intrusion, the lawyers and attorneys need sufficient knowledge of Cyber Security to be able to represent the client and provide the necessary protection.

4 Proposed framework and profiles for education and professional development

Based on the four use cases with the twelve scenarios presented in the previous section, and the existing skills framework presented in section 2, we have produced a hybrid framework for evaluating the importance of different skills for Cyber Security professionals. Below we detail the skills framework and the chosen profile descriptions used in our framework. In the next section we present an analysis that utilizes this framework.

4.1 Framework

As a result of T6.2, we propose the following framework, illustrated in Figure 11. The left hand size depicts different Knowledge Areas and right hand size reflects different skills belonging to a certain Knowledge Area. In the light of the existing frameworks, we utilize framework developed in D6.2, with specialized profile descriptions derived from each partner's use case. Illustration of using the framework is in Appendix A.

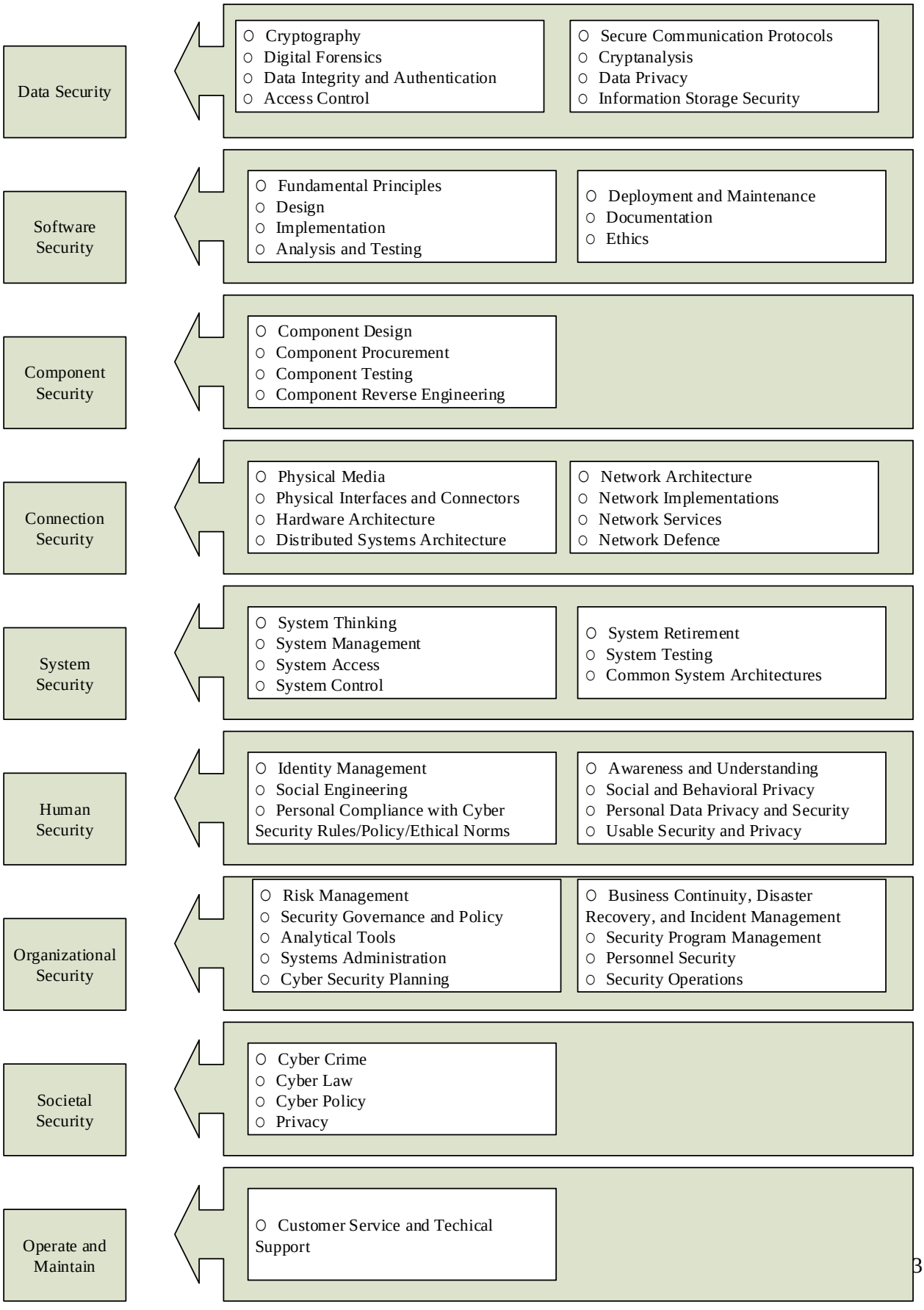
Data Security
Cryptography
Digital Forensics
Data Integrity and Authentication
Access Control
Secure Communication Protocols
Cryptanalysis
Data Privacy
Information Storage Security
Software Security
Fundamental Principles
Design
Implementation
Analysis and Testing
Deployment and Maintenance
Documentation
Ethics
Component Security
Component Design
Component Procurement
Component Testing
Component Reverse Engineering
Connection Security
Physical Media
Physical Interfaces and Connectors
Hardware Architecture
Distributed Systems Architecture
Network Architecture
Network Implementations
Network Services
Network Defence
System Security
System Thinking
System Management
System Access
System Control
System Retirement
System Testing
Common System Architectures
Human Security
Identity Management
Social Engineering
Personal Compliance with Cyber Security Rules/Policy/Ethical Norms
Awareness and Understanding
Social and Behavioral Privacy
Personal Data Privacy and Security
Usable Security and Privacy
Organizational Security
Risk Management
Security Governance and Policy
Analytical Tools
Systems Administration
Cyber Security Planning
Business Continuity, Disaster Recovery, and Incident Management
Security Program Management
Personnel Security
Security Operations
Societal Security
Cyber Crime
Cyber Law
Cyber Policy
Privacy
Operate and Maintain
Customer Service and Techical Support

Figure 11: An illustration of the developed framework with evaluated skills

4.2 Evaluating skills in the scenarios

For the skills, we defined a four-step rating scale consisting of the following criteria:

- **None**: The skill or knowledge is not necessary to perform in the given specialization;
- **Basic**: Understanding the basic principles of the skill or knowledge is needed in the specialization. Application of this skill or knowledge is not necessary to perform in the specialization;
- **Intermediate**: Applying the skill or knowledge is needed to perform in the specialization. The application of the skill or knowledge is not needed beyond standard procedures;
- **Advanced**: Applying the skill or knowledge is essential to perform in the specialization. The application of the skill or knowledge is necessary on an advanced level and beyond well defined standard procedures.

