Cybersecurity Optimisation and Training for Enhanced Resilience in Finance

D6.2 – Competence Catalogue (II)

[WP6 – Cybersecurity Training in Finance]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Lead Contributor	Paul Rabel, Uni Graz
	paul.rabel@uni-graz.at
Other Contributors	Eva-Maria Griesbacher, Uni Graz
	Martin Griesbacher, RISE
	Robin Renwick, Trilateral (External Review)

Due Date	31.10.2020
Delivery Date	31.10.2020
Type	Report
Dissemination level	PU = Public

Keywords	Cybersecurity, Competence, Finance, Threat Taxonomy, Competence Catalogue

Document History

Version	Date	Description	Reason for Change	Distribution
V01r00	04.06.2020	Draft	Updated ToC	04.06.2020
V01r01	16.06.2020	Draft	Preliminary Catalogue	16.06.2020
V01r02	24.06.2020	Revision	First review by RR	24.06.2020
V01r03	14.07.2020	Revision	Section 1 + 2; CC + ToC adjusted	14.07.2020
V01r04	07.09.2020	Revision	Integration of D2.1, change of structure	07.09.2020
V01r05	30.09.2020	Revision	Feedback (UNIGRAZ, RISE) integrated	30.09.2020
V01r06	23.10.2020	Revision	Expanded S3, finalised S4	23.10.2020
V01r07	27.10.2020	Revision	Internal Review	27.10.2020
V01r08	28.10.2020	Revision	External Review	29.10.2020
V01r09	30.10.2020	Revision	2nd Internal Review	30.10.2020
V02r00	31.10.2020	Final Version		31.10.2020

Abstract

The overarching goal of SOTER's Work Package 6 is to achieve enhanced cyberresilience in the financial services sector by a set of training activities. This deliverable is the second iteration of the competence catalogue. Within the first iteration (D6.1), general digital competences were outlined. Building up on D6.1, this document aims to provide a systematic competence catalogue of cybersecurity competences relevant to employees in the financial services sector. It is specifically targeted at regular employees in the financial services sector with different levels of previous education in cybersecurity. The financial services sector, as defined by SOTER, includes traditional banks as well as FinTechs. Within this document, numerous additional competences are defined, accounting for the particular requirements of the financial services sector and SOTER'S onboarding platform. These are intended to serve as the basis for the training actions to be conducted in WP6.

This deliverable has been developed through cooperation and coordination of the social science research partners, UNIGRAZ, RISE, and TRI. For the development of the competence catalogue, the mapping conducted in D2.1 provided a theoretical foundation for a human factor-based categorisation of competences.

Firstly, Section 2 of the document provides an overview of relevant definitions of "cybersecurity" and "competence" alongside with their theoretical underpinning. In Section 3, a literature review is conducted, analysing previous approaches to cybersecurity competence and discussing their limitations. Section 4 then elaborates on the threat taxonomy introduced in D2.1 and attempts to establish whether the previously identified competences within literature are sufficient for the purpose of SOTER. Lastly, Section 5 provides the competence catalogue in tabular form, listing all trainable elements of each competence. Section 5 also includes remarks on the methodology applied for the creation of the competence catalogue.

Table of contents

ABSTRACT 3

EXECUTIVE SUMMARY 6

LIST OF FIGURES 8

LIST OF TABLES 8

LIST OF ACRONYMS AND ABBREVIATIONS 8

1 CYBERSECURITY COMPETENCES IN FINANCE - INTRODUCTION 9

1.1 SCOPE OF THIS DELIVERABLE 10
1.2 STRUCTURE OF THIS DELIVERABLE 11
1.3 RELATION TO OTHER TASKS AND DELIVERABLES 11

2 DEFINITIONS AND METHODOLOGY 13

2.1 WHAT IS "CYBERSECURITY"? OVERVIEW OF AN EMERGING TERM 13
2.2 COMPETENCE AS AN EVOLVING CONCEPT 14
2.3 CYBERSECURITY COMPETENCE 16
2.4 METHODOLOGY OF THE LITERATURE REVIEW 16

3 PREVIOUSLY IDENTIFIED CYBERSECURITY COMPETENCE APPROACHES 18

3.1 LIMITATIONS OF THE LITERATURE REVIEW 18
3.2 PREVIOUS APPROACHES 19

4 MATCHING THE MAPPING – UNDERSTANDING THREATS AND ATTACK VECTORS 22

4.1 THREATS AND ATTACK VECTORS - THE CAPEC™ RESOURCE 22
4.1.1 PARAMETER INJECTION 24
4.1.2 IDENTITY SPOOFING 24
4.1.3 RESOURCE LOCATION SPOOFING 29
4.1.4 ACTION SPOOFING 30
4.1.5 SOFTWARE INTEGRITY ATTACK 31
4.1.6 INFORMATION ELICITATION 33
4.1.7 MANIPULATE HUMAN BEHAVIOUR 33
4.1.8 OBSTRUCTION (PHYSICAL SECURITY) 36
4.2 THREATS AND IDENTIFIED COMPETENCES IN LITERATURE 37

5 THE COMPETENCE CATALOGUE 39

5.1 NOTES ON THE ITERATIVE CREATION PROCESS 39
5.2 CYBERSECURITY COMPETENCE CATALOGUE 40

6 REFERENCES 56

Executive summary

SOTER is a European Commission H2020 funded project, entitled *'cyberSecurity Optimisation and Training for Enhanced Resilience in finance'* (SOTER). This deliverable is part of SOTER's Work Package (WP) 6 requirements and is entitled *D6.2 – Competence Catalogue (II)*. The overarching goal of SOTER's Work Package 6 is to achieve enhanced cyberresilience in the financial services sector by a set of training activities. The deliverable is the second iteration of the task entitled *T6.1 – Development of Competence Catalogue and training modules*. It responds to the information requested in the Description of Action (DoA):

"The Competence Catalogue will be the basis for creating the training modules. It will be fed by the activities developed in T2.1, and the definition of essential competencies for responding to cybersecurity threats and attacks."[1]

Within the first iteration (D6.1) of this deliverable, general digital competences were outlined. Building up on D6.1, this document aims to provide a systematic competence catalogue of cybersecurity competences relevant to employees in the financial services sector. It is specifically targeted at regular employees in the finance sector, with different levels of previous education in cybersecurity. The financial services sector, as defined by SOTER, includes traditional banks as well as FinTechs. Within this document, numerous additional competences are defined, accounting for the particular requirements of the financial services sector and SOTER'S onboarding platform. These are intended to serve as the basis for the training actions to be conducted in WP6, particularly with respect to the digital training handbook (D6.8).

This deliverable has been developed through cooperation and coordination of the social science research partners, UNIGRAZ, RISE, and TRI. For the development of the competence catalogue, the mapping conducted in D2.1 provided a theoretical foundation for a human factor-based categorisation of competences.

Firstly, Section 2 of the document provides an overview of relevant definitions of "cybersecurity" and "competence" alongside with their theoretical underpinning. In Section 3, a literature review is conducted, analysing previous approaches to cybersecurity competence and discussing their limitations. Section 4 then elaborates on the threat taxonomy introduced in D2.1 and attempts to establish whether the previously identified competences within literature are sufficient for the purpose of SOTER. Lastly, Section 5 provides the competence catalogue in tabular form, listing all trainable elements of each

[1] SOTER Description of Action, 33.

competence. Section 5 also includes remarks on the methodology applied for the creation of the competence catalogue.

List of figures

Figure 1. Interdisciplinary cybersecurity approach 13
Figure 2. Exemplary multi-stage structure of cybersecurity incidents 22

List of tables

Table 1. List of acronyms and abbreviations 8
Table 2. Skills and hands-on tasks of cybersecurity skills index (CSI) based on actual incident relevance in 2016 20
Table 3. Comparison of threats and corresponding skills and competences as identified by literature 37

List of acronyms and abbreviations

Abbreviation	Explanation
AI	Artifical Intelligence
CAPEC™	Common Attack Pattern Enumeration and Classification
CDA	Competence development and assessment framework
CDX	Cybersecurity defence exercise
CS	Cybersecurity
CSI	Cybersecurity Skills Index
DoA	Description of Action
DIGCOMP	European Digital Competence Framework
DNS	Domain Name System
ENISA	European Agency for Cybersecurity
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information Communication Technology
IS	Information Security
IT	Information Technology
LIBER	LiberBank SL.
OBVSG	Österreichische Bibliothekenverbund und Service GmbH
PT	Purple Team
RISE	Research Industrial Systems Engineering
SOTER	Cybersecurity Optimisation and Training for Enhanced Resilience in Finance
SSH	Social Sciences and Humanities
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TRI IE	Trilateral Research Ltd.
UNIGRAZ	University of Graz
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WiFi	Wireless Fidelity
WP	Work Package

Table 1. List of acronyms and abbreviations

1 Cybersecurity Competences in Finance - Introduction

> "*There are only two types of companies: those that have been hacked, and those that will be.*"
> (Robert Mueller, former FBI Director[2])

Digitalisation has transformed the finance industry in the last decades. According to the financial technology, security and compliance law specialist Tom C. W. Lin's investigations, trading is increasingly managed by autonomous, high frequency trading programmes with complex algorithms; smart machines and Artificial Intelligence (AI) do the research and risk analysis for financial institutions; Wealth management is run by Smart Software and the market making of financial institutions is done via high speed electronic communication networks (Lin 2016, 161-162). New payment systems, Bitcoin and Blockchain added to these big changes in the operations of the financial industry (ibid., 163). These observations led Lin to the conclusion that nowadays "every sophisticated financial company is essentially a tech company" (Lin 2016, 168).

Due to the rise of these new financial technologies, new risks appear for organisations, especially in the realm of cybersecurity (Lin 2016, 159). On the one hand, the very nature of the new financial technologies bring risks of widespread financial damage and crisis, even if not being manipulated malevolently. Simple, "normal accidents", as may always occur in complex, high tech systems (such as malfunctions or glitches), can cause serious disruptions to the finance sector, with cascading and spillover effects over the whole industry due to the interdependence and interconnectedness of the industry and to the widespread use of similar and interdependend code (Lin 2016, 169-171). Moreover, the high-speed nature of the new financial technology makes it hardly feasible to prevent these accidents or to intervene in time in order to limit the damage (Lin 2016, 170; Kryparos 2018, 52).

On the other hand, there are all kinds of technological threats that put financial institutions at risk just as they threaten every other business connected to digital networks. The exacerbated problem for the finance sector is that it faces the most data breaches throughout all sectors because there is potentially a lot of money to be gained with comparatively low risk of being caught or even discovered (Kryparos 2018, 46). Furthermore, cybersecurity attacks on financial institutions are often more organised than other attacks and therefore more successful (Kryparos 2018, 46). The success rate of cyber attacks on financial services was 47% in 2016 (Verizon 2017).

[2] Cowley, S. (2012). FBI Director: Cybercrime Will Eclipse Terrorism. Available at: https://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/

Technological threats are widespread nowadays, most prominently the threat of being hacked, with data or money being stolen, or information being leaked (Lin 2016, 173-174). As Lin puts it, "the robber with a gun has been replaced by the hacker with a laptop" (Lin 2016, 172). But financial institutions face threats not only from hackers as single actors, but also from competitors, foreign national secret services agencies and – primarily – organised cybercriminality (Lin 2016, 173). Internally, the security of financial institutions is threatened by "misguided" or "rogue" employees and independent contractors (Lin 2016, 174). However, as Lin points out quite accurately, "these types of bad acts and bad actors existed in the past analog eras of finance, the new high-tech nature of finance renders these malfeasances more likely, more accelerated, more threatening, and more devastating" (Lin 2016, 175).

