SOTER

Training Handbook: **HUMAN FACTORS**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

Authors: Eva-Maria Griesbacher, Paul Rabel, Martin Griesbacher and Robin Renwick

Design and Layout: Matthew Reilly and Ekaterina Kyulyumova

Published in January 2022 (Graz/Dublin/Madrid)

ISBN: 978-3-903374-13-3
DOI: 10.25364/978-3-903374-13-3

Table of contents

SOTER Training Handbooks Introduction

The financial sector is experiencing a real digital revolution in recent years, in which traditional entities are becoming providers of digital services in order to remain competitive. Although it is clear that this new era implies many advantages for businesses and citizens, in addition, the release of new digital services and connections imply the appearance of new threats and risks in terms of cybersecurity, data privacy and the use of digital identities.

These threats must be tackled under a holistic approach and pointing at their different origins, including the human factor.

Furthermore, the current regulations to be met, apart from involving a technological and mind-set challenge and increasing the number of entities with which to interact with, also aim to create or improve tools to prevent fraud and reduce cyber vulnerabilities as much as possible.

SOTER takes the challenge, considering both technological and non-technological (human factor and governance within organizations) aspects and providing innovative solutions that will act as a transformative process of the finance sector, helping their players to increase their cybersecurity level, improving the fight against present and future cyber attacks and vulnerabilities and, to summarise, increasing their cyber-resilience.

SOTER tackles two main challenges: how to improve the process of digital onboarding and how to implement state of the art cybersecurity culture.

This handbook summarizes the outcomes on the SOTER work on human factors.

1

Human factors: securing the social layer

For the improvement of the cyber resilience in the finance sector an understanding of the role of human behaviour for cybersecurity is critical. In SOTER we developed an interdisciplinary approach focusing on human factors. Tackling the human factor in cybersecurity can be understood as a circular and a linear task. Circular in the sense of a continual collaborative effort for every organization. Linear in the sense of understanding the initial dependent steps to get a principal grip on the relevant task components. Regarding human factor cybersecurity there are of course always overlaps with the basic tasks of technical cybersecurity or information security policies, so they should be understood as complementary activities. The conceptual framework presented here, introduces the relevant components identified in the SOTER project step-by-step and build up to a journey for understanding and tackling relevant human factor-based cybersecurity issues. The steps are:

- Keeping control of your digital assets and securing your vulnerability layers
- Understanding (non-)tech-based risks
- Identifying main areas of concern
- Enhancing cybersecurity competence in your organization

To introduce how human factors pose a rising challenge for cybersecurity, we propose a holistic view on all relevant objects in need for cybersecurity measures, which are the digital assets of an organisation (see Figure 1). These include not only digitally stored information (data) and financial assets, but also the knowledge/know-how and reputation of an organisation (in so far as they are stored/represented digitally and can therefore be targeted via digital based attacks). Cybersecurity is successfully maintained if an organisation is the only entity who can change the integrity, control rights and access rules of those assets (= asset security properties). Cybersecurity measures address the technical and non-technical (= human factor related) vulnerability layers of an organisation: the soft-/hardware layer (as handled by IT security), the physical layer (e.g. door security, access rules for buildings), the social layer (all employees of an organisation), the legal layer (responsible for legally based threats to an organisation) and the ethical layer (e.g. when disinformation campaigns attack the reputation of an organisation).