Using this scale, writers of the scenarios evaluated related skills levels required in each of the scenarios on the scale of 0-3. The averages of the skill that are required in each of the the scenarios are illustrated in the Table 2.

Table 2. Skill levels required in scenarios

		Scenario											
	Skill	DP	SC	ST	NA	IS	IA	UI	UE	CL	SI	CB	CS
Data Security	Cryptography	1.0	2.0	1.0	2.0	1.0	1.3	1.3	1.3	2.4	0	0	1.3
	Digital Forensics	0	1.0	0	0	0	1.6	1.6	1.6	1.6	1.0	0	1.1
	Data Integrity and Authentication	0	2.0	2.0	2.0	2.0	2.6	2.6	2.6	2.5	1.0	2.7	1.1
	Access Control	0	2.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	2.0	0	1.1
	Secure Communication Protocols	1.0	3.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	1.0	2.8	1.3
	Cryptanalysis	0	0	0	0	0	1.0	1.0	1.0	1.0	0	0	1.3
	Data Privacy	2.0	2.0	2.0	2.0	2.0	2.2	2.2	2.2	2.5	0	2.6	1.8
	Information Storage Security	2.0	2.0	2.0	2.0	2.0	1.9	1.9	1.9	2.5	1.0	0	1.6
Software Security	Fundamental Principles	0	2.0	2.0	0	1.0	2.0	2.0	2.0	2.8	0	0	0.8

	Design	0	0	0	0	0	1.4	1.4	1.4	2.0	0	0	0.8
	Implementation	0	1.0	0	0	0	1.4	1.4	1.4	2.0	0	0	0.8
	Analysis and Testing	0	3.0	1.0	0	0	0.8	0.8	0.8	1.6	0	0	0.8
	Deployment and Maintenance	0	1.0	0	0	3.0	0.9	0.9	0.9	1.7	0	0	0.8
	Documentation	0	3.0	0	0	1.0	1.7	1.7	1.7	1.6	0	0	1.2
	Ethics	2.0	3.0	1.0	0	1.0	0.6	0.6	0.6	1.5	0	0	1.1
Component Security	Component Design	0	0	0	0	1.0	1.9	1.9	1.9	1.3	0	0	0.6
	Component Procurement	0	0	0	0	1.0	0.7	0.7	0.7	1.0	0	0	0.6
	Component Testing	0	3.0	1.0	0	0	1.0	1.0	1.0	1.1	0	0	0.6
	Component Reverse Engineering	0	3.0	1.0	0	1.0	1.0	1.0	1.0	1.1	0	0	0.6
Connection Security	Physical Media	0	0	1.0	3.0	2.0	1.4	1.4	1.4	1.6	0	0	1.2
	Physical Interfaces and Connectors	0	0	2.0	3.0	2.0	1.1	1.1	1.1	2.5	0	0	0.8
	Hardware Architecture	0	0	1.0	2.0	2.0	1.8	1.8	1.8	2.2	0	0	0.8
	Distributed Systems Architecture	0	1.0	1.0	2.0	3.0	1.3	1.3	1.3	2.6	0	0	0.5
	Network Architecture	0	1.0	2.0	3.0	3.0	1.4	1.4	1.4	2.6	1.0	0	0.4
	Network Implementations	0	2.0	2.0	3.0	3.0	1.2	1.2	1.2	2.6	0	0	0.4

	Network Services	0	2.0	2.0	3.0	2.0	1.3	1.3	1.3	2.6	1.0	0	0.4
	Network Defense	0	2.0	2.0	3.0	3.0	1.8	1.8	1.8	2.5	1.0	0	0.5
System Security	System Thinking	0	1.0	1.0	1.0	1.0	0.0	0.0	0.0	1.1	0	0	0.4
	System Management	0	2.0	2.0	1.0	2.0	1.3	1.3	1.3	0.9	0	0	0.6
	System Access	0	2.0	2.0	2.0	2.0	2.3	2.3	2.3	1.4	0	0	0.8
	System Control	0	1.0	2.0	1.0	2.0	1.8	1.8	1.8	1.4	0	0	0.8
	System Retirement	0	1.0	0	0	0	0.7	0.7	0.7	0.8	0	0	0.6
	System Testing	0	3.0	1.0	0	1.0	0.6	0.6	0.6	1.3	0	0	0.6
	Common System Architectures	0	1.0	2.0	2.0	2.0	1.2	1.2	1.2	1.5	0	0	0.4
Human Security	Identity Management	1.0	2.0	2.0	1.0	2.0	2.2	2.2	2.2	2.7	0	2.6	1.2
	Social Engineering	2.0	3.0	3.0	0	0	1.7	1.7	1.7	2.1	0	0	0.6
	Personal Compliance with Cyber Security Rules/Policy/ Ethical Norms	3.0	3.0	3.0	0	0	1.7	1.7	1.7	1.8	0	0	1.2
	Awareness and Understanding	2.0	2.0	3.0	0	0	1.7	1.7	1.7	1.5	0	0	0.8
	Social and Behavioral Privacy	3.0	3.0	3.0	0	0	1.8	1.8	1.8	1.3	0	2.3	1.2
	Personal Data Privacy and Security	3.0	3.0	3.0	1.0	2.0	1.9	1.9	1.9	3.0	0	2.5	2.1