Traditionally, financial institutions reacted to cybersecurity threats by building themselves isolated silos, where all business-sensitive data was stored and only a chosen few employees had access to (Kryparos 2018, 46). This changed dramatically due to the emergence of FinTechs, organisations which provide financial services that are available on the Internet always and everywhere (Kryparos 2018, 47). Having financial services "always on" and "always available" blurred the network perimeters of financial institutions providing these services and made it impossible for them to use the old silo-approach for all their data (Kryparos 2018, 54).

However, not every risk can be reduced by technology ("security by design"): training humans to act and interact in a secure manner with new technologies is essential. They have to acquire the competences to do that. Employees require trust and empowerment from companies in accordance with their capabilities so they can learn and perform awareness and security behaviour and thus fulfill their responsibility (Kryparos 2018, 54).

1.1 Scope of this deliverable

This deliverable is part of the requirements for Work Package 6 (WP6) for the SOTER project. The deliverable is the second iteration of the task entitled *T6.1 – Development of Competence Catalogue and training modules*. The deliverable is entitled D6.2 – *Competence Catalogue (II)*. It responds to the information requested in the Description of Action (DoA):

> "The Competence Catalogue will be the basis for creating the training modules. It will be fed by the activities developed in T2.1, and the definition of essential competencies for responding to cybersecurity threats and attacks."[3]

[3] SOTER Description of Action, 33.

This report is based on information that exists as of the deliverable date - 31st October 2020. If any details change, or further information becomes available after document submission, it will be integrated into the following deliverables, particularly the digital training handbook (D6.8).

This deliverable aims to provide a systematic competence catalogue of cybersecurity competences relevant to employees in the finance sector. It is specifically targeted at regular employees in the finance sector, with different levels of previous education in cybersecurity. The financial services sector, as defined by SOTER, includes traditional banks as well as FinTechs.

This deliverable is the second iteration of the competence catalogue. Within the first iteration (D6.1), general digital competences were outlined. Within this document (D6.2), numerous additional competences are defined, accounting for the particular requirements of the finance sector and SOTER'S onboarding platform. These are intended to serve as the basis for the training actions to be conducted in WP6.

1.2 Structure of this deliverable

This document is composed of five main sections. Section 2 provides an overview of relevant definitions and the methodology applied for the creation of the competence catalogue. Section 3 provides a literature review on previous competence approaches in cybersecurity. Section 4 then elaborates on the threat taxonomy introduced in D2.1 and attempts to establish whether the previously identified competences within literature are sufficient for the purpose of SOTER. Lastly, Section 5 provides the competence catalogue in tabular form, listing all trainable elements of each competence.

1.3 Relation to other tasks and deliverables

The SOTER project has a number of deliverables related to the human factor-based elements of cybersecurity resilience, coordinated primarily through the social science and humanities (SSH) research partners, with support and guidance from the technical partners, specific end-users drawn from the financial services sector, as well as advisory board members drawn specifically from the finance and cybersecurity sector. The social science research activities form the basis for aspects of WP2, WP5, and WP6, as well as contributing to aspects of WP5. The research tasks and associated deliverables within those work packages should be viewed as complementary to this deliverable. In summary, deliverables that relate specifically to this deliverable as of the deliverable date (M16) are:

- *D2.1 – Mapping and understanding human factors in effective cyber-security*
- *D5.1 – Standardisation focused on human aspects in cyber-security*
- *D6.3 – Training Modules (I)*

- *D6.4 – Training Modules (II)*

For the development of the competence catalogue, the mapping conducted in D2.1 is intended to provide a theoretical foundation for a human factor-based categorisation of competences. This includes three threat dimensions (motivation, agent, localisation; see Section 3.4), as well as a review of the processes related to human-factor based cyberresilience (such as organisational, individual, sociological and psychological processes). Finally, a map of threat types has been created for D2.1, which may be linked to technical threat categories such as Injects or Spoofing.

This deliverable (D6.2) has been developed through cooperation and coordination of the social science research partners, UNIGRAZ, RISE, and TRI. Cooperation is expected to continue throughout the human factor-based aspects of the SOTER research, which primarily consists of the following research actions:

- *T2.1 - Mapping and understanding human factors in effective cyber-security* (WP2)
- *WP4 - Use cases and cybersecurity awareness*
- *WP5 – Cybersecurity standard whitepaper for present and future threats in finance*
- *WP6 - Cybersecurity training in finance*

Most importantly, research actions within this deliverable will contribute to the development of a series of deliverables found within tasks related to WP6:

- *T6.2 – Hands-on Training actions for bank employees*
- *T6.3 – Training actions for new key players*
- *T6.4 – Masterclasses in cybersecurity training*
- *T6.5 – Creation of the Digital Training Handbook for cybersecurity competencies*

2 Definitions and Methodology

Within this section, definitions for essential terminology used in the remainder of this deliverable shall be laid out. Initially, the term "cybersecurity" is analysed and adapted to accommodate for the human factor-based perspective central to SOTER. Subsequently, this section focuses on exploring the theoretical background of competence and its components. Additionally, the methodology of the literature review as well as of the underlying literature research shall be explained in detail.

2.1 What is "cybersecurity"? Overview of an emerging term

In SOTER we are deploying an interdisciplinary cybersecurity ontology. A first version of this approach has been worked out in D6.3 "Training Modules Compilation (I)", which has been further defined in detail in D2.1 "Mapping of human behaviour related threats and mitigation measures (I)". This section therefore focuses on a short summary of the key elements of this interdisciplinary approach[4]:

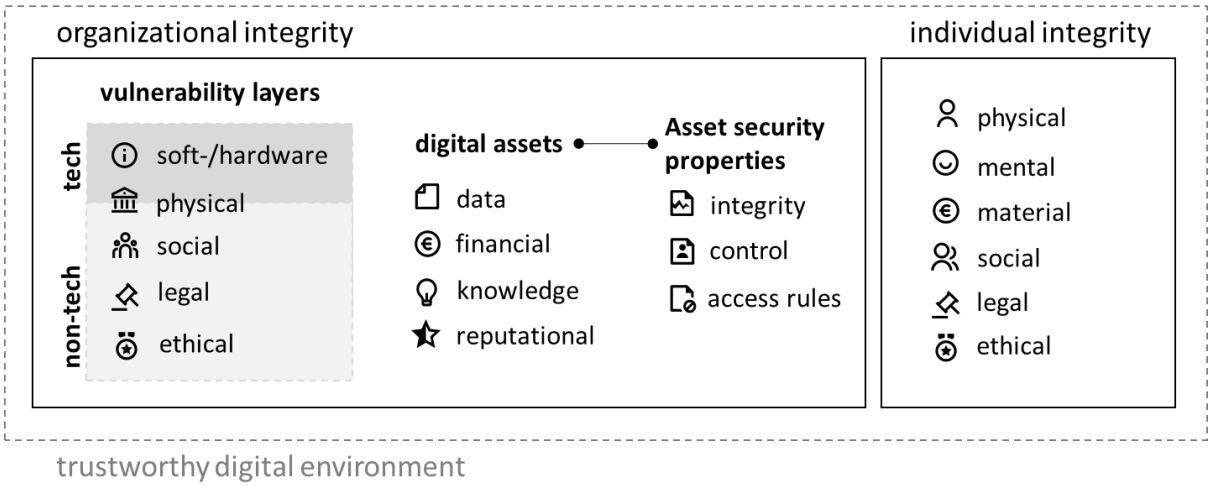

Figure 1. Interdisciplinary cybersecurity approach, Version 1.1

The general question of security addresses the protection of all *digital assets* in the organisational environment (*organisational integrity*). We identify four main types of digital assets:

1. *data*: all types of digitally stored information (e.g. personal information of customers)
2. *financial*: all digital assets which can be directly exchanged into any payment currency

[4] For this version 1.1 the figure has been slightly changed. The "soft-/hardware layer" was called "information layer" in the first version.

3. *knowledge*: know-how and intellectual property which is digitally stored or can be accessed digitally[5]
4. *reputational*: the reputation of an organisation in cyber space (e.g. user ratings)

Cybersecurity is connected to the protection of *security properties* of these assets. Security properties can be reduced to three main aspects:

1. *integrity*: the contents of the assets
2. *access rules*: the rules for accessing the asset, incl. confidentiality and availability
3. *control*: the rights to change, transfer or copy of the asset

The risk for unintended changes of security properties of digital assets (= security incidents), can be located on the following vulnerability layers of an organisation:

1. soft-/hardware layer: all soft- and hardware deployed within or connected to an organisation
2. physical layer: all potentical physical access points to an orginations digital assets
3. social layer: all personell of an organisation with access rights to digital assets
4. legal layer: all possible legal avenues for targeting an organisation
5. ethical layer: all possible ethical avenues for harming an organisation (e.g. dissemination of wrong information about the organisation)

Finally, all measures for improving cybersecurity in the context of the European Union need to take into account European values and fundamental rights. This means, all activities of an organisation targeted at improving cybersecurity need to consider causing potential harm to involved individuals, in regard to all individual integrity attributes (physical/bodily; mental/psychological; material/financial; social (connectedness); legal/rights; ethical (standards)). By adding the consideration of the individual integrity to the efforts in improving the organisational integrity, this interdisciplinary cybersecurity approach targets the overall goal of establishing a trustworthy digital environment.

2.2 Competence as an evolving concept

Similar to the term cybersecurity, *competence* has been more frequently used within academia in recent decades, potentially eclipsing other concepts such as awareness, skills or qualification. Today, there is a vast body of academic literature concerned with competence, ranging across various fields of study such as educational sciences, personnel development, psychology, industrial sciences, information security, linguistics and sociology. However, despite having been acknowledged as a central concept relevant to many social sciences, there is considerable ambiguity as to what competence actually comprises.

[5] Knowledge has become a primary asset in modern economies. Accordingly, losses and theft of knowledge have become a recognised risk for companies (see North et al. 2019; Thalmann/Ilvonen 2020).

Conversely, this is certainly an outcome of the highly interdisciplinary nature of this field of study. As a result, differing concepts of competence are being used simultaneously and inconsistently. This subsection attempts to shed some light on the debate, while establishing a workable definition of competence.

It is important to address the terminological difference on a linguistic level first. While the term "Kompetenz" is uncontested in the German-speaking area, within the Anglo-American region there is a distinction between "competence" and "competency", with the latter being significantly more popular (Bergmann and Daub 2006). The terms are not interchangeable, and while definitions vary, in general competencies describe a set of task-related skills or abilities within organisations, i.e. within a specific workfield, that may be compared according to certificates, much like any qualification (Drexel 2002; Tsohou and Holtkamp 2018). Moreover, a large portion of Anglo-American academia focuses on prerequisite terms such as *skills*, *capabilities* or *capacities*, further exacerbating efforts towards attaining a consistent terminology. Continental European research has seemingly moved towards a more holistic understanding of competence, with a focus on independent problem-solving and problem-oriented solution behaviour (for instance, see Ferrari et al. 2013, 37).