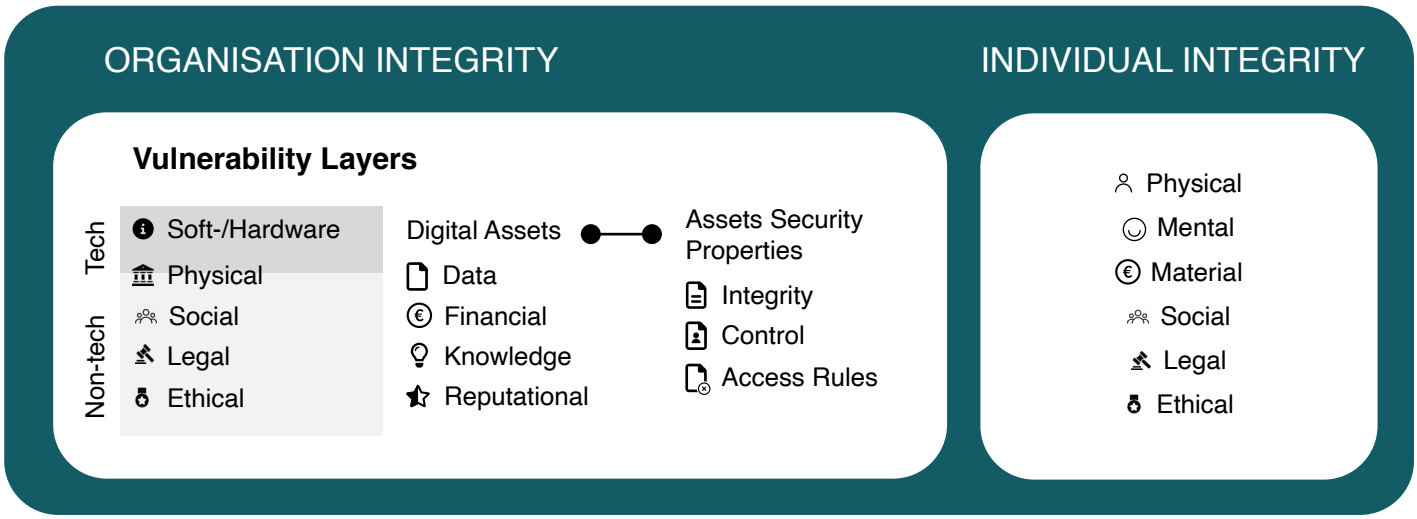


Figure 1 Interdisciplinary approach to cybersecurity

As the cybersecurity research & innovation efforts of the SOTER project must be understood within the European legal and ethical frameworks, European values and fundamental rights must

be considered as integral part of any effort for improving cybersecurity. In SOTER this is represented by additionally considering the integrity of any individual involved in cybersecurity measures (incl. the physical, mental, material, social, legal, and ethical integrity). Cybersecurity "made in Europe" therefore should put efforts to protect the organizational as well as the individual integrity together to implement and support not just in a stricter sense secure but an overall trustworthy digital environment. In the following human factor-related sections we will focus on the social layer, where behaviour of internal and external actors has an impact on cybersecurity.

2

Threats and Risks

2.1. Understanding the role of the human factor

While cybersecurity is broad in both nature and scope, it is important to consider that human behavior is nearly always at the heart of effective cybersecurity.

Human conduct can be split into different forms depending on their foundational processes and the intentionality underlying them (see Table.1).

Human Processes	Unintentional	Intentional
Psychologically founded	Behaviour	Action
Socio-psychologically founded	Practice	
Socially founded		

Table 1: Forms of human conduct

Organizations rely on humans at every layer of their operations, and in every department. It is possible to view human factors-based cybersecurity as situated in individual and psychological human attributes, in turn impacted by sociological and organizational factors.

At the individual and psychological level, attributes such as situational awareness, threat perception, cognition and decision making, demographics, motivation, personal and professional responsibility all impact on how the human affects cybersecurity in organizations.

At the organizational and sociological level, aspects such as governance, team dynamics, team work, management style and management culture all influence and shape how humans navigate the sometimes-complex world of cybersecurity in the workplace.

2.2 Human factor threats

The more recent holistic views of cybersecurity increasingly incorporate the human as an integral part of effective cybersecurity, especially when trying to develop effective cybersecurity policies and procedures within their own organization. It is possible to understand the human factors threat model of organizations through four core dimensions:

- Malpractice
- Negligence
- Accidental
- Malicious intent

The basic understanding in the outline of (non-) tech-based risks in cybersecurity lead to the identification of three main areas of concern:

1. Human error
    a. Lack of compliance
    b. Negligence
    c. Malpractice
2. Malicious insiders
    a. Actions intended to harm the organisation
3. Legal & ethical threats
    a. GDPR related incidents
    b. Disinformation
    c. Public perception of organization

The three areas need to be distinguished because each one of them needs dedicated measures to improve the overall cybersecurity of an organisation. Human error is principally based on the assumption that employees do not intend to cause cyber incidents and therefore can be trained to enhance their awareness and skills to avoid future errors. Additionally, organisational obstacles for proper cybersecurity behaviour can be addressed. Malicious insiders on the other hand cannot be trained, as they intend to cause damage to the organisational integrity. On the one hand prime causes of their motivation might be removed (e.g. disgruntlement of employees due to bad management practices) and basic monitoring of sensitive domains can be used. Legal & ethical threats need specialized employees who are able to perceive and handle them (e.g. the legal or marketing department).