	Usable Security and Privacy	3.0	2.0	3.0	1.0	1.0	2.1	2.1	2.1	1.5	0	2.3	1.2
Organizational Security	Risk Management	0	3.0	2.0	2.0	2.0	1.6	1.6	1.6	1.7	2.0	0	0.8
	Security Governance & Policy	0	3.0	2.0	2.0	2.0	2.1	2.1	2.1	2.1	0	0	1.1
	Analytical Tools	0	2.0	1.0	2.0	2.0	2.0	2.0	2.0	0.7	3.0	0	0.9
	Systems Administration	0	1.0	1	2.0	2.0	1.6	1.6	1.6	2.1	3.0	0	0.6
	Cyber Security Planning	0	3.0	2.0	2.0	2.0	0.7	0.7	0.7	1.7	0	0	0.9
	Business Continuity, Disaster Recovery, and Incident Management	0	2.0	2.0	3.0	3.0	1.4	1.4	1.4	0.6	3.0	0	1.3
	Security Program Management	0	2.0	2.0	2.0	3.0	0.8	0.8	0.8	1.0	0	0	1.4
	Personnel Security	0	2.0	3.0	0	0	1.6	1.6	1.6	0.9	0	0	1.4
	Security Operations	0	3.0	2.0	2.0	1.0	1.1	1.1	1.1	0.7	0	0	1.4
Societal Security	Cybercrime	3.0	3.0	3.0	0	0	1.6	1.6	1.6	1.8	0	0	1.4
	Cyber Law	3.0	3.0	2.0	0	0	0	0	0	1.8	0	0	1.5
	Cyber Policy	3.0	3.0	2.0	0	1.0	1.8	1.8	1.8	1.8	0	0	1.5
	Privacy	3.0	3.0	3.0	1.0	1.0	1.1	1.1	1.1	1.6	0	2.4	2.1
Operate and Maintain	Customer Service and Technical Support	1.0	1.0	3.0	2.0	2.0	0.2	0.2	0.2	0.2	0	0	0.8

4.3 Profiles based on the scenarios

Based on the use cases and scenarios provided by partners of the project, we chose 18 profiles for Cyber Security professionals that are relevant in these scenarios and also more generally in different contexts and organisations. These profiles and their short descriptions are presented in **Error! Reference source not found.**3. The profiles are in no particular order, as they can represent several distinct organization structures.

Table 3. Cyber Security professional profiles

Company Lawyer	Person that is in charge of ensuring the legality of commercial transactions, advising corporations on their legal rights and duties, including the duties and responsibilities of corporate officers. They must also negotiate agreements with different parties and verify all accounts and finances for business transactions. Another key task corporate lawyers are involved with is navigating the provisions of a company's constitution, shareholder and directors' rights.
Data Protection Officer	Person in charge of ensuring that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. In charge of implementing the data protection plan in a company and assuring the fulfilment of the data protection regulation GDPR. also trains the personnel.
Chief Compliance Officer	Person in charge of overseeing and managing compliance issues within their company or organization. The CCO ensures that the organization is in compliance with various regulatory requirements and that employees are in adherence with internal procedures and policies.
Chief Security Officer	Person accountable for the development and oversight of policies and programs intended for the mitigation and/or reduction of compliance, operational, strategic, financial and reputational security risk strategies relating to the protection of people, intellectual assets and tangible property.
Digital forensic analyst	Person in charge of analysing the digital fingerprints after a cyber-criminal incident with the objective of discover the origin of the attack.
Network administrator	Person that configures and manages the network components in an organization (security, identity, configuration, application of countermeasures). This person is also in charge of updating the firmware of the components.
Security Operation Center Manager	Person in charge of leading and managing a Security Operations Center. He is primarily responsible for security event monitoring, management and response. In addition he must ensure incident identification, assessment, quantification, reporting, communication, mitigation and monitoring. Finally, he is in charge ensuring compliance to SLA, process adherence and process improvisation to achieve operational objectives

Incident management team member	Person responsible for monitoring the state of the system, detect incidents and decide the appropriate mitigations and actions to avoid or reduce the risk and the impact over the system.
Software Engineer	Person who applies the principles of software engineering to the design, development, maintenance, testing, and evaluation of computer software.
Data protection lawyer or consultant	Person that assess a client (e.g., manufacturer, organization) about the compliance of the regulation GDPR, in order to ensure that the products are in line with it.
Security certification agent	Person in charge of evaluating the security of a system according to a specific certification scheme, processes and standards.
Security Trainer	Person in charge of training personnel of an organization to be aware of the security concerns and to train them on how to avoid security issues. This could include group sessions, cyber ranges, flagships and other techniques, depending on the organization domain.
IoT Security Manager	Person in charge of managing the security of the IoT devices that are part of the system (configuration, protocols, security changes, communications, information shared, reassessment, vulnerability datatabse consultation, etc.).
Chief Information Security Officer	Person in charge of ensuring adaptation of information security to other security domains, including privacy protection. Monitor and ensure compliance with information security requirements and architecture and consistent application of Security-by-Design and Privacy-by-Design.
Information Security Officer	Person in charge of adapting information security activities and projects to other information security domains, including privacy protection and physical security Provide information security designs and solutions and the implementation of security-by-design and privacy-by-design in information systems
Policy Manager	Person in charge of managing the permissions of the different components of the network to access to other resources.
Cloud Trust Manager	Person in charge of managing the reputation in distributed systems, allowing de-anonymization of the real owner identity of the associated shared data in case of law enforcement inspection is needed.
Dynamic security deployment manager	Person in charge of managing the secure network deployment of the different components willing to join the network (initial assessment, initial configuration, information obtaining, etc.).

Thus our framework consists of these 18 profiles and the 55 skills that we have already previously identified as the core of Cyber Security knowledge. In the following Table 4, we illustrate the profiles and what is their average Cyber Security skill level required in each of the scenarios. Scenario Cyber Security for Lawyers (CS) is also included in the Table 4, but it differs from the other scenarios so, that the profiles are replaced by the different fields of law (see Sections 4.6 and 5.3). The purpose for including this scenario is to illustrated the application of our process for discovering Cyber Security properties in non-IT professional context, the field of law. Therefore, the values have to be considered from their own context. Also for this reason, the grouping of the skills in this scenario is different, thus the scenario CS it can not be directly compared with the other scenarios in this aspect. It however offers an example, that however distinctly separate field, that is not directly understood as Cyber Security-related, the Cyber Security properties can still be defined from it and thus related requirements for education can be just as well derived, like in the case from traditional IT fields. In the following, we will analyse main required Cyber Security properties, of each scenario.