Nonetheless, the distinction above highlights what may be considered to lie at the heart of the debate: Whether competence is a concept merely distinguished by its explicit relation to a specific task within a specific (work) context, or whether it entails a fairly broad approach applicable to a wide range of comparable situations (see also Windeler 2014, 10; Kurtz 2010, 13). Thus, it is useful to bring the overarching goals of SOTER and the deliverables within WP6 to mind. Firstly, as was established in the previous subsection, cybersecurity is a multi-layered, complex concept, which also accounts for the dynamic, ever-changing nature of the digital world. Accordingly, cybersecurity threat taxonomies may only be exhaustive temporarily, as attack vectors and threats are constantly evolving. Secondly, this deliverable aims to provide a foundation for the SOTER training actions. Convincingly, this implies that any conceptualisation of competence that is focused on its relation to specific tasks will fall short of providing employees in the finance sector with the necessary training to achieve lasting cyberresilience.

Therefore, for the competence catalogue we have adopted the continental European definition of *competence* provided by Empirical Educational Research and Personnel Development, since it is interdisciplinary and covers nearly all aspects we deem necessary for effective training actions. Competence is thus defined as the general capability of persons to act and solve problems independently in a given situation based on their abilities, knowledge, skills, proficiency and attitude (Müller-Frommeyer 2017, 308; Arnold et al. 2010, 173; Kaufhold 2006, 21-25). While many definitions in Empirical Educational Research locate the realisation of competence only within the individual (Kurtz 2010, 8),

from a sociological perspective said realisation is necessarily contextual. As research on the subject of the performance of competences has shown, competences can only be realised in and through the consent of the social system in which the individual is situationally located (ibid.). Individuals not only need the capability to act competent, they also need the authority to do so (Pfadenhauer 2010). Furthermore, there is another aspect to be considered, as individuals need to be motivated or willing to perform their competences in a given situation as well (ibid.).

Adjusted for these aspects of the realisation of competences, we define competence as the *general capability, willingness and agency of individuals to act and solve problems independently or in cooperation with others in a given situation based on their abilities, knowledge, skills, proficiency and attitude*.

2.3 Cybersecurity Competence

Thus, bringing the aforementioned definitions of competence and cybersecurity together, *cybersecurity competence* is the *capability, willingness and agency of individuals to solve cybersecurity problems individually or in cooperation with others based on their knowledge, skills, attitude and proficiency in a way that the organisational integrity (technical, social, legal, ethical) and the physical, mental, material, social, ethical and legal integrity of the individuals involved is safeguarded.*

2.4 Methodology of the literature review

For the desk-based research that served as a foundation for this deliverable, a literature review was conducted. The objectives were to, firstly, establish a workable definition of competence based on the most relevant literature (Section 2), and secondly, to identify competence approaches with similar theoretical and conceptional grounding (Section 3).

Following established literature review methodology, a search of academic databases such as ScienceDirect, OBVSG[6] and WebOfScience was conducted. The first round of the search included search terms such as “cybersecurity”, “competence” and “cybersecurity competence”. As the first two terms proved to be rather broad and the latter term merely yielded a few relevant results, the search was then expanded to include synonymous terms such as “IT security”, “information security”, “competency”, “awareness”, and any combination of those. At multiple points during the review, web resources such as cybersecurity training courses (for instance the European Cyber Security Month[7]) were also considered. Literature related to “cybersecurity training” and other variations of the term

[6] www.obsvg.at
[7] Available at https://cybersecuritymonth.eu/

was analysed as well, in the hopes of gaining additional insight and material. After further refinement and a few iterations of the literature search, the literature analysed in Section 3 was selected. This was based on two selection criteria; firstly, the theoretical fit of the employed competence approach with our definition, and secondly the proximity of identified competences to useful competences within the finance sector (the project's context).

3 Previously identified Cybersecurity Competence approaches

According to the methodology outlined above, a literature review on cybersecurity competence approaches was conducted. This section aims to briefly discuss the identified academic literature, while also establishing why further refinement of competence approaches was necessary.

3.1 Limitations of the literature review

Regarding competence (trainings) in sectors apart from banking and finance, there appears to be little research. The reasons for this are manifold and shall be briefly outlined here. Firstly, as has been noted by Carlton et al. (2019), many organisations have focused on cybersecurity awareness programs in the past. The resulting dominance of awareness trainings certainly increased employees' exposure to cybersecurity topics, however, they typically only affected employees in the short run, severely limiting the applicability of awareness trainings to skill (and competence) development (Whitman and Mattord 2018).

Secondly, academia is far from having established a consistent terminology regarding competence, as was already outlined in Section 2. This may in part be attributed to the highly interdisciplinary nature of this branch of research, as competence development has been subject to studies in fields such as information security, computer science, educational science or sociology. Additionally, on a linguistic level, the distinction between "competence" and "competency" (with the latter being significantly more popular within the Anglo-American region) certainly exacerbates efforts towards attaining a consistent terminology. As a result, most of academia focuses on usually prerequisite aspects of competence, such as cybersecurity education (knowledge) or skills.

Lastly, returning to the organisational level, most private companies design and implement cybersecurity trainings considering recent security incidents affecting the company. Hence, cybersecurity trainings in private companies typically focus on particular aspects of cybersecurity, such as increasing employees' password security (Eminağaoğlu et al. 2009). Accordingly, the short-term perspective employed by corporations suggests that it is likely that empowering employees by (holistic) competence trainings may be perceived as too unspecific or costly, and thus not feasible. In addition, the perspective employed by organisations may also contribute to a rather narrow focus within scientific research, as it is also a matter of feasibility (i.e. cost and/or time) to conduct large-scale experiments, as well as to gain access to statistically significant amounts of data.

Nevertheless, there are studies that provide somewhat comprehensive analyses of notions prerequisite to competence, such as skills. In the following section, the most promising studies regarding cybersecurity competence shall be reviewed.

3.2 Previous approaches

Brilingaitė et al. (2020)

Brilingaitė et al. (2020) discuss competence development and assessment in the context of cybersecurity defence exercises (CDX). While the authors focus primarily on ICT or CS professionals, their study design also yields some insight regarding non-ICT professionals (end-users). Namely, the so-called hybrid CDX conducted included both an external and internal team representing employees of a simulated organisation and business end-users.

They find that proper arrangement of CDX could enable the development of competencies of all involved participants. CDX is a resource-intensive event, and it could be used more effectively than just for a specific group of individuals (Brilingaite et al. 2020). Their results show that non-ICT professionals (also called "Purple Team" (PT) members) also gain knowledge about cybersecurity, and they would like to be involved more actively than usual. PT members represents business users, decision-makers, managers, and non-technical users whose actions have a considerable impact on cyberresilience in any organisation. Thus, organisations could include specific tasks for PT members in the scenario to increase their cybersecurity awareness (Brilingaitė et al. 2020). For the PT members, a set of skills was defined:

- Firewall
- Specialised Software
- Network Analysis
- Forensics
- WindowsOS
- Linux
- Database Admin
- Soft skills
- Other skills

However, the authors do not elaborate further on the actual tasks associated with the above skills. Therefore, it is debatable which and how many of those skills are actually relevant to employees in the finance sector. Most importantly, though, the authors' theoretical underpinning of the employed competence approach remains unclear. Therefore, due to the narrow approach to the term competence and the significant costs incurred by CDX, the paper by Brilingaitė et al. (2020) only provides general guidance for the purpose of this deliverable, and may not serve as a foundation for the competence catalogue. However, the competence development and assessment framework (CDA) developed by Brilingaite et al. (2020) features an assessment focus and draws from the

ENISA and NIST frameworks (ENISA 2016; NIST 2017). This served as a useful point of reference when attempting to draw up the threat taxonomy in Section 4. Additionally, the authors' insights regarding training development and assessment may be highly relevant for other tasks within WP6, such as the training modules creation.

Carlton et al. (2019)

The study conducted by Carlton et al. (2019) develops a cybersecurity skills index (CSI) comprised of nine platform-independent cybersecurity skills for non-IT professionals. The authors reviewed literature (MacMillan and Yadron 2014) on recent cyber attacks and identified 12 cybersecurity threats, along with their corresponding skills. A panel of cybersecurity experts then ranked threats and skills according to their importance and relevance, finally yielding a list of the top 9 cybersecurity threats and corresponding skills (see Table). The authors define cybersecurity skill as "an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security to mitigate cyber-attacks (ibid. 2019, 102; Carlton et al. 2016).

Carlton et al. assigned a set of four scenario-based, hands-on tasks, increasing in difficulty to each of the nine skills. The more difficult tasks only unlocked when participants completed the previous ones. Thus, for each cybersecurity skill, participants may be assigned a skill level corresponding to a quartile. Aggregating the results for all nine skills, employees may be ranked according to the CSI and trained accordingly. The concept was transferred into an app for scenario-based, hands-on tasks (MyCyberSkills™, Carlton et al. 2016).

Skill
Preventing the leaking of confidential digital information to unauthorised individuals
Preventing malware via non-secure websites
Preventing PII theft via access to non-secure websites
Preventing PII theft via email phishing
Preventing malware via email
Preventing credit card theft by purchasing from non-secure websites
Preventing unauthorised information system access via password exploitations
Preventing PII theft via social networks

Table 2. Skills and hands-on tasks of cybersecurity skills index (CSI) based on actual incident relevance in 2016. Source: Carlton et al. 2019.

The sum of theoretical models implemented in the CSI of Carlton et al. (2019), totals a concept akin to cybersecurity competence as defined within the SSH part of SOTER. Their definition of skills as comprising of knowledge, ability and experience resembles our model that distinguishes between the ability to recognise cybersecurity incidents and to react accordingly based on employees' knowledge, skills and proficiency. However, the model of Carlton et al. distinguishes other stages of the process and labels them differently. Notably,

within D6.1 Carlton et al.'s (2019) work served as the foundation for the outline of general digital competences.

As Carlton et al. (2019, 102) stated, previous research suggests that the "use of observable hands-on skills provides unbiased evidence of competence" (see also D'Arcy and Hovav 2009; Hu et al. 2011). Despite the differences in theoretical underpinning of competence, it is therefore considered imperative to integrate the work of Carlton et al. (2019) into the competence catalogue, particularly with the training actions to follow in mind.

Ferrari et al. (2013)

Within the DIGCOMP report by Ferrari et al. (2013), a framework for digital competence for all citizens is proposed, feeding into lifelong learning and society participation considerations of the EU. The authors identified a total of 21 competences, each of which feature at least one element of knowledge, skill and attitude. The definition of competence employed was considered the best fit for WP6 overall, as it builds up on European policy documents (European Parliament and the Council 2006; European Parliament and the Council 2008). Accordingly, competence is viewed as the "proven ability to use knowledge, skills and personal, social and/or methodological abilities, in work or study situations and in professional and personal development" (Ferrari et al., 2013, 37).

After the original DIGCOMP report, Vuorikari et al. (2016) and Carretero et al. (2017) have continued development of the European Digital Competence Framework for Citizens. The now labelled DIGCOMP 2.0 and DIGCOMP 2.1, respectively, feature five slightly adjusted competence areas, shown in the list below (Vuorikari et al. 2016):

- Information and data literacy
- Communication and collaboration
- Digital content creation
- Safety
- Problem solving

Due to the nature of DIGCOMP, those competences may be considered the very basic digital competences for any European citizen. They do, however, also yield insights for finance-specific competence catalogue to be developed as part of this deliverable. Additionally, digital competences enable significantly easier progress regarding learning objectives of finance-specific competences.