2.3. Existent human factor based threat vectors in the finance sector

Based on ENISA's threat landscape reports and the CAPEC™ taxonomy, we will explain the human-factor related threats briefly in turn and argue why further adjustment is needed for a more plausible perspective on human factor related cybersecurity threats in the extended financial services sector.

According to ENISA, **web applications** attacks are on the rise. These attacks include SQL (i) Injection and Cross-Site scripting (XSS) attacks, exploiting weaknesses in web applications and services. However, with one exception (the Flash Injection, see CAPEC) web application attacks commonly do not require to deceive the end-user. This becomes clear from ENISA's suggested mitigation measures as well, hence this attack vector is discarded from the threat ranking related to the human factor.[1]

Insider threats are cybersecurity incidents that result from actions of an "insider", i.e. someone working for or affiliated with the potential victim (organisation). The most common insider threat pattern occurs when the attacker collaborates with an inside actor, often providing monetary incentives to convince the insider. However, it is often difficult to distinguish between legitimate, malicious and erroneous actions of insiders.[2]

Malware is perhaps the best-known cyberattack next to Phishing emails. It comes in all shapes and sizes, ranging from viruses, worms, spyware to ransomware. The common goals of a malware attack are information or identity theft and service disruption.[3] Malware is also a significant threat in the human factor domain because it often depends on the successful manipulation of, for example, an employee of an organisation (e.g., installation of malicious software in the attachment of an e-mail).

In a **data breach**, sensitive and sometimes confidential information is accessed without proper authorisation, typically by a malicious actor. It is commonly the result of a previously conducted cybersecurity attack, such as a phishing attack. Frequently, data breaches can be attributed to human error.[4]

As elaborated in D6.2[5], 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"[6]. An Identity Spoofing attack may manifest in various ways, certainly most prominently as a Phishing attack. As such, it is relevant to two of the top three threats listed by ENISA.

CAPEC™ defines **Resource Location Spoofing** as "an adversary deceiving an application or user and convincing them to request a resource from an unintended location"[7]. By spoofing the location, the attacker may cause an alternate resource (such as malware) to be used. Thus, this attack pattern may be considered as a variant of phishing attacks and is frequently employed in social engineering attacks.