Table 4. Profiles' average Cyber Security skill required in different scenarios

		Scenarios											
Profiles	DP	SC	ST	NA	IS	IA	UI	UE	CL	SI	CB	Fields of law	CS
Company Lawyer	N/A	N/A	N/A	N/A	N/A	0.8	0.8	0.8	0.8	N/A	0.3	**Administrative law**	1.1
Data Protection Officer	N/A	N/A	N/A	N/A	N/A	1.2	1.2	1.2	0.8	N/A	0.4	**Arbitration law**	0.6
Chief Compliance Officer	N/A	N/A	N/A	N/A	N/A	0.8	0.8	0.8	0.8	N/A	0.4	**European law**	1.1
Chief Security Officer	N/A	N/A	N/A	N/A	N/A	2.2	2.2	2.2	0.8	N/A	0.4	**Tax law**	0.9
Digital forensic analyst	N/A	N/A	N/A	N/A	N/A	1.8	1.8	1.8	0.8	N/A	0.3	**International law**	1.0
Network administrator	N/A	N/A	N/A	1.2	N/A	1.8	1.8	1.8	0.8	N/A	0.3	**Civil law**	1.0
Security Operation Center Manager	N/A	N/A	N/A	N/A	N/A	1.7	1.7	1.7	0.8	N/A	0.4	**Commercial law**	1.2

Incident management team member	N/A	N/A	N/A	N/A	N/A	1.7	1.7	1.7	0.8	0.4	0.4	**Banking and finance law**	1.6
Software Engineer	N/A	N/A	N/A	N/A	N/A	1.2	1.2	1.2	0.8	N/A	0.3	**Transport law**	1.0
Data protection lawyer or consultant	0.7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.4	**Family law and the law of persons**	0.5
Security certification agent	N/A	2.0	N/A	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.4	**Medical law**	1.1
Security Trainer	N/A	N/A	1.6	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.4	**Intellectual property law**	1.1
IoT Security Manager	N/A	N/A	N/A	N/A	1.4	N/A	N/A	N/A	0.8	N/A	0.4	**Criminal law**	1.5
Chief Information Security Officer	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.4	**Damages and restitution law**	0.8
Information Security Officer	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.4	**Constitutional law**	0.5
Policy Manager	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.3		
Cloud Trust Manager	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.4		
Dynamic security deployment manager	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.8	N/A	0.3		

4.3.1 Federated IdM Scenarios on Public Sector

4.3.1.1 Data Protection Lawyer in University

In the case of data protection lawyer in university, the required skills on an advanced level are fields of Societal Security, namely *Cybercrime*, *Cyber Law*, *Cyber Policy*, and *Privacy*. In addition, skills related human security are needed on an advanced level: *Personal Compliance with Cyber Security Rules/Policy/ Ethical Norms*, *Awareness and Understanding*, *Social and Behavioral Privacy*, *Personal Data Privacy and Security*, and *Usable Security and Privacy*.

4.3.1.2 Security Certification Agent in University

Skills that are needed for the scenario Security Certification Agent in University on an advanced level are *Analysis and Testing*, *Documentation*, *Ethics*, *Component Testing*, *Component Reverse Engineering*, *Network Defense*, *System Testing*, *Social Engineering*, *Personal Compliance with Cyber Security Rules/Policy/ Ethical Norms*, *Social and Behavioral Privacy*, *Personal Data Privacy and Security*, *Risk Management*, *Security Governance and Policy*, *Cyber Security Planning*, and finally, *Security Operations*, *Cybercrime*, *Cyber Law*, *Cyber Policy* and *Privacy*.

4.3.1.3 Security Trainer in University

Skills that are needed most for the scenario Security Trainer in University are *Social Engineering*, *Personal Compliance with Cyber Security Rules/Policy/ Ethical Norms*, *Awareness and Understanding*, *Social and Behavioral Privacy*, *Personal Data Privacy and Security*, and finally, *Usable Security and Privacy*. In addition, *Personnel Security*, *Cybercrime*, *Privacy*, and *Customer Service and Technical Support* are needed on an advanced level.

4.3.1.4 Network Administrator in University

For the scenario Network Administrator in University, the most required skills are *Access Control*, *Secure Communication Protocols*, *Physical Media*, *Physical Interfaces and Connectors*, *Network Architecture*, *Network Implementations*, *Network Services*, *Network Defense*, *Business Continuity*, *Disaster Recovery*, *Incident Management*, and finally, *Customer Service and Technical Support*.

4.3.1.5 IoT Security Manager in University

Concerning the scenario IoT Manager in University, the most required skills are on an advanced level *Access Control*, *Secure Communication Protocols*, *Deployment and Management*, *Distributed Systems Architecture*, *Systems Architecture*, *Network Implementations*, *Network Defense*, *Business Continuity*, *Disaster Recovery and Incident Management*, and finally, *Security Program Management*.

4.3.2 Open Banking and Revised Payment Service Directive

4.3.2.1 Ensuring Integrity and Confidentiality 1, Ensuring Integrity and Confidentiality 2, and Ensuring Integrity and Confidentiality 3

The profiles in these scenarios were Company Lawyer, Data Protection Officer, Chief Compliance Officer, Chief Security Officer, Digital Forensic Analyst, Network Administrator, Security Operation Center Manager, Incident Management Team Member and Software Engineer. For them, the average most advanced needed skills (value greater or equal with 2) were *Data Integrity and Authentication*, *Access Control*, *Security Communication Protocols*, *Data Privacy*, *Fundamental Principles*, *System Access*,

Identity Management, *Usable Security and Privacy*, *Security Governance and Policy*, and finally, *Analytical Tools*.

4.3.2.2 Ensuring Legitimate Access

This scenario includes all the profiles of the framework. The averages of the required skills on an advanced level are *Cryptography*, *Data Integrity and Authentication*, *Access Control*, *Secure Communication Protocols*, *Data Privacy*, *Information Storage Security*, *Fundamental Principles*, *Design and Implementation*, *Physical Interfaces and Connectors*, *Hardware Architecture*, *Distributed Systems Architecture*, *Network Architecture*, *Network Implementations*, *Network Services*, *Network Defense*, *Identity Management*, *Social Engineering*, *Personal Data Privacy and Security*, *Security Governance and Policy*, and finally, *Systems Administration*.

4.3.3 Security-enhancing Platforms

4.3.3.1 Security Intelligence

The profile in the scenario of Security Intelligence is Incident Management Team Member. The most required skills on an advanced level are *Analytical Tools*, *Systems Administration*, and finally, *Business Continuity, Disaster Recovery, and Incident Management*.

4.3.3.2 Cross-Border Authentication

The scenario Cross-Border Authentication includes all the profiles of the framework, and the most required skills on an advanced level are *Data Integrity and Authentication*, *Secure Communication Protocols*, *Data Privacy*, *Identity Management*, *Social and Behavioral Privacy*, *Personal Data Privacy and Security*, *Usable Security and Privacy*, and finally, *Privacy*.