4 Matching the Mapping – Understanding threats and attack vectors

Since we have conducted a thorough literature review on existing cybersecurity competence approaches in Section 3, it is now feasible to introduce the mapping of threats from D2.1. Firstly, the basis for the technical threats (the attack vectors) will briefly be discussed, along with its limitations. Secondly, it will be argued why there is the need to further adjust the identified threats in D2.1. Lastly, it will be shown that the competences as provided by literature do not cover all of the identified threats and vulnerabilities. The Competence Catalogue to follow in Section 5 aims to bridge that gap.

In regard to the listed threats and attack vectors in the following sections, it should be considered that many incidents (esp. those based on criminal/malevolent intent) have a multi-stage structure (see Figure 2). A successful social engineering attack opens the door to a data breach, which causes a loss of reputational assets and subsequently causes a GDPR-related incident in the legal layer (or is used to gain financial resources through cyber fraud). In such cases, it is useful to start securing the first link in the chain of events to prevent loss of organisational integrity. **In more and more situations, this first link is in the social domain** – especially since the technical security in the finance sector is continually improving. Therefore, enhancing the resilience in the social layer of an organisation through improving the overall cybersecurity competence of all employees can also prevent a significant number of follow-up attacks on the technical infrastructure.

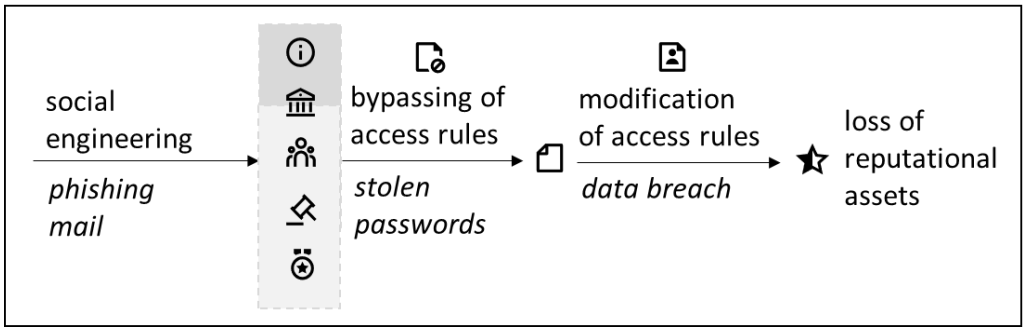

Figure 2. Exemplary multi-stage structure of cybersecurity incidents

4.1 Threats and attack vectors - The CAPEC™ resource

The Common Attack Pattern Enumeration and Classification (CAPEC™) is a publicly available "catalogue of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities"[8]. The catalogue provides a comprehensive overview of "attack patterns" along with an associated description. Its goal is to provide an up-to-date community resource of common attack methods, both technical

[8] Common Attack Pattern Enumeration and Classification (CAPEC™), Available at: https://capec.mitre.org/data/index.html

and human factor-based. The CAPEC™ catalogue served as the basis within the mapping conducted in D2.1, as it is the most up-to-date and well-maintained catalogue of attack vectors and was updated as recently as July 2020[9].

In its current version (3.3), the CAPEC™ catalogue features a total of 524 attack patterns. A further selection of human factor-based attack patterns has been undertaken in D2.1. Fortunately, the CAPEC™ catalogue provides its own hierarchical categorisation to facilitate the selection. The two overarching categories are "Mechanisms of Attack" and "Domains of Attack". While the first category is focused on "mechanisms that are frequently employed when exploiting a vulnerability"[10], the second category organises attack patterns based on the attack domain, i.e. the target domain. Within the second category, the most relevant target domain within the scope of this deliverable is „Social Engineering", which includes attack patterns that focus on „the manipulation and exploitation of people"[11]. The domain features eight meta attack patterns, which will be discussed in more detail below to enable comprehensive matching to trainable competences. The eight meta attack patterns considered for this deliverable are:

- Parameter Injection
- Identity Spoofing
- Resource Location Spoofing
- Action Spoofing
- Software Integrity Attack
- Information Elicitation
- Manipulate Human Behaviour
- Obstruction

Note that these meta attack patterns are a „decidedly abstract characterisation of a specific methodology or technique used in an attack"[12], thus providing merely a high-level overview of attack patterns. To be able to identify the actual involvement of the human factor, it is necessary to analyse attack patterns on a lower level of abstraction, focusing on standard and detailed attack patterns[13].

Moreover, it is important to consider stages of an attack, and to identify whether a specific attack pattern is enabling others or merely following another previously successfully

[9] Update information available at:
https://capec.mitre.org/news/index.html#july302020_CAPEC_List_Version_3.3_Now_Available
[10] https://capec.mitre.org/data/definitions/1000.html
[11] https://capec.mitre.org/data/definitions/403.html
[12] https://capec.mitre.org/about/glossary.html#Meta_Attack_Pattern
13 https://capec.mitre.org/about/glossary.html#Standard_Attack_Pattern and
https://capec.mitre.org/about/glossary.html#Detailed_Attack_Pattern

conducted attack (e.g. already installed malware). Within the CAPEC™ catalogue, this is indicated by the tags „CanPrecede“ and „CanFollow“. While these tags may provide guidance, it is still necessary to consider detailed attack patterns individually for the systematic matching of threats and competences. This individual consideration aims to establish whether a potentially critical cybersecurity situation may arise. A critical cybersecurity situation was heuristically defined within D2.1 as the result of the interplay of a technical threat (attack pattern) and psychosocial factors (vulnerabilities). The latter have been elaborated on within D2.1 and comprise individual and psychological processes, as well as organisational and sociological processes.

4.1.1 Parameter Injection

According to CAPEC™, a parameter injection is present when an “adversary manipulates the content of request parameters for the purpose of undermining the security of the target”[14]. These injections are frequent in the context of HTTP GET messages or in the form of Email Injections, abusing meta-characters in email headers. Most of these injections are not visible to the end-user and do not require the end-user to be deceived, thus they do not play a major role within the SSH part of SOTER. However, there is one standard attack pattern, Flash Injection, where the human factor may be considered relevant. On the level of detailed attack patterns, both Flash Parameter Injection[15] and Cross-Site Flashing[16] in some cases require the end-user to click on a link crafted by the attacker. The attack patterns are exploiting native Flash functionalities within browsers and the fact that Flash files can reference external URLs. It is to be assumed that most banks’ cybersecurity departments will disable running Flash applications altogether, however, this likely does not apply to employees’ and end-users’ personal devices.

A typical mitigation measure is to only allow known URLs to be included as remote flash movies in a flash application (courtesy of the CS department). End-users, however, should be wary of trusting Flash applications and documents (.SWF files) from unknown sources, particularly when using their private devices. Recalling Section 3, literature did not provide a competence suited to mitigate Flash Injections. Within the competence catalogue, this threat was thus addressed by the newly-introduced “Safe Browsing” and “Assurance of Device Safety” competences.

4.1.2 Identity Spoofing

[14] https://capec.mitre.org/data/definitions/137.html
[15] https://capec.mitre.org/data/definitions/174.html
[16] https://capec.mitre.org/data/definitions/178.html

CAPEC™ defines Identity Spoofing as the "action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal"[17]. An Identity Spoofing attack may manifest in various ways, certainly most prominently as a Phishing attack. CAPEC™ lists the following standard attack patterns as form of Identity Spoofing:

- Pharming
- Phishing
- Fake the Source of Data
- Principal Spoof
- Signature Spoof

Pharming

According to CAPEC™, Pharming (which is a neologism based on "farming" and "phishing") deceives the victim "into entering sensitive data into supposedly trusted locations"[18]. These trusted websites frequently require entering or handle sensitive information, and may include online banking sites or trading platforms. The attacker provides an impersonation of the supposedly trusted website, which the victim is then directed to, rather than to the originally intended one. This is achieved by "poisoning" the DNS (Domain Name System) server or the local hosts file, which are responsible for directing the victim to the original website. Crucially, the URL remains identical to that of the original, trusted website, providing no indication to the victim. Furthermore, the spoofed website is usually completely identical[19] to the original site, which also may cause the victim to trust the site. Unlike other social engineering attacks, the victim is not required to click on malicious links. The Pharming attack is successful when the victim enters sensitive information, such as credentials or account numbers, into the spoofed website.

Mitigation

On the technical side, Pharming attacks can be mitigated or thwarted by patching known vulnerabilities in DNS or router software. However, end-users are also able to mitigate Pharming attacks. Firstly, end-users need to ensure they handle any sensitive information while using a secure connection only, i.e. not while browsing on a public WiFi and when HTTPS is available. Secondly, when entering sensitive information into supposedly trusted websites, end-users need to verify that the website's certificate (SSL/TLS) is valid and was issued by a well-known certificate authority. Accordingly, within the competence catalogue,

[17] https://capec.mitre.org/data/definitions/151.html
[18] https://capec.mitre.org/data/definitions/89.html
[19] Note that according to CAPEC™ and CS experts, the creation of a fake website is rather trivial.

Pharming threats are covered directly by the "Safe Browsing" and "Network Handling" competences, as well as by, of course, the "Social Engineering Recognition" competence.

Fortunately, most modern web browsers provide visual cues (the padlock) or notifications when visiting a website without HTTPS. Invalid (outdated) certificates are also recognised by many browsers and users are usually prompted if that is the case.

Phishing

The most well-known social engineering technique, Phishing, is a form of information gathering derived from "fishing for information". It is defined by CAPEC™ as an technique "where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (very frequently authentication credentials) that can later be used by an attacker" [20]. The attacker creates a spoofed website that closely resembles the website they are trying to impersonate, optionally at an URL looking similar to the original URL. Frequently, the spoofed website will feature a login form to put in authentication credentials. The attacker then uses some means of digital communication, commonly email, to send the link to the spoofed website to his victims. The message is usually crafted in a way to convince the victim it is coming from a legitimate entity, for instance by spoofing the email address and/or by emulating the look of emails from a well-known bank. The message also features a call to action to prompt the victim to click the provided link. Once the victim has accessed the spoofed website and entered his/her authentication credentials or other sensitive information such as credit card information, the phishing attack has been successful and the attacker is free to leverage the stolen information.

Note that the above description is merely the main variation of phishing attacks. CAPEC™ lists two more detailed attack patterns, Spear Phishing[21] and Mobile Phishing[22]. Spear Phishing is basically an enhanced version of the Phishing attack, as it targets specific users or groups. It therefore requires the attacker to obtain or elicit contextual information about the targeted user in order to craft a more convincing message. Thus, Spear Phishing is often a follow-up to a successful Pretexting attack (see 4.1.6). Mobile Phishing relies on text messages sent to mobile phone users, but does otherwise not differ from a standard Phishing attack.

[20] https://capec.mitre.org/data/definitions/98.html
[21] https://capec.mitre.org/data/definitions/163.html
[22] https://capec.mitre.org/data/definitions/164.html

Mitigation

Since a successful phishing attack requires the attacker to correctly guess the entity the victim is doing legitimate business with, attackers typically increase the likelihood of the attack's success by sending out vast amounts of emails to many potential victims. Email is likely the "most efficient and cost effective attack distribution available"[23]. Most attackers therefore use the most popular banks or service providers for impersonation. This has implications for mitigation, as phishing attacks are less targeted (or tailored to the potential victim) than other social engineering techniques and often provide an imperfect impersonation or spoofed website. Thus, end-users should avoid following links within emails, unless they are able to clearly verify the identity and integrity of the email sender. If the end-user has already clicked on the link, it is crucial to double-check the URL and compare it to the trusted URL before entering any kind of sensitive information. More generally, end-users should be wary of replying to emails that ask them to provide sensitive information of any kind. Within the competence catalogue, the competences "Safe Browsing", "Confidential personal data and information handling" as well as "Business data and information handling" directly aim at enabling end-users to avoid falling for phishing attacks. The "Social Engineering Recognition" competence is essential as well. For Mobile Phishing, the "Safe Digital Communication" is also highly relevant.