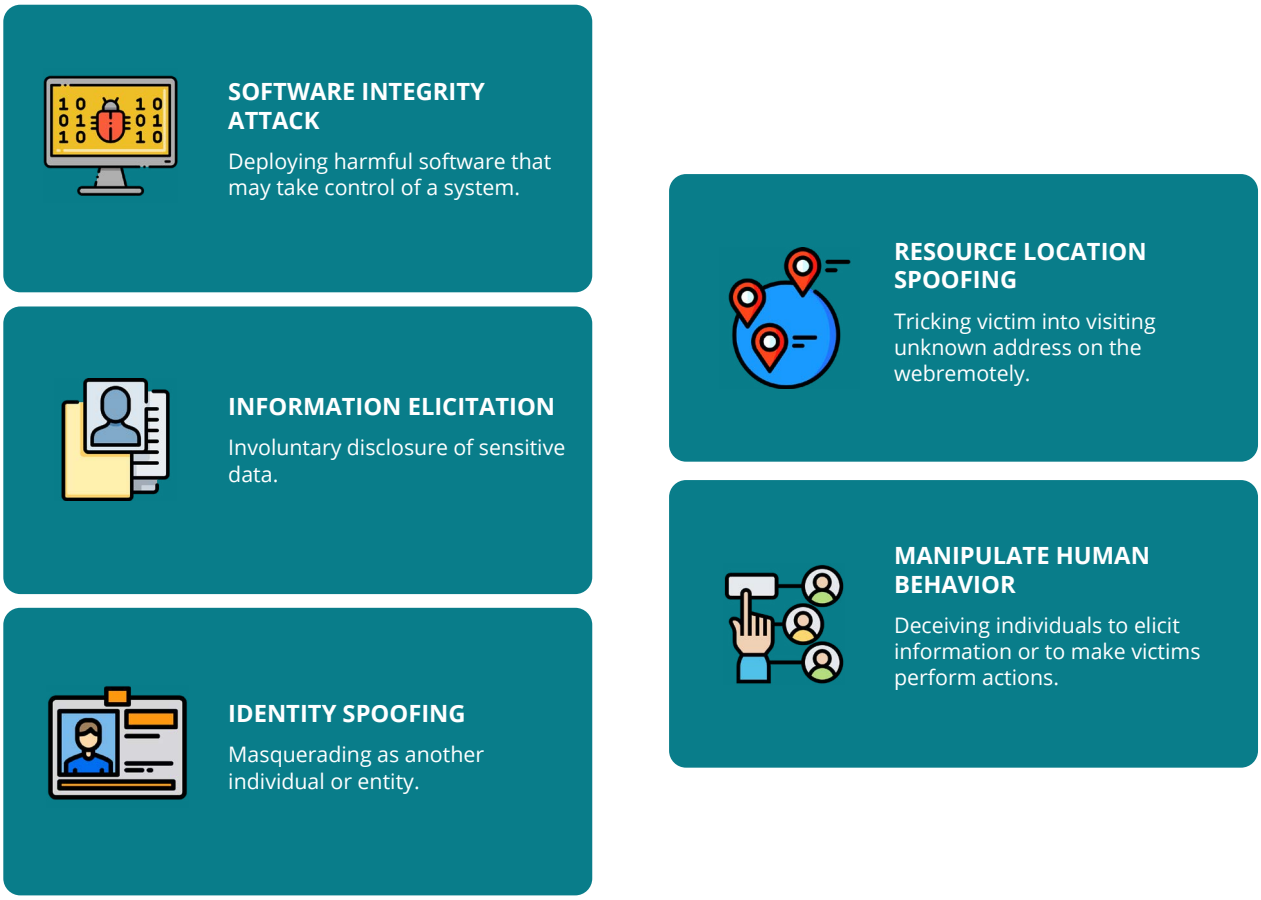
In a **Software Integrity Attack**, "an attacker initiates a series of events designed to cause a user, program, server, or device to perform actions which undermine the integrity of software code, device data structures, or device firmware,

1 ENISA Threat Landscape 2020 - Web application attacks. Report, available at https://www.enisa.europa.eu/publications/webapplication-attacks/at_download/fullReport. Accessed 2021/07/08.
2 ENISA Threat Landscape 2020 - Insider Threat. Report, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat/at_download/fullReport. Accessed 2021/07/08.
3 ENISA Threat Landscape 2020 – Malware. Report, available at https://www.enisa.europa.eu/publications/malware/at_download/fullReport. Accessed 2021/07/08.
4 ENISA Threat Landscape 2020 - Data Breach. Report, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach. Accessed 2021/07/08.
5 D6.2, pp. 24-37
6 https://capec.mitre.org/data/definitions/151.html. Accessed 2021/07/08
7 https://capec.mitre.org/data/definitions/154.html. Accessed 2021/07/08.

achieving the modification of the target's integrity to achieve an insecure state"[8]. It is therefore equivalent to ENISA's malware threat.

The **Information Elicitation** 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"[9]. This broad definition covers a lot of ground, with the most notable standard attack pattern being Pretexting. It is therefore relevant to virtually every social engineering attack.

Lastly, the Manipulate Human Behaviour 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"[10]. 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. Taking both together should encompass many, if not all, typical social engineering techniques.



8 https://capec.mitre.org/data/definitions/184.html. Accessed 2021/07/08.
9 https://capec.mitre.org/data/definitions/410.html. Accessed 2021/07/08.
10 https://capec.mitre.org/data/definitions/416.html. Accessed 2021/07/08.

Based on research conducted in SOTER's D6.2, we have matched meta attack patterns as provided by CAPEC™ to the corresponding top threats as suggested by ENISA. Web application attacks and related terms are in brackets to signal that the attack vector was excluded from the human factor-based analysis. Other terms in brackets signal that the attack vector is usually a result from a previous successful attack. The following table presents the most prevalent human-factor based cybersecurity threats as provided by two of the most renowned threat taxonomies.