4.3.4 Framework targeted for lawyers

In addition to the framework above, UM customized a specialized framework for lawyers (see Appendix A). This is a detailed example of the construction of the framework applied in a specific profession field, and it offers valuable conclusions that can be drawn from it. This framework had some differences to the one that was used for Cyber Security professionals. The previously presented framework cannot necessarily be applied to lawyer audience, due to the semantics of profiles in some organisations. In the case of lawyers, it is more meaningful to separate between different fields of law rather than the profiles. The framework has also been simplified by reducing the granularity of the Cyber Security knowledge units.

The Cyber Security knowledge units were collected from the preceding deliverable D6.2 Education and Training Review, where nine knowledge areas were defined containing in total fifty-five different knowledge units (as seen in section 4.1 of this deliverable). For the purposes of this evaluation, some of the knowledge units were merged in order to create a more manageable evaluation form size. We made sure to only merge units within the same knowledge area, and we only merged related knowledge units, where we do not expect the differences between them to be of any large significance when looking at them from the legal perspective. We have merged *Cryptography*, *Secure Communication Protocols* and *Cryptanalysis*; *Access Control* and *Data Integrity and Authentication*; *Implementation*, *Deployment and Maintenance* and *Analysis and Testing*; *Hardware Architecture* and *Physical Interfaces* and *Connectors*; *Network Architecture*, *Network Implementations* and *Network Services*; *System Management*, *System Testing* and *System Retirement*; *System Access* and *System Control*; *Personnel Security*, *Security Program Management* and *Security Operations*; *Component Design* and *Component Procurement*; *Design* and *Fundamental Principles*; *Analytical Tools* and *Cyber Security Planning*; and *Cyber Law* and *Cyber Policy* knowledge

units. From the starting fifty-five knowledge units, the number of input fields in the evaluation form was reduced to thirty-eight.

The same as in the case of Cyber Security knowledge units, there are also many fields of law. Here there is an added complexity of slight differences of perception or rather exactly what is included in each of the fields between different countries/legal systems. As it is not expected for participants to use hours for studying and filling out the entire form, we have again chosen to simplify the structure of the included fields of law.

For the fields of law, we chose to include the four main fields of law (*Administrative law*, *Civil law*, C*riminal law*, and *Constitutional law*) to cover as wide an area of law as possible. Additionally, some of the more specific fields were also included (*Arbitration law*, *European law, Tax law*, *International law*, *Commercial law*, *Banking and finance law*, *Transport law*, *Family law and the law of persons*, *Medical law*, *Intellectual property law*, and *Damages and restitution law*). They were included as subcategories of the general four fields and on the basis that they were more likely to require Cyber Security knowledge. Again, we did not want to overwhelm the participants with too many combinations of knowledge units and fields of law. Altogether, we have included fifteen fields of law.

5 Analysis of skills importance based on our framework

5.1 Summary of the skill evaluations of the scenarios

Even though skill requirements related to the scenarios represent the scenario writer's point of view, we can draw some conclusions. First of all, for people working in a certain work environment, such as staff working in the university, the variance of required skills can be vastly different depending on the role. Therefore, some general Cyber Security programs targeted to a certain work environment might be useful to some extent, but to efficiently bring value to the target group, there is a need for well-justified and customized skill education for a certain professional group. Secondly, analysis of a scenario of this kind, in the form of standard and easily comparable table framework, may help point the breadth of required skills. The framework can help visualize Cyber Security fields that could be highly relevant for the profession, but are difficult to come up with when considering a certain work group. For instance, when considering Cyber Security education offering in general for IT professionals, usability skills might often be overdriven by technical skills, but the skill *Usable Security and Privacy* is required in many of our scenarios on an advanced level. Third, this kind of illustration reveals overlapping in education needs, and may help combine different target groups when arranging Cyber Security education.

The scenarios and related evaluations represent how security requirements can be defined for the certain profession group. Generally, the framework is the most suitable to be applied as traditional IT fields, but as presented in Section 3.4, we can apply the framework for non-IT fields as well. We discuss the framework applied to lawyer audience further in Section 5.3. From the scenario evaluations, we can conclude, that the skill requirements are of course related to the context (environment and roles) of the scenario, but the main needed skills are Data Integrity and Authentication, Access Control, Secure Comminication Protocols and Usable Security and Privacy. Less required skills are related to Cryptanalysis, Design, Component Procurement and System Thinking. In general, most scenarios require rather broadly various Cyber Security skills.

5.2 Expert evaluation of the framework including all skills

After the required skills and their importance (on the scale 0-3) in each of the scenarios were evaluated, we gathered information from companies involved in the project on the importance of all skills for all professionals described in our framework (in other words, all profiles) based on our rating scale. We received 6 evaluations and this information was summarized as an average in the final description. The summary of the skill importance analysis is presented in Appendix A.

5.2.1 Main results for the expert evaluation

Average level of skills categories over all profiles:

1. Human Security 1.9
2. Data Security 1.7
3. Societal Security 1.7
4. Connection Security 1.6
5. Organizational Security 1.5
6. Software Security 1.3
7. System Security 1.3
8. Component Security 1.0
9. Operate and Maintain 0.7

Five most demanding profiles (based on the average over all skills)

1. Digital forensic analyst 1.8
2. CISO 1.8
3. Security operations centre manager 1.7
4. Information security officer 1.7
5. Software engineer 1.6

Five most demanded skills (based on the average over all profiles)

1. Personal Data Protection and Privacy 2.3
2. Secure Communication Protocols 2.2
3. Data Integrity and Authentication 2.2
4. Data Privacy 2.2
5. Access Control 2.1

It is interesting to note that four out of the five most demanded skills are from the Data Security category.

Five least demanding profiles (based on the average over all skills)

1. Company lawyer 0.8
2. Data protection lawyer or consultant 1.1
3. Chief compliance officer 1.4
4. Policy manager 1.4
5. Network administrator 1.5

Five least demanded skills (based on the average over all profiles)

1. Cryptanalysis 0.6
2. Customer Service and Technical Support 0.7
3. Component procurement 0.8
4. System Retirement 0.9
5. Component Reverse Engineering 1.0

The number of answers is quite low, thus all the results are only indicative and may be slightly biased. Future work, including surveys and using relevant stakeholder expertize will be utilized to further validate the skill ratings with a larger audience. We plan to expand the validation in the D6.6.