Fake the Source of Data

This standard attack pattern is defined by CAPEC™ rather broadly as "an adversary taking advantage of improper authentication to provide data or services under a falsified identity"[24]. The perhaps simplest variation of this attack is the creation of an email message with a modified "From" field, in order to veil the actual email sender and to convey that the message was sent from someone else. Most commonly used email protocols are not able to properly authenticate the source, displaying the spoofed email sender and potentially triggering the end-user to perform actions (such as clicking a link) as instructed in the email.

Out of the five detailed attack patterns listed by CAPEC™ here, only Counterfeit Websites[25] and Counterfeit Organisations[26] are considered a social engineering technique for the purpose of this deliverable, as they require additional user input (visiting the website) to be effective. Whereas the former creates duplicates of legitimate websites to deceive the end-user into entering sensitive information or downloading malware, the latter attempts to create false front organisations, which appear to be a legitimate supplier.

[23] https://capec.mitre.org/data/definitions/41.html
[24] https://capec.mitre.org/data/definitions/194.html
[25] https://capec.mitre.org/data/definitions/543.html
[26] https://capec.mitre.org/data/definitions/544.html

Mitigation

CAPEC™ provides no additional information on mitigation measures here. The standard attack pattern appears to be quite similar to the second stage of phishing attacks, where a spoofed website is used. However, sometimes malicious injects may be used that do not require the end-user to enter sensitive information on the website itself, a fact which may serve as a useful distinction. The end-user needs to ensure not to visit any unknown or suspicious websites in the first place. Thus, the "Safe Browsing" competence is well-suited to provide mitigation strategies, while the "Social Engineering Recognition" competence is necessary as well.

Principal Spoof

CAPEC™ defines Principal Spoof as "a form of Identity Spoofing where an adversary pretends to be some other person in an interaction"[27]. The interaction is typically a message crafted to appear to come from a legitimate source, hence phishing and pharming attacks often employ the Principal Spoof technique. As the possible outcomes of a Principal Spoof mirror those of Identity Spoofing, most techniques for Identity Spoofing can be used for a Principal Spoof attack. However, because a Principal Spoof is used to impersonate a person, social engineering can be both an attack technique (using social techniques to generate evidence in support of a false identity) as well as a possible outcome (manipulating people's perceptions by making statements or performing actions under a target's name).

Mitigation

As the focus of Principal Spoofing is on pretending to be some other person, end-users need the "Safe Digital Communication", "Social Engineering Recognition" and "Identity Fraud Recognition" competences to mitigate the threat. To some degree, the "Confidential personal data and information handling" as well as the "Business data and information handling" competences are also relevant. The focus of any mitigation strategy needs to be on proper identity verification.

Signature Spoof

CAPEC™ describes a Signature Spoof as "an attacker generating a message or datablock that causes the recipient to believe that the message or datablock was generated and cryptographically signed by an authoritative or reputable source"[28]. Mitigation strategies are exclusively available to CS or IS professionals and the end-user is not concerned. Thus, the Signature Spoof attack is not considered relevant for the human factor-based part of SOTER.

[27] https://capec.mitre.org/data/definitions/195.html
[28] https://capec.mitre.org/data/definitions/473.html

4.1.3 Resource Location Spoofing

On the rather abstract level of meta attack patterns, CAPEC™ defines Resource Location Spoofing as "an adversary deceiving an application or user and convincing them to request a resource from an unintended location"[29]. By spoofing the location, the attacker may cause an alternate resource (such as malware) to be used.

CAPEC™ distinguishes between two standard attack patterns here, namely Redirect Access to Libraries[30] and Establish Rogue Location[31]. The former involves manipulating libraries such as DLLs and does not require the end-user to be deceived or manipulated into actions. Thus, it is not considered relevant within the SSH part of SOTER.

Establish Rogue Location

This attack pattern arises when "an adversary provides a malicious version of a resource at a location that is similar to the expected location of a legitimate resource"[32]. When the victim visits the rogue location and accesses the malicious resource, the attack is successful.

This standard attack pattern features a number of detailed attack patterns that are considered social engineering techniques. Typosquatting[33] takes advantage of typing errors when users enter URLs, the classic example being "www.goggle.com". The attacker registers the mistyped domain name and often spoofs the original website. As a result, the user is redirected to the attacker-controlled domain. Note that this technique is also frequently employed in phishing attacks.

Variations of Typosquatting are Soundsquatting[34], where the attacker-controlled domain name sounds the same as a trusted domain, but has a different spelling, and the Homograph Attack via Homoglyphs[35], where the attacker-controlled domains looks similar to the trusted domain (e.g. www.paypa1.com instead of www.paypal.com). Both techniques may also be part of a phishing attack.

Additionally, CAPEC™ also considers the Evil Twin Wi-Fi Attack to be a variation of Establish Rogue Location, where the attacker "installs Wi-Fi equipment that acts as a legitimate Wi-Fi

[29] https://capec.mitre.org/data/definitions/154.html
[30] https://capec.mitre.org/data/definitions/159.html
[31] https://capec.mitre.org/data/definitions/616.html
[32] Ibid.
[33] https://capec.mitre.org/data/definitions/630.html
[34] https://capec.mitre.org/data/definitions/631.html
[35] https://capec.mitre.org/data/definitions/632.html

network access point"[36]. This may be hard to detect for the end-user and is thus not considered a typical social engineering technique. However, it may be argued that the end-user should be able to recognise that there are duplicate Wi-Fi networks available (e.g. when already logged into the company's network) and become suspicious.

Mitigation
Because of the proximity to phishing attacks, the most relevant competence for end-users to mitigate attacks involving rogue locations is "Safe Browsing". Additionally, "Social Engineering Recognition" may also help with mitigation. The latter may also be applicable to the Evil Twin Wi-Fi Attack, which is also addressed by the "Network Handling" competence.

4.1.4 Action Spoofing

In an Action Spoofing attack, the "adversary is able to disguise one action for another and therefore trick a user into initiating one type of action when they intend to initiate a different action"[37]. For example, a button that says it will submit a form might instead download software. This may be performed by deceiving the victim to click the button as part of a social engineering technique, or by technical means such as clickjacking. The corresponding standard and detailed attack patterns listed by CAPEC™ account for this distinction, with Clickjacking being perhaps the only truly social engineering based attack pattern in some cases.

The other attack patterns, namely Activity Hijack[38], Task Impersonation[39], Scheme Squatting[40] and Tapjacking[41], may only be conducted after previously installing malicious applications on the targeted device. Thus, they are considered to be mainly on the technical side rather than human factor-based attack patterns, as mitigation needs to happen earlier to avoid malware infection (see 4.1.5).

While Clickjacking[42] attacks may operate similarly to the attack patterns mentioned above and require previously installed malware, some of them exploit the fact that web-based UIs are widespread nowadays. When using a web-based UI instead of a thick client[43], the attacker may tamper with the displayed UI and trick the victim into initiating an action that was unintended. Note that Clickjacking is usually only possible after visiting an attacker-controlled malicious site.

[36] https://capec.mitre.org/data/definitions/615.html
[37] https://capec.mitre.org/data/definitions/173.html
[38] https://capec.mitre.org/data/definitions/501.html
[39] https://capec.mitre.org/data/definitions/504.html
[40] https://capec.mitre.org/data/definitions/505.html
[41] https://capec.mitre.org/data/definitions/506.html
[42] https://capec.mitre.org/data/definitions/103.html
[43] A „fat client" or „thick client" typically provides rich functionality independent of the server.

Mitigation

CAPEC™ recommends to avoid clicking suspicious links and interacting with suspicious sites to prevent Action Spoofing in general. For avoiding Clickjacking, it is advisable to turn off various browser scripts (JavaScript, Flash etc.), which is typically handled by the company's CS department. Additionally, it is recommend to log out of any authenticated session (e.g. social media or online banking) before visiting unknown sites within the same browser. Within the competence catalogue, "Safe Browsing" and "Social Engineering Recognition" are the most relevant competences with regard to mitigation. Considering private devices might an entry point for this attack pattern as well, the "Assurance of Device Safety" competence is of particular importance.

4.1.5 Software Integrity Attack

In a Software Integrity Attack, "an attacker initiates a series of events designed to cause a user, program, server, or device to perform actions which undermine the integrity of software code, device data structures, or device firmware, achieving the modification of the target's integrity to achieve an insecure state"[44]. The standard attack patterns subsumed here are Malicious Software Download[45] and Malicious Software Update[46], which may be considered classic examples of social engineering techniques.

Malicious Software Download

While it has to be noted that there are several variations of this attack pattern, typically, there are two distinct stages. Firstly, the attacker needs to deceive a user into downloading a malicious file containing malicious code. This implies that the attacker has already managed to direct the user to an attacker-controlled source or has convinced the user to open an email attachment. Attackers may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl[47]. Secondly, the user needs to open the malicious file, thus executing the code and leading to successful completion of the attack.

It is immediately apparent that attacks featuring malware execution require the attacker to deceive the user at several points in time, making these attacks quite complex. Most users should be aware that downloading, opening or installing files from unknown sources is dangerous, as this is a common pitfall of using the internet. For this reason, malware attacks are frequently incorporated into phishing attacks and conducted after the preceding stages

[44] https://capec.mitre.org/data/definitions/184.html
[45] https://capec.mitre.org/data/definitions/185.html
[46] https://capec.mitre.org/data/definitions/186.html
[47] https://attack.mitre.org/techniques/T1204/002/

of an attack have been successful. Within the early stages of such an attack, Pretexting and subsequent Spearphishing are commonly employed techniques. In another notable variation, the malicious file is placed on a user's desktop or in a shared directory, hoping to exploit the user's curiosity.

Mitigation

CAPEC™ does not provide specific mitigation measures for this standard attack pattern. Generally, files and software should not be downloaded from unknown sources, or after following a link from an unknown entity. Most (if not all) banks restrict user privileges for regular employees to prevent them from downloading any file or software to their work devices. For practical reasons, however, this typically does not apply to email attachments, which may include harmless-looking documents in .doc or .xls format containing malicious code. In this case, users need multiple competences to avoid falling for a malware attack. The most relevant competences are "Safe Browsing", "Safe Digital Communication", "Assurance of Device Safety" as well as "Social Engineering Recognition" and "Malware (Infection) Recognition". Considering private devices might an entry point for this attack pattern as well, the "Assurance of Device Safety" competence is of particular importance.

Malicious Software Update

As the general population has been made aware of the potential risks of downloading files from unknown sources for several decades now, and due to the rise of mobile apps rather than desktop applications, attackers have adapted and frequently focus on malicious software updates instead. In this attack pattern, the attacker deceives the user into downloading and installing a software update that is believed to originate from a trusted source. While there are several variations to this strategy of attack, the attack methods are united in that all rely on the ability of an attacker to position and disguise malicious content such that it masquerades as a legitimate software update. The attack's popularity may be attributed to the fact that virtually all software requires frequent updates or patches, which also implies there are many potential targets. One phishing-assisted variation of this attack involves hosting what appears to be a software update, then harvesting actual email addresses for an organisation, or generating commonly used email addresses, and then sending spam, phishing, or spear-phishing emails to the organisation's users requesting that they manually download and install the malicious software update. Importantly, apart from the Malicious Automated Software Update[48] as listed by CAPEC™, the primary vector for achieving the installation of the update remains a manual user-directed process. Similar to the standard attack pattern discussed above, this implies that frequently, preliminary setup stages such as Pretexting and Phishing are required for an successful attack.