ENISA	CAPEC™
(Web application attacks)	(Parameter Injection) (Action Spoofing)
Insider threat	Identity Spoofing Resource Location Spoofing Information Elicitation Manipulate Human Behaviour (Software Integrity Attack)
Malware	Software Integrity Attack Manipulate Human Behaviour
Data breach	Identity Spoofing Resource Location Spoofing Information Elicitation Manipulate Human Behaviour

Table 2 Comparison of ENISA and CAPEC hf-based threats

3

SOTER Risk Mitigation Solutions

3.1. What to train: Cybersecurity competences needed by general employees in the finance sector

Through digitization the finance sector has been transformed and is ever more transforming. New digital services alter the threat landscape rapidly[1], bringing forth new risks for financial services employees. Because the sector is part of critical infrastructure, its continuous functioning is indispensable. However, the list of threats to its security ranges from simple accidents to highly sophisticated and organized cybersecurity attacks[2]. 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. This changed dramatically due to the emergence of FinTechs, organisations which provide financial services that are available on the Internet always and everywhere. Having financial services "always on" and "always available" blurred the network perimeters of financial institutions providing these services and made it impossible to use the old silo-approach for all business data[3]. Increasingly sophisticated technical cybersecurity measures are thus being implemented, using "security by design" as a central approach. However, in order to maintain certain business functions, a trade-off between security and functionality is often being made, leaving humans in the loop. There, training humans to act and interact in a secure manner with new technologies is essential

Analyses within the SOTER project showed that one of the most promising ways of enhancing employee's cybersecurity behaviour is competence training, as only raising cybersecurity awareness does not seem to result in consistently measurable behavioural change.[4] Many existing cybersecurity training approaches, however technically profound, lack a sound pedagogical foundation and a genuine understanding of human behaviour. We are going to fill that gap by introducing a holistic training approach that is pedagogically as well as social-theoretically sound and which applies methods suitable for behavioural change.

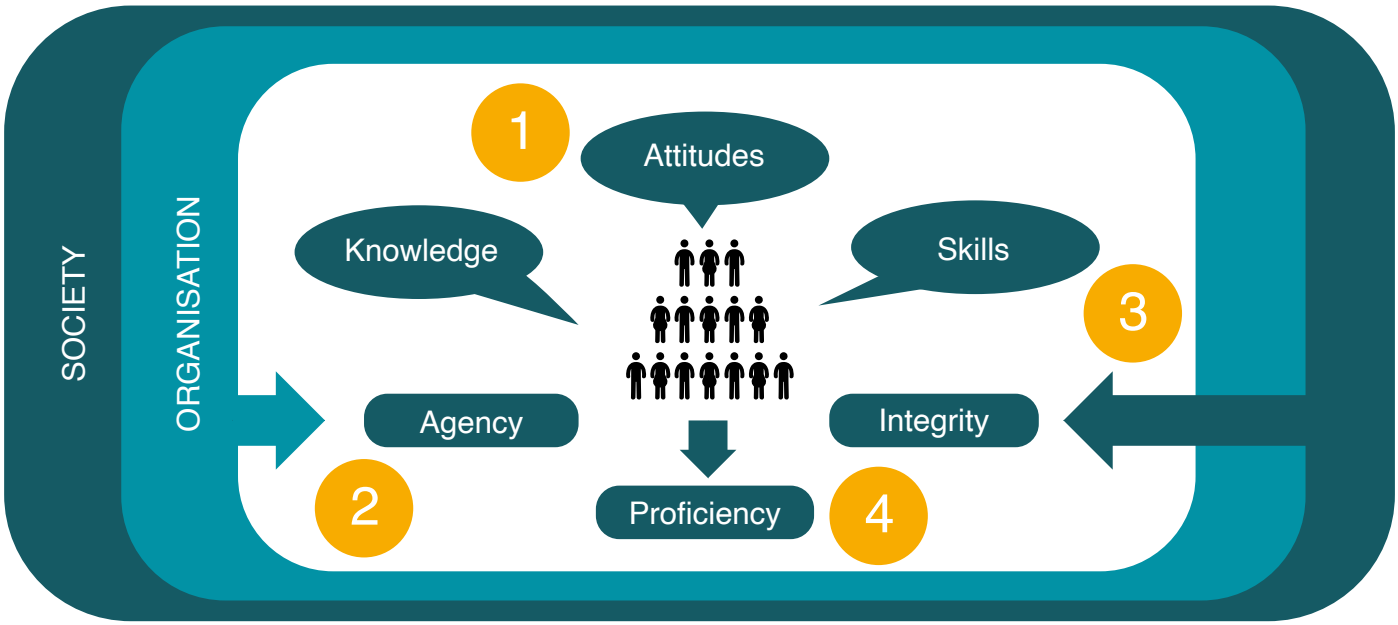
In scientific literature, competence is defined as the general capability of individuals to act and solve problems independently in a given situation based on their capabilities, knowledge, skills, proficiency and attitudes[5]. While many definitions in research and practice attribute the realization of competence merely to the individual[6] , we want to add a genuine social-context-perspective. As