5.3 Framework applied to lawyer audience

To demonstrate the framework applicability to the non-ICT audience, in this section we will present, as a special case, our framework applied to lawyers.

5.3.1 Expert evaluation

Cyber Security is a broad subject that includes many different fields, and consequently, the related knowledge (knowledge unit) is also very varied. They include everything from human behaviour to cryptography knowledge on the structure and inner workings of the cryptography primitives. Similarly, the law is also a large and diverse subject that includes fields as varied as constitutional law and criminal law. Based on how diverse both Cyber Security and the subject of law are, it becomes evident that the majority of Cyber Security knowledge units are not required for the professionals working in any specific field of law. However, there still remains the question of which Cyber Security knowledge units are important when

working in which field of law. We have therefore focused our work on gaining the information on which Cyber Security knowledge is the most relevant for those working as lawyers or related professions in a particular field of law.

To ascertain which Cyber Security knowledge is most often used by the law professionals, we have created a form (see Appendix A). The form was used to evaluate how crucial individual Cyber Security knowledge units are for professionals working in a given field of law.

For each of the combinations of the Cyber Security knowledge units and the fields of law (570 combinations), the participants could evaluate the importance of the knowledge for the field with values from zero to three, where:

- 0 - Knowledge of this topic is practically never required
- 1 - Knowledge of this topic is sometimes required
- 2 - Knowledge of this topic is often required
- 3 - Deep knowledge of this topic is important and is almost always required

5.3.2 Results for lawyers

The form for gathering data on the importance of Cyber Security knowledge in the field of law was distributed to the law experts working in the CyberSec4Europe project. Due to the nature of the project and the partners involved, which are primarily focused on Cyber Security research or are companies working in this field, the pool of potential participants was limited. The main drawback of the small number of participants is a fairly high deviation between answers in certain parts of the questionnaire. We will address this in the analysis of the data; however, regardless of this issue, the collected responses were enough to show patterns and give some interesting information about the importance of Cyber Security knowledge (and which types of knowledge are more important) in the fields of law.

Let us first address the most crucial question of which Cyber Security knowledge do lawyers consider the most important to have overall. In descending order, the most important and close second are the knowledge of *Privacy* and *Personal Data Privacy and Security*, then followed by *Data Privacy*, *Information Storage Security*, and *Cyber Law & Cyber Policy*. Clearly, the emphasis is on privacy, data privacy and its storage. Units *Privacy* and *Personal Data Privacy and Security* have on average and combined across all fields of law been evaluated at over 2 and 2,1 respectively (on the 0 to 3 scale) on the frequency of its usage, which is very high. When looking at the least useful Cyber Security knowledge for lawyers, the results indicate entire knowledge areas of *System Security*, *Connection Security* (with the exception of *Physical Media* unit), and *Component security* (with average scores across all fields of law as low as 0,36 out of 3).

When looking at the fields of law that were judged to require the most Cyber Security knowledge overall, the winner was *Banking and finance law* (average just below 1,6 out of 3 across all Cyber Security knowledge units), followed closely by *Criminal law* (average slightly above 1,5 out of 3 across all Cyber Security knowledge units). Other fields of law that have also scored reasonably high, but nowhere close to the first two are the *Commercial law*, *European law*, and *Intellectual property law*. All in all, an understandable selection, given the risks and involved technologies in the mentioned fields, with a slight exception to the field of *European law*, which has scored extremely highly in the knowledge areas related to (data) privacy and organizational security management (this is very likely in reference to the GDPR). On the other end of the scale are the fields of law that were evaluated as least likely to require any Cyber Security knowledge. There were three fields that were clearly singled out in this regard. They were (in order of least required knowledge to most), *Constitutional law*, *Family law & the law of persons*, and the *Arbitration law*, with averages across all Cyber Security knowledge units of 0,52, 0,54, and 0,63 out of 3 respectively.

We have previously mentioned the deviation among answers of different participants. On closer inspection, it becomes clear that these differences are not uniformly distributed but are clustered around specific fields of law and Cyber Security knowledge units. When comparing these sections with the results mentioned so far, it becomes apparent that the knowledge areas that were marked as important to have and fields of law that were marked as requiring more Cyber Security knowledge are the areas of higher deviations among participants. On the other hand, all the knowledge units and fields of law that were scored low have much smaller differences between participants. This would indicate that the participants agree on areas of Cyber Security knowledge that are of little use to a lawyer but are not as united in their estimations of exactly how important are fields of knowledge to a field of law when they are relevant and useful to lawyers. While this research gives good indications regarding relevant Cyber Security knowledge in fields of law, to gather conclusive evidence a much larger base of law professionals would have to participate, which is unfortunately impossible in the scope of our project. In the future, expanding the experiment to involve the participants from the entire Cyber Security Competence Network could help bring more conclusive results.

Among Cyber Security knowledge units, we have also noticed a few that were very important when working in a certain field of law, while they were scored as not required in all other fields of law. The prime examples of this are the knowledge areas of *Digital Forensics* and *System Access & System Control*, which has scored very highly for *Criminal law*. Others examples include *Data Privacy*, which as stated before scored very highly across all fields of law, however, it was marked exceptionally highly (on average 2,6 out of 3) in *Medical law*; *Personal Compliance with Cyber Security Rules/Policy/Ethical Norms*, which scored highly for *Banking and finance law* and *European law*; *Cybercrime* and *Cyber Law & Cyber Policy*, which both scored extremely highly in *Criminal law* (*Cybercrime* received on average 3 out of 3) and *Banking and finance law*.

To summarize the results of the assessment of Cyber Security knowledge required to work in the field of law, the primary knowledge that is used in the majority of the fields of law and is the most likely to come in useful regardless on which of these a lawyer works on is the knowledge concerning privacy and data privacy. This types of knowledge should, therefore, be primarily included in more general or basic courses offered to lawyers. Some specific profiles of lawyers, like those working in the fields of banking and finance law or criminal law, should receive much more extensive training, covering a much more broad spectrum of Cyber Security knowledge. Results of the assessment are illustrated in Appendix A.

6 Conclusion

Regarding Cyber Security education for professionals, there is a recognized need for example for exercises and awareness, competences and certifications, and competence-building by Cyber ranges as digital competence building programs within Europe.