[48] https://capec.mitre.org/data/definitions/187.html

Mitigation
The most tailored mitigation strategy, as identified by CAPEC™, is to validate software updates before installing them. Due to the setup stages required for a successful attack, numerous competences are part of a successful mitigation strategy. Among the most important are the "Safe Browsing", "Safe Digital Communication" and "Assurance of Device Safety" competences, while naturally "Social Engineering Recognition" and "Malware (Infection) Recognition" are needed as well.

4.1.6 Information Elicitation

Simply put, this meta attack pattern covers all attacks where an attacker "engages an individual using any combination of social engineering methods for the purpose of extracting information"[49]. This broad definition covers a lot of ground, with the most notable standard attack pattern being Pretexting.

Pretexting[50]

During a pretexting attack, the adversary creates an invented scenario, assuming an identity or role to persuade a targeted victim to release information or perform some action. This may involve creating a new identity to manipulate the victim. Among the many variations, CAPEC™ identified Pretexting via Customer Service, Tech Support, Delivery person and Phone. The success of any Pretexting attack is dependent on the employed information gathering techniques and the trust the attacker can build with the victim. Authentic mimicry combined with detailed knowledge increases the success of Pretexting attacks. It is thus perhaps the most iconic example of social engineering techniques.

Mitigation
CAPEC™ suggests quite generally that an organisation should provide regular, robust cybersecurity training to its employees to prevent successful social engineering attacks. As Pretexting is usually the first stage of an attack, it is considered imperative to provide employees with adequate mitigation strategies. The competences needed are "Confidential personal data and information handling", "Business data and information handling", "Responsible sharing of private information" and "Privacy settings for private digital devices and services". Additionally, competence in "Social Engineering Recognition" and "Identity Fraud Recognition" contributes to overall avoidance of Pretexting threats as well.

4.1.7 Manipulate Human Behaviour

[49] https://capec.mitre.org/data/definitions/410.html
[50] https://capec.mitre.org/data/definitions/407.html

Similar to Information Elicitation, this meta attack pattern is primarily concerned with classic social engineering techniques. It is defined by CAPEC™as an "adversary exploiting inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the adversary's interests"[51]. Manipulation techniques may take many different shapes, which are represented by numerous standard and subordinate detailed attack patterns listed by CAPEC™. It is immediately apparent that there are potential overlaps with Information Elicitation (see 4.1.6 above), not least because Pretexting is also included in the Manipulate Human Behaviour meta attack pattern. Hence, this subsection focuses on the other standard attack patterns.

Influence Perception

Firstly, Influence Perception[52] is focused on altering the victim's perception of the relationship between the attacker and themselves. As with the other techniques, the attacker's goal is to convince the target to unknowingly perform actions, such as divulging information, that are beneficial to the attacker. On the level of detailed attack patterns, CAPEC™ further distinguishes between the avenues attackers can pursue in an Influence Perception attack, such as basing their attack on authority, reciprocation or social proof. As the focus is on the relationship between the attacker and the victim, this attack pattern may be considered a typical prerequisite for successful Identity Spoofing (in particular Principal Spoofing) attacks (see 4.1.2).

Mitigation
As for mitigation strategies on the level of meta attack patterns, CAPEC™ does not provide any recommendations beyond the somewhat succinct regular cybersecurity training of all employees. However, regarding the Influence Perception attack, mitigation should be focused on the same elements as when preventing Principal Spoofing, namely proper identity verification. Thus, "Safe Digital Communication", "Social Engineering Recognition" and "Identity Fraud Recognition" are essential competences to mitigate the threat. To some degree, the "Confidential personal data and information handling" as well as the "Business data and information handling" competences are also relevant.

Target Influence via Framing

The second standard attack pattern, labelled Target Influence via Framing[53], features framing techniques employed by the attacker to contextualise a conversation in order to

[51] https://capec.mitre.org/data/definitions/416.html
[52] https://capec.mitre.org/data/definitions/417.html
[53] https://capec.mitre.org/data/definitions/425.html

make the victim more likely to be influenced by the attacker's point of view. In this context, framing is understood as a "methodology of conversation that slowly encourages the target to adopt the adversary's perspective"[54]. For instance, a framing technique might focus on contextualising responses in a positive manner by avoiding the word "No" or any responses with potential negative connotations. Thus, framing techniques may be considered prerequisites of various other attack patterns, such as Pharming and Phishing.

Mitigation
Apart from regular cybersecurity training for all employees, CAPEC™ recommends to avoid sharing unnecessary information during interactions beyond what is absolutely required for effective communication. Accordingly, the essential competences to mitigate Target Influence via Framing attacks are "Safe Digital Communication", "Social Engineering Recognition", "Confidential personal data and information handling", "Business data and information handling" and "Assessment of accuracy and integrity of information".

Influence via Incentives

The third standard attack pattern listed by CAPEC™, Influence via Incentives[55], is noticeably distinct from the others within this meta attack pattern. The attacker attempts to evoke certain behaviour from the victim by financial, social or ideological incentivisation. The most effective incentive against one target is highly individual, and as such may require additional information gathering by the attacker prior to a successful Influence via Incentives attack. Examples of this technique include bribery, monetary fraud, peer pressure and appealing to the target's morals or ethics.

As was already outlined in D2.1, this attack pattern explicitly addresses the "insider threat" (the malicious insider). In the recent past, there have been numerous reports on attempted bribes of government contractors for critical infrastructure in the USA[56].

Mitigation
The essential competence here is certainly "Insider Threat Recognition". Additionally, "Social Engineering Recognition" and "Identity Fraud Recognition" may come into play here as well. Notably, preventing insider threats successfully also involves training elements of competence beyond knowledge and skills, particularly with regard to attitude and agency.

Lastly, CAPEC™ cites Influence via Psychological Principles as "shaping the target's actions or behaviour by focusing on the ways human interact and learn, leveraging such elements as

[54] https://capec.mitre.org/data/definitions/425.html
[55] https://capec.mitre.org/data/definitions/426.html
[56] See, for instance, https://thehackernews.com/2020/08/job-offer-hackers.html

cognitive and social psychology"[57]. Thus, this may be considered a meta category, comprising elements to be utilised within all of the abovementioned standard attack patterns. Note that there is obviously some interplay between all of the standard attack patterns listed, as attackers may employ these techniques in virtually any combination.

4.1.8 Obstruction (Physical Security)

In general, the attack patterns within this category focus on exploiting weaknesses in the physical security of a system. While many of those attack patterns are realised through technical means, some of them focus on the exploitation of the human factor, employing social engineering techniques. The standard attack patterns included in Obstruction are Physical Destruction of Device or Component[58], Route Disabling[59], Jamming[60] (e.g. Wi-Fi Jamming) and Blockage[61] (e.g. DNS Blocking). While Jamming and Blockage typically do not require the employment of social engineering techniques to be successful, both Physical Destruction and Route Disabling may exploit human factor-based vulnerabilities, most frequently by gaining unauthorised access to the victim's company premises.

Physical Destruction of Device or Component

The attacker needs to gain physical access to the targeted devices or components. Therefore, unless the attacker is an insider, unauthorised access to the company's premises is required. A classic example of this attack is when an attacker feigns making a delivery of goods to a company, thus gaining access to otherwise restricted areas.

Route Disabling

The attacker disables the network route between two targets and hopes to evoke a desired (over-)reaction from the individuals responsible for the (critical) network infrastructure. Disabling or shutting off critical system resources prevents them from performing their service as intended, which can have direct and indirect consequences on other systems. To be able to successfully conduct the attack, the attacker requires physical access to the targeted communications equipment.

Mitigation
CAPEC™ suggests to ensure rigorous physical defensive measures are in place. Depending on the company, this may be among the responsibilities of employees spread across various departments. These defensive measures may include access locks, key cards and strict

[57] https://capec.mitre.org/data/definitions/427.html
[58] https://capec.mitre.org/data/definitions/547.html
[59] https://capec.mitre.org/data/definitions/582.html
[60] https://capec.mitre.org/data/definitions/601.html
[61] https://capec.mitre.org/data/definitions/603.html

identify verification. The most essential competences to prevent attackers from accessing critical systems are “Physical Safety”, “Physical Environment Sensibility” and “Social Engineering Recognition”.

Note that these attack patterns may be complemented by social engineering techniques at any stage of the attack. For instance, Pretexting or Influence Perception may be employed to assure that the front office employees will be deceived. A combination of these attack patterns (including malware) may result in an attacker being able to connect a compromised USB memory device to the company’s IT system.

4.2 Threats and identified competences in literature

As laid out earlier, the following table aims to match previously identified competences within academia (Section 3) with the threats as suggested by CAPEC™ above. Whenever the threat was not sufficiently or only partially addressed within literature, a competence was added to the catalogue. For instance, Carlton et al. (2019) provide specific skills for many of the threats identified, however, these skills often merely cover a few elements of the competence we identified as necessary for mitigation. This process was conducted iteratively. Note that the most feasible level of abstraction was used for the “Threat” column, i.e. meta, standard or detailed attack patterns.

Threat	Covered by previous approaches	SOTER Competence Catalogue
Parameter Injection	Not covered	Safe Browsing Assurance of Device Safety
Pharming	Preventing PII theft via access to non-secure websites (Carlton et al. 2019) Safety (Vuorikari et al. 2016)	Safe Browsing Network Handling Social Engineering Recognition
Phishing	Preventing the leaking of confidential digital information to unauthorised individuals (Carlton et al. 2019) Preventing PII theft via email phishing (Carlton et al. 2019) Safety (Vuorikari et al. 2016)	Safe Browsing Confidential personal data and information handling Business data and information handling Safe Digital Communication Social Engineering Recognition
Fake the source of data	Preventing PII theft via access to non-secure websites (Carlton et al. 2019) Preventing credit card theft by purchasing from non-secure websites (Carlton et al. 2019)	Safe Browsing Social Engineering Recognition
Principal Spoof	Preventing the leaking of confidential digital information to unauthorised individuals (Carlton et al. 2019) Safety (Vuorikari et al. 2016)	Safe Digital Communication Social Engineering Recognition Identity Fraud Recognition Confidential personal data and information handling Business data and information handling

Establish Rogue Location	Preventing PII theft via access to non-secure websites (Carlton et al. 2019)	Safe Browsing Social Engineering Recognition Network Handling
Clickjacking	Not covered	Safe Browsing Social Engineering Recognition Assurance of Device Safety
Malicious Software Download	Preventing malware via non-secure websites (Carlton et al. 2019) Preventing malware via email Carlton et al. (2019) Safety (Vuorikari et al. 2016)	Safe Browsing Safe Digital Communication Assurance of Device Safety Social Engineering Recognition Malware (Infection) Recognition
Malicious Software Update	Preventing malware via non-secure websites (Carlton et al. 2019) Preventing malware via email Carlton et al. (2019) Safety (Vuorikari et al. 2016)	Safe Browsing Safe Digital Communication Assurance of Device Safety Social Engineering Recognition Malware (Infection) Recognition
Pretexting	Preventing the leaking of confidential digital information to unauthorised individuals (Carlton et al. 2019) Preventing PII theft via social networks (Carlton et al. 2019) Safety (Vuorikari et al. 2016)	Confidential personal data and information handling Business data and information handling Responsible sharing of private information Privacy settings for private digital devices and services Social Engineering Recognition Identity Fraud Recognition
Influence Perception	Preventing the leaking of confidential digital information to unauthorised individuals (Carlton et al. 2019) Safety (Vuorikari et al. 2016)	Safe Digital Communication Social Engineering Recognition Identity Fraud Recognition Confidential personal data and information handling Business data and information handling
Target Influence via Framing	Not covered	Safe Digital Communication Social Engineering Recognition Confidential personal data and information handling Business data and information handling Assessment of accuracy and integrity of information
Influence via Incentives	Not covered	Insider Threat Recognition Social Engineering Recognition Identity Fraud Recognition
Obstruction (Physical Security)	Not covered	Physical Safety Physical Environment Sensibility Social Engineering Recognition

Table 3. Comparison of threats and corresponding skills and competences as identified by literature. Author's compilation based on Carlton et al. (2019), Vuorikari et al. (2016) and CAPEC™ threat taxonomy.