research about the performance of competences has shown, competences can only be realized in and through the consent of the social system in which the individual is situationally located[7]. Individuals not only need the ability to act competent, they also need agency and contextual motivation to perform their competences[8]. In combination with the overall definition of cybersecurity developed

1 Lin 2016
2 Lin 2016, Kryparos 2018
3 Kryparos 2018
4 Dodge et al. (2007); Briggs et al. (2017).
5 Müller-Frommeyer et al. 2017
6 As identified by Kurtz & Pfadenhauer 2010
7 Kurtz & Pfadenhauer 2010
8 Pfadenhauer 2010

in the SOTER project, the following definition of cybersecurity competence arises:

> *"Cybersecurity competence is the capability, **willingness** and **agency** of persons to **solve cybersecurity problems individually or in cooperation with others** based on their **knowledge**, **skills, attitudes** 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 measurably safeguarded."*



1. Employees need knowledge, skills and corresponding attitudes as a sound basis
2. The organizational context supports employees in performing their competence by boosting their agency and motivation
3. By supporting the feeling of integrity with societal rules and norms, the organization fosters attitudes and motivation to perform cybersecurity competence
4. Through applying and exercising their skills and knowledge, employees reach proficiency

3.2. How to train: Training modules and methods

Our training methods focus on fostering cybersecurity knowledge, skills and proficiency as well as enhancing the willingness and agency of trainees to solve cybersecurity problems individually or together with others. To reach that goal, training methods go beyond mere knowledge-building. According to the definition of competence we are applying, knowledge is only one of five dimensions of performable competence to be trained.

Cybersecurity competence trainings must provide employees with the necessary knowledge about potentially problematic cybersecurity situations

and subsequently convey the appropriate behaviour to address these situations. Building on that knowledge, the corresponding job-function-oriented skills must be acquired and practiced until employees reach proficiency in performing these skills. In addition, attitudes of employees to foster their motivation and sense of agency have to be built up. Because of our trainings, employees should experience growing levels of proficiency in tackling critical cybersecurity situations in a context that enables high levels of individual agency for them to perform their competences.

However, solely training employees in a way that motivates them to act and to feel empowered to act is not enough to ensure they can realize their cybersecurity competences within their organisational context. To that end, the overarching organisational structures must support and cultivate the realization of competences. Organisations often cultivate structures that work well for some intended goals, but result in unintended consequences for others. For example, in banks certain quantity-oriented performance measures like customer contact counts motivate employees to work more efficiently, but at the same time these measures may be counteracting secure cyber behaviour, because employees are encouraged to prioritize quantity over security. For cybersecurity competence trainings to work effectively, these conflicting structures need to be identified and tackled. This conflict may be resolved by conducting trainings for employees as well as for management. Management also needs to acquire knowledge and skills to direct organisational structures in a way that secure behaviour by their employees is enabled as best as possible and that their employees feel safe to make use of their cybersecurity competences.

That is why in the SOTER Cybersecurity Competence Training solution is applied on the employee level as well as on the management level and does not only target the individual – but the building of cybersecurity neural nets within single individuals as well as throughout the whole organisation.