To improve the situation, various means are needed, such as market studies regarding industry demands and characteristics of Cyber Security professionals. Also, an European-level certification scheme should be developed. In addition, an European-wide education framework for Cyber Security should be developed. For these, appropriate representatives at national and international level should be involved and the outcomes should be generally accepted on an international level.

What can the expected as a benefit from improving Cyber Security education of professionals, is increased awareness and increasing number of Cyber Security professionals, reduced cyberattacks and their impact both in economic terms and consumers' trust, and producing a more secure and reliable European ecosystem. Also, ensuring a new and prepared generation of cyber specialists is necessary for maintaining and increasing the Cyber Security maturity level of the sector. A regulatory Cyber Security framework applied to all players (EU and non-EU working in EU) will reduce uncertainty, ensure comparability and allow for more competitive solutions on a global basis.

We have analyzed the most relevant European frameworks related to Cyber Security professional education. We have built a framework with related skill descriptions, and described four use cases that include twelve scenarios and built the related profile descriptions derived from the scenarios. We have evaluated the skills required in each of the scenarios, and evaluated the profiles and what is their average Cyber Security skill level required in each of the scenarios according to a four-step skill rating scale. Also, we have analyzed the required skill level, in other words skill importance, in each profile of the framework by conducting an expert evaluation within organizations. In this evaluation, organizations evaluated the relevant skill level according to a four-step skill rating scale from their point of view, for each of the professional profiles. From these evaluations, an average number was constructed. As a special case, a framework targeted to lawyers is constructed.

From the skill evaluation in the scenarios we can conclude, that the variance of required skills can be vastly different depending on the profile even in same working environment, thus, to efficiently bring value to the target group, it might useful to offer well-justified and customized skill education for a certain professional group. Analysis of a scenario in the form of comparable table framework may help point the breadth of required skills. The framework can help visualize relevant Cyber Security fields, but are difficult to come up with when considering a certain work group, for instance, regarding usability skills. This kind of framework illustration reveals overlapping in education needs, and may help combine different target groups when arranging Cyber Security education.

From the framework skill assessment we can conclude, that applying framework is rather easy process, and gives an evaluation of the required skills in an comparable and understandable way, to motivate education program development for a certain professional group. The framework is flexible to be used to a certain profession group, as can be seen from the case in section 5.3, where we applied the framework for lawyers.

Our initial results from the framework assessment are, that the most demanded skills are in a declining order Personal Data Protection and Privacy, Secure Communication Protocols, Data Integrity and Authentication, Data Privacy and Access Control. The most demanding profiles are Digital Forensic Analyst, Chief Information Security Officer, Security Operations Centre Manager, Information Security Officer and Software Engineer, whereas the most demanded skill categories over all profiles are Human Security, Data Security, Societal Security, Connection Security and Organizational Security.

As the number of skill level evaluators is rather small, there is a need to refine the results further with a larger number of evaluators. Future work will include extended validation of the framework and refining results with the help of surveys and consulting relevant experts in the field.

7 Bibliography

NICE2016 W. Newhouse, S. Keith, B. Scribner, and G. Witte, "A Guide to the National Initiative for Cybersecurity Education (NICE) Cyber Security Workforce Framework (2.0)," Auerbach Publications, 2016.

NICE2020 Petersen, R. Santos, D. Smith, M.C. Wetzel K.A. Witte G. Workforce Framework for Cybersecurity (NICE Framework) NIST Special Publication 800-181 Revision 1, 2020.

A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin, "The Cyber Security Body of Knowledge (CyBoK) 1.0," 2019.

CyBOK2020 Hallett, J. Nautiyal, L. Shreeve, B. Rashid, A. "CyBOK Mapping Reference 1.1."2020

ECSO2018, "Gaps in European Cyber Education and Professional Training," 2018.

ECSO, "WHITE PAPER Information and Cyber Security Professional Certification," 2018.

The Association for Computing Machinery (ACM) The Association for Information Systems (AIS) The Computer Society (IEEE-CS), "Computing Curricula, the Overview Report," 2005. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf

CSEC2017 Joint Task Force (ACM, IEE-CS, AIS SIGSEC, IFIP WG 11.8), "Curriculum Guidelines for Post-Secondary Degree Programs in Cyber Security - A Report in the Computing Curricula Series Joint Task Force on Cyber Security Education," 2017.

The European Digital Strategy https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy (access date 1.12.2020)

European ICT professional role profiles - Part 4: Case studies http://www.ecompetences.eu/wp-content/uploads/2018/05/CWA_Part_4_EU_ICT_PROFILES_CASE_STUDIES.pdf

QIS: Job profiles for information security 2.0. A basis for uniform qualification of information security professionals http://nioc.nl/archief/proceedings/NIOC2015/NIOC%20-%20Slides-Proceedings/Donderdag%20N-091/N-091-artikel.pdf

ECSO Report: Results on simulation-based Competence Development Survey http://www.ecs-org.eu/documents/publications/5fad53f4ac4ed.pdf

ENISA2019 De Zan, T. Di France, F. Cybersecurity Skills Development in the EU - The certification of cybersecurity degrees and ENISA's higher education database, 2019. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/at_download/fullReport (access date 1.12.2020)

ECSO2020 Input from the European Cyber Security Organisation (ECSO) to the Horizon Europe Programme – 2021-2027 https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf

WG5ANALYSIS Information and Cyber Security Professional Certification Task Force WG5 I European Human Resources Network for Cyber, ECSO, 2020. https://ecs-org.eu/documents/publications/5fdb27c54ac93.pdf

Annex A: Framework illustration

In this section, we present a visual description of the developed framework functions. Figures 12 and 13 illustrate the developed framework, that is used for skill evaluation. For each profile, e.g. Company Lawyer, and under each category, e.g. data security and its subcategory, cryptography, the skill is given a relevant value. More precisely, skills are evaluated by organisations on a scale between 0-3, and after collecting all the evaluations, an average number of the values is constructed. Figures 14-18 illustrate skill evaluations in the scenarios, that are presented in 3.4.1. Figure 19 presents a special case of the framework by illustrating evaluation of skills with framework targeted to lawyers, derived from the scenario Cyber Security for Lawyers (CS). See section 5.3 for more precise description of how the special case framework was constructed.