5 The Competence Catalogue

5.1 Notes on the iterative creation process

As stated earlier, the competence catalogue was developed in close cooperation with the SSH research partners of the SOTER project (UNIGRAZ, RISE and TRI). Every iteration of the competence catalogue went through the same process: desk research, compiling of drafts, distribution to the SSH research partners for feedback, and subsequent integration of said feedback.

Certain elements of a competence are represented by the dimensions in the catalogue below (knowledge, skills and attitude), while others (proficiency and agency) are not. This is due to knowledge, skills and attitude being dimensions of competence with specific distinguishable contents, while proficiency is an element of exercise, fulfilled during the process of training. The element of agency is a dimension of competence that is developed in and through the shaping of contextual factors and will thus be fostered separately within the masterclass of WP6.

Accordingly, feedback from UNIGRAZ focused on the three competence elements to be trained, while RISE provided insights on the technical side (threat taxonomy), and, finally, TRI provided feedback on the interplay of privacy and data protection.

It is to be noted that within the further stages of the project, feedback from the consortium's bank partner (LIBER) will be essential for refinement and adjustment of training contents.

The following competence catalogue is based on the previously identified competence approaches in academia (Section 3) with a focus on Ferrari et al. (2013), Vuorikari et al. (2016), Iordache et al. (2017) and Carlton et al. (2019). Additionally, the threat taxonomy based on CAPEC™ (Section 4) served as a reference point. Note that the catalogue has been grouped into four categories (hence the separation of tables) for easier association with training modules in the remainder of WP6.

5.2 Cybersecurity Competence Catalogue

Competence	Knowledge	Skills	Attitude	Threat
Confidential personal data/information handling (processed by organisation)	Knows which data or information is personal Knows about the risks associated with involuntary disclosure of unsolicited personal data or information Is aware of personal data being one of the main responsibilities of the company Knows about GDPR and respective company protocols Understands the severity of consequences for the company in case of a GDPR violation or a data breach	Can handle requests for any confidential personal data or information with due diligence and in compliance with GDPR Can verify the authenticity of requests for confidential personal data or information Can independently verify identity and integrity of the individual or company issuing any request for confidential personal data or information Can verify integrity of request for personal data or information even in internal communication for GDPR compliance	Values the legal, ethical, physical, material, mental and social integrity of others in regard to their personal data/information Values privacy of data from other persons	Phishing Principal Spoof Pretexting Influence Perception Target Influence via Framing
Business data/information handling	Knows which information is sensitive/confidential Knows about the risks associated with involuntary	Can handle requests for any business information with due diligence and in compliance with sector specific regulation	Values the integrity of their employers' organisation in regard to business data and information as long as it is in accordance with respective	Phishing Principal Spoof Pretexting Influence Perception Target Influence via Framing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Competence	Knowledge	Skills	Attitude	Threat
	disclosure of unsolicited information or data braches, like loss of material or reputational assets Understands which information may offer an entry point for attackers (e.g. supply-chain information)	Verifies the authenticity of requests for business information (e.g. request for list of suppliers) Can independently verify identity and integrity of the individual or company issuing any request for business information	applicable law and European Values	
Responsible sharing of private information	Knows the risks associated with disclosure of private information like online fraud, social engineering and cyber bullying Knows that involuntary sharing of private information may be (virtually) irreversible Knows that lack of diligence about private information may lead to adverse effects on the business sphere (via social engineering)	Is able to distinguish between private information that can be shared and private information that should better kept to oneself or only shared with chosen social circles Can track down digital information about oneself Can monitor own digital identity and footprints Can act prudently regarding privacy/data protection issues	Values privacy of own data	Pretexting
Privacy settings for private digital devices and services	Knows about personalised advertisement and other privacy settings (e.g.	Can monitor own digital identity and footprints	Values privacy and data protection for oneself and for others	Pretexting

Competence	Knowledge	Skills	Attitude	Threat
	geodata) Knows that there are privacy considerations beyond personalised ads, such as the Right to be forgotten Understands the importance of concepts of privacy and data protection Understands common terms of service, active protection of personal data, as well as other people's privacy Knows that platforms have to adhere to regulation and provide a minimum of privacy options Is aware of the impact and longevity of digital information that one considers for publishing Knows that lack of diligence about privacy settings may lead to adverse effects on the business sphere (via social engineering)	Can configure (software, device, social media, account) privacy settings to avoid involuntary disclosure of personal data		
Assessment of accuracy and	Understands how	Can assess the usefulness,	Is critical about information	Pretexting

Competence	Knowledge	Skills	Attitude	Threat
integrity of information	information is generated, managed and made available Is aware of different search engines Understands the reliability of different sources Recognises that not all information can be found on the Internet Understands online and offline information sources	timeliness, accuracy and integrity of the information Can evaluate media content for verifiability, authenticity, integrity and consistency Can analyse retrieved information Can compare, contrast, and integrate information from different sources Can individually check sources of obtained information to verify their reliability	found	Target Influence via Framing

Competence	Knowledge	Skills	Attitude	Threats
Physical Safety	Understands that the principles of identity verification apply to physically present clients or suppliers as well as they apply in digital communication Knows that physically present suppliers (such as	Acts in accordance with access control protocols Can enforce company's access controls on unauthorised third parties Will alert company security if unauthorised access to company's premises is	Takes a critical stance towards unfamiliar or external persons and digital devices	Obstruction (Physical Security)

Competence	Knowledge	Skills	Attitude	Threats
	employees of delivery services) or even clients have restricted access to the company's premises Understands that access controls within a company are to be taken seriously and that there are significant assets at risk Knows that ICT infrastructure need to be guarded from unauthorised physical access	detected Lets new or unfamiliar devices be cleared by IS department before using them on-premise Can make sure that no sensitive information on paper or on screen is visible to unauthorised entities Can make sure that no third party may listen in on conversations containing confidential (financial) information Will only meet with clients within his/her office if there is no sensitive information present (see also GDPR), otherwise uses designated meeting rooms		
Safe Browsing	Knows that websites may not be authentic, even if they look that way Knows that fake websites can steal information	Checks for HTTPS and SSL/TLS certificates Verifies the authenticity of websites based on other indicators (design, address, URL)	Takes a critical stance towards unfamiliar links and websites	Flash Injection Pharming Phishing Fake the Source of Data Establish Rogue Location Clickjacking Malicious Software

Competence	Knowledge	Skills	Attitude	Threats
	Knows that spoofed websites can host a myriad of threats, such as Malware or harmful Scripts Knows that entering information on spoofed websites may constitute a typical entry point for attackers Understands that attackers may conduct a multi-staged attack, wherein entering unsolicited information on a spoofed website may be an important steppingstone Understands that company assets are at risk just as much as with any other social engineering technique	Takes his/her time to verify the authenticity of a web site Can identify a fake website even though it may have an SSL certificate		Download Malicious Software Update
Network Handling	Knows that there exist different networks with different security properties Understands that WiFi networks are generally less secure and trustworthy Understands that public	Makes sure to always be logged into the secure work network (as provided by the company) Can set up a secure network for remote work (e.g. uses VPN in home office)	Takes a critical stance towards unfamiliar networks	Pharming Establish Rogue Location

Competence	Knowledge	Skills	Attitude	Threats
	networks are prone to uninvited listeners Understands the risks associated with using insecure networks Knows how a VPN works Knows that information transmitted via public networks may easily be intercepted Knows about permitted messenger clients (according to company's policy)			
Safe digital communication	Is aware of different digital communication means (e.g. email, chat, VoIP, video-conference, SMS) Knows which digital communication means are considered to be safer than others Knows the basics of encryption of digital communication	Can verify authenticity of external and internal communication Only uses company-approved messenger clients Uses the safest possible communication channel when handling confidential information Is able to use encryption for digital communication	Takes a critical stance towards the unreflected use of unsafe digital communication means Values the integrity of all entities involved who act in accordance with respective applicable law when communicating digitally	Principal Spoof Malicious Software Download Malicious Software Update Influence Perception Target Influence via Framing

Competence	Knowledge	Skills	Attitude	Threats
	Knows that internal communication may also be fake Is aware of the risks linked with online communication with unknown (unverified) people Is aware that intercepted communication may lead to data breaches and asset loss			
Assurance of device safety	Understands that devices may get compromised during remote working as well as office working Knows that some (mobile) apps can sniff information from used devices Knows about current and up-to-date strategies to avoid risks (e.g. regular security updates) Knows how to secure used digital devices	Can secure personal devices before activating business email Can install and regularly update antivirus software on private device Regularly checks for available security updates Checks with the IS department if he/she is unsure about installing software on his/her personal device	Has internalised that digital devices with network connection are hardly ever completely private spaces Values own digital safety as well as the digital safety of their employer	Flash Injection Mobile Phishing Clickjacking Malicious Software Download Malicious Software Update
Creation of safe credentials	Is aware of authentication methods, such as 2FA	Is able to create and manage strong passwords	Values own digital safety as well as the digital safety of their employer	

Competence	Knowledge	Skills	Attitude	Threats
	Understands the risks associated with weak passwords/login credentials and the potential effects on the company's IT system's integrity Knows about brute-force method and the resulting requirements for safe passwords Knows that it is necessary to use as many different passwords as possible, for each given digital service/device	Uses different passwords for accessing work computers and services and often changes passwords, while complying with password requirements Uses advanced authentication methods and considers separate 2FA based password managers for personal and work devices	Believes in the worth and practicality of strong authentification routines	

Competence	Knowledge	Skills	Attitude	Threats
Social Engineering Recognition	Understands that many successful CS attacks are based on Social Engineering Knows about typical attack mechanisms employed during Social Engineering, such as Spoofing, Phishing or Pretexting Knows that every Social Engineering attack needs to	Can verify request issuer's identity Can verify the integrity of the request Checks for integrity of email senders (e.g. by checking email address) Can distinguish between secure and non-secure	Takes a critical stance towards requests regarding company assets like information or money Enters a state of alertness when requests for business assets contain pleas for reciprocity, commitment, liking, consensus and urgency or apply undue authority	Pharming Phishing Fake the Source of Data Principal Spoof Establish Rogue Location Clickjacking Malicious Software Download Malicious Software Update Pretexting Influence Perception Target Influence via Framing