The SOTER CSCT solution is built on a comprehensive collection of competences needed by employees for good cybersecurity practice in an adaptable competence catalogue. Until now it contains 22 cybersecurity competences, ranging from handling personal and business information confidentially over interacting safe in the digital realm to identity fraud recognition and incident reporting. The identified competences will be extended as new insights, risks and threats come up. For a better handling in training, these competences were grouped into four training modules. The first two training modules cover competences that are needed to prevent incidents, while the third and fourth module are more concerned with recognizing threats and anomalies, and handling incidents in the case of their occurrence. Cross-cutting all modules, reflective and problem-solving competence is built up through targeted exercises. The suggested training methods for each submodule are state of the art in pedagogical research.

SOTER CSCT allows for flexibly building use cases tailored to the problems at hand, may it be a need for routine cybersecurity competence development or a training that reacts to a new, unforeseen threat. Also, it allows analysing, tracking, and assessing competence development throughout the whole organization in a systematic and traceable process.

A - DIGITAL INFORMATION COMPETENCE

- A1 - Confidential personal data and information handling
- A2 - Confidential business data and information handling
- A3 - Responsible sharing of private information
- A4 - Privacy setting for private digital devices and services
- A5 - Assessment of accuracy and integrity of information

B - DIGITAL SAFETY COMPETENCE

- B1 - Physical Safety
- B2 - Safe Browsing
- B3 - Network Handling
- B4 - Safe Digital Communication
- B5 - Assurance of Device Safety
- B6 - Creation of Safe Credentials

C - THREAT AND ANOMALY RECOGNITION

- C1 - Social Engineering Recognition
- C2 - Malware (Infection) Recognition
- C3 - Physical Environment Sensibility
- C4 - Identity Fraud Recognition
- C5 - Insider Threat Recognition

D - INCIDENT HANDLING

- D1 - Incident Documentation
- D2 - Incident Reporting
- D3 - Incident Communication
- D4- Collaborative Incident Management

X - CROSS-CUTTING CYBERSECURITY COMPETENCES

- X1 - Identification of Cybersecurity Competence Gaps
- X2 – Problem Solving Competence

3.3. Set up your own cybersecurity training program and governance strategy

In this section of the Digital CSCT Handbook, you receive guidance on how to set up your own cybersecurity program.

At first you need to identify the training needs of your organization. This is important for a careful use of your business resources, because it allows you to align your organizational security needs with an ideal customization of cybersecurity trainings for your employees. The following steps are crucial for determining your organizational training needs and customizing the trainings to fit your employees:

1. Ask yourself: What are your sector specific cybersecurity risks and what do different employee groups need to face these risks?
2. Make a list of these cybersecurity risks and associate employee groups with the risks you identified.
3. If you are unsure about cybersecurity risks in your organization, it might be worthwhile integrating your cybersecurity team or contractor into the process. Also, connect with cybersecurity experts within your sector on the newest threats and risks.
4. Select the competences you want to train based on your threat analysis.

Now you know what you need to train within your CSCT and which employee groups you are targeting. A few more tips to consider:

USE LANGUAGE YOUR EMPLOYEES UNDERSTAND BEST

Use simple language that reflects the educational level of the employee group you want to adress. While employee groups concerned with ICT related tasks may prefer the use of technical terms, other employee groups may not understand them. Translate technical terms for these employee groups into explanations they can easily understand.

MOTIVATE YOUR EMPLOYEES TO PERFORM THEIR CYBERSECURITY COMPETENCES

Set up a cybersecurity training regimen that applies just the right amount of control while respecting your employees' privacy rights. Empower your employees to take over responsibility for their cybersecurity-behaviour in a way that fits their abilities. Balance control and empowerment well.

GAMIFY WITH CARE

For some employees gamification works best, but there are some who do not like it at all. Especially minimalistic gamification is proven to enhance acceptance of training programs of banking employees. Animate your training actions visually, apply narrative-based storytelling and motivate your employees with interactive elements. But always give those who do not like gamification an option to train traditionally.

USE USE CASE COURSES FOR NEW CHALLENGES

For adapting to new or complex cybersecurity challenges within your sector, train your employees on preventing, recognizing and handling cybersecurity incidents through cross-cutting interactive use case courses.

Use Case courses could cover:

- Identity fraud
- New account fraud
- Biometric spoofing
- Synthetic identity fraud
- Risks in digital customer onboarding
- Social Engineering for ransomware attacks
- Employee taregeted phishing
- ...