D6.2, Section 3.4	Knowledge area			
Profile / Description	**Knowledge unit**	**Cryptography**	**Digital Forensics**	**Data Integrity and Authentication**
Company Lawyer	Person that is in charge of ensuring the legality of commercial transactions, advising corporations on their legal rights and duties, including the duties and responsibilities of corporate officers. They must also negotiate agreements with different parties and verify all accounts and finances for business transactions. Another key task corporate lawyers are involved with is navigating the provisions of a company's constitution, shareholder and directors' rights.	0.80	0.40	1.20
Data Protection Officer	Person in charge of ensuring that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. In charge of implementing the data protection plan in a company and assuring the fulfilment of the data protection regulation GDPR. also trains the personnel.	1.80	1.00	2.40

Figure 12: An illustration of the developed framework with evaluated skills

Dynamic security deployment manager	Person in charge of managing the secure network deployment of the different components willing to join the network (initial assessment, initial configuration, information obtaining, etc.).	1.50	0.75	1.75
	AVERAGE	1.46	0.98	2.19
None	The skill or knowledge is not necessary to perform in the given specialization			
Basic	Understanding the basic principles of the skill or knowledge is needed in the specialization. Application of these is not necessary to perform in the specialisation			
	Applying the skill or knowledge is needed to			

Figure 13: An illustration of the developed framework with evaluated skills

D6.2, Section 3.4	Knowledge area			
Profile / Description	Knowledge unit	Cryptography	Digital Forensics	Data Integrity and Authentication
Data protection lawyer or consultant	Person that assess a client (e.g., manufacturer, organization) about the compliance of the regulation GDPR, in order to ensure that the products are in line with it.	1	0	0
Security certification agent	Person in charge of evaluating the security of a system according to a specific certification scheme, processes and	2	1	2
Security Trainer	Person in charge of training personnel of an organization to be aware of the security concerns and to train them on how to avoid security issues. This could include group sessions, cyber ranges, flagships and other techniques, depending on the organization domain.	1	0	2

Figure 14: Framework constructed of the scenarios DP, SC, ST, NA and IS

D6.2, Section 3.4	Knowledge area		
Profile / Description	Knowledge unit	Cryptography	Digital Forensics
Company Lawyer	Person that is in charge of ensuring the legality of commercial transactions, advising corporations on their legal rights and duties, including the duties and responsibilities of corporate officers. They must also negotiate agreements with different parties and verify all accounts and finances for business transactions. Another key task corporate lawyers are involved with is navigating the provisions of a company's constitution, shareholder and directors' rights.	0	0
Data Protection Officer	Person in charge of ensuring that the organisation processes the personal data of its staff, customers, providers or any other	2	0
Chief Compliance Officer	Person in charge of overseeing and managing compliance issues within their company or organization. The CCO ensures	0	0

Figure 15: Framework constructed of the scenarios IA, UI and UE

D6.2, Section 3.4	Knowledge area			
Profile / Description	**Knowledge unit**	**Cryptography**	**Digital Forensics**	**Data Integrity and Authentication**
Company Lawyer	Person that is in charge of ensuring the legality of commercial transactions, advising corporations on their legal rights and duties, including the duties and responsibilities of corporate officers. They must also negotiate agreements with different parties and verify all accounts and finances for business transactions. Another key task corporate lawyers are involved with is navigating the provisions of a company's constitution, shareholder and directors' rights.	1	1	1
Data Protection Officer	Person in charge of ensuring that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. In charge of implementing the data protection plan in a company and assuring the fulfilment of the data protection regulation GDPR. also trains	3	2	3

Figure 16: Framework constructed of the scenario CL

Network administrator	Person in charge of configure and manage the network components in an organization (security, identity, configuration, application of countermeasures). This person is also in charge of updating the firmware of the components.			
Incident management team member	Person responsible of monitoring the state of the system, detect incidents and decide the appropriate mitigations and actions to avoid or reduce the risk and the impact over the system.	0	1	1
Cloud Trust Manager	Person in charge of managing the reputation in distributed systems, allowing de-anonymization of the real owner identity of the associated shared data in case of law enforcement inspection is needed.			

Figure 17: Framework constructed of the scenario SI

Company Lawyer	Person that is in charge of ensuring the legality of commercial transactions, advising corporations on their legal rights and duties, including the duties and responsibilities of corporate officers. They must also negotiate agreements with different parties and verify all accounts and finances for business transactions. Another key task corporate lawyers are involved with is navigating the provisions of a company's constitution, shareholder and directors' rights.	0	0	1
Data Protection Officer	Person in charge of ensuring that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. In charge of implementing the data protection plan in a company and assuring the fulfilment of the data protection regulation GDPR. also trains the personnel.	0	0	3

Figure 18: Framework constructed of the scenario CB

	Fields of cybersecurity	Knowledge area / Knowledge unit	Data Security: Cryptography, Secure Communication Protocols & Cryptoanalysis	Data Security: igital Forensi	Data Security: Access Control & Data Integrity and Authentication	Data Security: ata Priva	Data Security: ormation Storage Secu
ds of	Administrative law		1.4	1.2	1	1.4	1.4
		Arbitration law	0.8	0.6	0.8	1.4	1
		European law	1.4	1	1.2	1.8	1.6
		Tax law	1.2	0.8	1.2	1.6	1.4
		International law	1.6	1.2	1.2	1.4	1.4
	Civil law		1.6	1.2	1	1.6	1.4
		Commercial law	1.2	1.2	1.2	1.8	1.6
		Banking and finance law	2	1.6	1.6	2.2	2.2
		Transport law	1.4	0.8	1	1.6	1.6
		Family law & the law of	0.6	0.2	0.6	1.6	1.4
		Medical law	1.2	0.8	0.8	2.6	2.2
		Intellectual property law	1.8	1.8	1.4	1.8	1.8
	Criminal law		2	2.4	1.8	2.2	2
		Damages and restitution	1	1	1	1.8	1.4
	Constitutional law		0.6	0.4	0.6	1.2	1
	SUM for cybersecurity a know		1.320	1.080	1.093	1.733	1.560
0	Knowledge of this topic is practically never required						
1	Knowledge of this topic is sometimes required						
2	Knowledge of this topic is often required						
3	Deep knowledge of this topic is important and is almost alwa						

Figure 19: Framework applied in skill evaluation of lawyers (Scenario CS)