Competence	Knowledge	Skills	Attitude	Threats
	have a “catch” (e.g. needs confidential information to be disclosed without authorisation) Understands that multi-stage attacks might start simply with eliciting information about a company’s suppliers Understands that the company’s IS department may be powerless after a successful Social Engineering attack	websites and file sources independently (e.g. check for HTTPS, SSL)		
Malware (Infection) Recognition	Understands that every file that was not pre-installed on their work devices is potentially dangerous Knows that downloaded files and email attachments might be infected Knows that malware may infect entire systems quickly, while being tremendously tedious to remove Understands that malware infection is the usual	Can identify different file types and is able to assess their risk potential Treats any executable file or archive with special care Can use anti-malware software to scan files or archives before opening them Handles unknown file extensions cautiously Treats download links with	Does not indulge in a false sense of security due to the perception of the IT-Security-Systems in place as impenetrable	Malicious Software Download Malicious Software Update

Competence	Knowledge	Skills	Attitude	Threats
	prerequisite for (very costly) ransomware attacks	due care When in doubt, does not open or download anything without checking in with the IT Security department		
Physical Environment Sensibility	Knows which physically present suppliers (such as employees of delivery services) or clients are allowed on the company's premises or knows how confirmed access is represented (e.g. through badges for visitors) Knows which digital devices are to be expected at the individual workplace and its surroundings Knows that information or data that is physically accessible can be taken advantage of for different kinds of threats to the organisation Knows that listening devices (such as smartphones) might be used to record conversations	Can identify third parties that are physically present, but are not supposed to be here Can identify suspicious digital devices	Perceives the workplace as a semi-public place in which certain data and information have to be protected from unauthorised access Takes a critical stance towards any unknown person or digital device present at the workplace	Physical Security (Obstruction)

Competence	Knowledge	Skills	Attitude	Threats
	Knows that external memory drives (such as USB sticks) pose a high risk to the company's IT system			
Identity Fraud Recognition	Knows how to verify the identity of a communication partner Knows about the importance of verifying the communication partner's identity for avoiding identity fraud Understands that Identity Spoofing is one of the most common attack vectors Understands the risks of digital customer onboarding in contrast to on-premise customer onboarding	Can verify identity of the individual or company issuing any request for access to business services or assets	Takes a critical stance towards unknown persons or organisations	Principal Spoof Pretexting Influence Perception Influence via Incentives
Insider Threat Recognition	Knows about the prevalence of "malicious insiders" Knows about behaviours usually displayed by	Can identify highly suspicious behaviour of colleagues within the same department or team without becoming a snitch	Is benevolent towards co-workers, but is not overly trusting in everyone.	Influence via Incentives

Competence	Knowledge	Skills	Attitude	Threats
	"malicious insiders" Knows about possible motivators for "malicious insiders", like monetary incentives, game debts etc. Understands that acting as a malicious insider is a bargain with serious long-term, individual repercussions	Can report highly suspicious activity discreetly		

Competence	Knowledge	Skills	Attitude
Incident documentation	Knows about the company's incident documentation protocol Knows that covering up individual mistakes can lead to serious harm for the organisation, and hence also to themselves Understands that it is crucial to provide detailed information about CS incidents, which can be used in company training actions	Provides a detailed, truthful account of the CS incident from their point of view	Is willing to give a detailed account of an incident, even if it was caused by an own mistake and reflect on it
Incident reporting	Knows about the company's incident reporting protocol (usually defined by	Can provide a comprehensive, formal report about a CS incident in	Is conscientious about filing incident reports according to protocol

Competence	Knowledge	Skills	Attitude
	regulation) Knows the appropriate authorities to contact in case of an incident Understands that it is crucial to provide detailed information about CS incidents to authorities and others, to prevent further incidents	line with relevant regulation	
Incident communication	Knows about who to ask or talk to in case of an incident Knows when to escalate an incident to a superior Knows that it is the IS department's job to help her/him Knows about the appropriate channels to contact IS professionals/department Knows that mere suspicions also warrant contacting the IS department	Is able to communicate with IT/IS professionals about incidents comprehensibly Is able to contact IS department for analysis of suspicious external devices Is able to alert company security if unauthorised access to company's premises is detected	Trusts in company's IT Security department or contractor Is willing to ask for help in the face of an incident that exceeds own knowledge and skills
Collaborative incident management	Knows that CS compliance within a team is dependent	Is able to identify that a colleague might have been	Is of the perception that accidents happen, and thus

Competence	Knowledge	Skills	Attitude
	on every team member Knows that multi-team structures offer numerous entry points for attackers Understands that human behaviour is prone to error	subject to social engineering Is able to communicate about incidents within the team, if expected Proactively ensures that CS standards are complied within the working team and when working with members of other teams	will address CS issues with colleagues without patronising Is supportive towards team members

Competence	Knowledge	Skills	Attitude
Identification of CS Competence Gaps	Understands the wider context of digital tools in a 'digital age' characterised by globalisation and networks Knows that digital environment is ever-changing and maintaining CS competence is a constant process Knows how to update his/her knowledge about digital tools and security measures	Proactively makes use of the company's provided digital competence trainings Can verify their sources of information	Takes a critical stance towards his/her own CS competence

Competence	Knowledge	Skills	Attitude
	Knows that CS compliance within a company is dependent on every employee		
Problem-Solving	Knows how a computer or digital device is built Knows about the company's IT infrastructure Knows internal and external sources of information and where to find help for problem-solving and troubleshooting	Can identify a problem when it arises and name it Can analyse the cause of the problem at hand Can apply appropriate solving strategies or search for possible solutions creatively by taking advantage of technologies and digital tools as well as non-technological tools and procedures Can assess the success of own problem-solving processes	Takes an active approach towards solving problems Is willing to seek IS department's advice when a problem arises Has a sense of responsibility for the quality of the problem-solving process

6 References

Arnold, R., Nolda, S. and Nuissl, E. (2010). *Wörterbuch Erwachsenenbildung*. Bad Heilbrunn: Klinkhardt.

Bergmann, G. and Daub, J. (2006). *Systemisches Innovations- und Kompetenzmanagement. Grundlagen – Prozesse – Perspektiven*. Wiesbaden: Gabler Verlag.

Brilingaitė, A., Bukauskas, L. and Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security* **88**, 101607.

Carlton, M., Levy, Y., Ramim, M.M. and Terrell, S.R. (2016). *Development of the MyCyberSkillsTM iPad app: a scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills*. Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC – Workshop on Information Security and Privacy (WISP) 2015, Ft. Worth, TX.

Carlton, M., Levy, Y. and Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Info and Computer Security* **27** (1), 101–121.

Carretero, S., Vuorikari, R. and Punie, Y. (2017). *DigComp 2.1. The digital competence framework for citizens with eight proficiency levels and examples of use*. Luxembourg: Publications Office of the European Union.

D'Arcy, J. and Hovav, A. (2009). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. In *J Bus Ethics* **89** (S1), 59–71.

Drexel, I. (2002). Das Konzept von Kompetenz und die Interessen der gesellschaftlichen Akteure – Erfahrungen aus dem europäischen Ausland. In: Dehnbostel, P. et al. (eds). *Vernetzte Kompetenzentwicklung. Alternative Positionen zur Weiterbildung*. Berlin: edition sigma, 339-355.

Eminağaoğlu, M., Uçar, E., and Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information security technical report*, **14** (4), 223-229.

European Parliament and the Council (2006). Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning. *Official Journal of the European Union*, L394/310.

European Parliament and the Council (2008). Recommendation of the European Parliament and of the Council on the establishment of the European Qualifications Framework for lifelong learning. *Official Journal of the European Union*, C111/111.

European Union Agency for Network and Information Security (ENISA, 2016). *Distributed Ledger Technology & Cybersecurity. Improving information security in the financial sector*. Available at: https://www.enisa.europa.eu/publications/blockchain-security/at_download/fullReport

Ferrari, A., Punie, Y. and Brečko, B. (2013). *DIGCOMP: A framework for Developing and Understanding Digital Competence in Europe.* Luxembourg: Publications Office of the European Union.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, **54** (6), 54-60.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Iordache, C., Mariën, I. and Baelden, D. (2017). Developing Digital Skills and Competences: A Quick-Scan Analysis of 13 Digital Literacy Models. *Italian Journal of Sociology of Education*, **9** (1), 6-30.

Kaufhold, M. (2006). *Kompetenz und Kompetenzerfassung. Analyse und Beurteilung von Verfahren der Kompetenzerfassung*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Kryparos, G. (2018). Information Security in the Realm of FinTech. In: Teigland, R., Siri, S., Larsson, A., Puertas, A.M. and Ingram Bogusz, C. (eds). *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*. Abingdon: Routledge, 43-65.

Kurtz, T. (2010). Der Kompetenzbegriff in der Soziologie. In: Kurtz, T. and Pfadenhauer, M. (eds). *Soziologie der Kompetenz*. Wiesbaden: VS Verlag für Sozialwissenschaften, 7-28.

Lin, T.C.W. (2016). *Compliance, technology, and Modern Finance*. 11 Brooklyn Journal of Corporate, Financial & Commercial Law, **159**.

MacMillan, D. and Yadron, D. (2014). *Dropbox blames security breach on password reuse*. The Wall Street Journal, Digits, available at: http://blogs.wsj.com/digits/2014/10/14/dropbox-blamessecurity-breach-on-password-reuse/

Müller-Frommeyer, L. C., Aymans, S. C., Bargmann, C., Kauffeld, S. and Herrmann, C. (2017). *Introducing competency models as a toll for holistic competency development in learning factories: Challenges, examples and future applications*. Procedia Manufacturing, **9**, 307-314.

National Institute of Standards and Technology (NIST, 2017). *Framework for improving critical infrastructure cybersecurity (version 1.1)*. Available at: www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1.pdf.

North, K., de Carvalho, A.B., Maria, A., Durst, S., Carvalho J.A., Gräslund, K. and Thalmann, S. (2019). Information and knowledge risks in supply chain interactions of SMEs. An exploratory study. In: Heisig, P. (ed). *Knowledge Management in Digital Work Environments – State-of-the-Art and Outlook* (Proceedings 10th Conference Professional Knowledge Management). Potsdam, 268-277.

Pfadenhauer, M. (2010). Kompetenz als Qualität sozialen Handelns. In: Kurtz, T. and Pfadenhauer, M. (eds). *Soziologie der Kompetenz*. Wiesbaden: VS Verlag für Sozialwissenschaften, 149-172.

Thalmann, S. and Ilvonen, I. (2020). *Why should we investigate knowledge risks incidents?- Lessons from four cases*. Proceedings of the 53rd Hawaii International Conference on System Sciences, 4940-4949.

Tsohou, A. and Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology & People*, **31** (5), 1047-1068.

Verizon Enterprise Solutions (2017). *Data Breach Investigations Report*. Available at https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Vuorikari, R., Punie, Y., Carretero, S. and van den Brande, L. (2016). *DigComp 2.0. The digital competence framework for citizens*. Luxembourg: Publications Office.

Whitman, M. and Mattord, H. (2018). *Principles of Information Security*, 6th Edition. Boston, MA: Cengage Learning.

Windeler, A. (2014). Kompetenz. Sozialtheoretische Grundprobleme und Grundfragen. In: Windeler, A. and Sydow, J. (eds). *Kompetenz – Sozialtheoretische Perspektiven*. Wiesbaden: Springer VS, 7-18.