APPLY SINGLE CONTENT COURSES AS REFRESHERS OR INTRODUCTIONS

Single content courses are ideal as introduction or short refreshers on certain competences.

Single Content Courses could cover:

- Confidential personal data handling
- Confidential business data handling
- Assurance of private device safety for home office
- Password security
- Incident reporting
- GDPR Compliance
- ...

Regular cybersecurity competence training is a good way of securing your organization from cybersecurity incidents that are based on human error. However, sometimes you might need to get cybersecurity relevant information including actual real-world incident information to your employees quick and short, or you may want to keep their vigilance up constantly. Also, some of your employees you might not reach with classical training courses. For that, experts in research and practice suggest implementing a multi-channeled training regimen with a high density of interactions between the staff that is implementing your training regimen and the employees to be trained.[1] Through using different channels and modes for cybersecurity relevant information you may reach every kind of employee in a way they understand best. Using media richness in your training regimen may counteract monotony of your training actions and thus prevent your employees from overseeing important cybersecurity information due to habituation.

It may also increase the effect of your training regimen to match channels and modes with the problem at hand. [2] Time sensitive cybersecurity problems may best be addressed with fast communication channels like e-mails and screen saver messages, while training on basic cybersecurity competence may best be achieved by e-learning or face-to-face courses.

- face to face courses
- online training
- e-learning
- presentations
- information events
- e-mail communication
- newsflashes
- posters
- flyers
- videos
- Information snippets during startup of computers of employees
- Screensaver messages
- companywide cybersecurity campaigns
- cybersecurity guides, manuals and policies on the intranet

When you are training your employees on cybersecurity competence and they are doing well within these trainings, but do not seem to transfer the learned contents into practice, maybe take a closer look at your management practices. Sometimes, employees cannot perform their cybersecurity competences because performance goals are in the way. Stress may overwhelm your employees, so they prioritize the tasks that have the next urgent deadline, while cutting back other tasks that are not (yet) pending. Cybersecurity tasks thus might get overlooked, until their neglect causes an incident. But not only stress might cause neglection of cybersecurity tasks. Employees might also backrow cybersecurity tasks if they perceive them as not important for their work or career ambitions.

1 Bauer et al. 2017, Abawaji 2014 and Aldawood/Skinner 2019
2 Abawaji 2014

4

Compliance and Regulation

4.1. Legal Requirements for Awareness and Training

Since the human factor in cybersecurity is widely recognized as a main concern for incidents, measures related to improve the cybersecurity awareness and behaviour of general employees are increasingly addressed in regulatory considerations. The main elements are awareness and training. Currently, legal requirements are yet just addressing basic elements for human factor related aspects of cybersecurity. A main challenge for compliance considerations is the indirect obligation to follow state-of-the-art cybersecurity procedures which are defined not in the regulatory texts but through standards of the cybersecurity industry.

The Payment Services Directive and the respective national implementing law requires an information security policy be implemented in the process of application for authorisation as a payment institution[1], which shall take into account the guidelines issued by the EBA on ICT and security risk management[2].

While PSD2 does not explicitly contain requirements in regard to **training** and the NIS Directive only requires Member States to ensure that operators of essential services take appropriate and proportionate technical and organisation measures to manage the risks posed to the security of network and information systems[3], the EBA considers "security training and awareness, and monitoring of emerging risks, to be reasonable and plausible security measures designed to mitigate security and operational risks"[4] in their corresponding guideline. Therefore, information security policies, training and awareness can be considered as important domains for cybersecurity measures in the finance sector.

4.2. Human factors of cybersecurity governance

This section turns attention towards the human-factor based aspects of cybersecurity, through analysis of current standards, guidelines, and best practices, especially in relation to incident handling in the context of cybersecurity governance. The SOTER project follows a broad understanding of incident handling, as it is understood to not only refer to completed *action after a cybersecurity incident occurs* (e.g., incident reporting) but also to the organisational and individual capacities to *detect early potential incidents*. It starts with an overview of key elements on training and awareness in sectoral guidelines, adds information on requirements from leading standards, and then discusses current relevant initiatives for improving cybersecurity in the human factors domain. While only a few aspects of these discussions are currently represented or just superficially addressed in the regulatory landscape, the contents point to potentially significant improvements to address human factor related cybersecurity incidents.

4.2.1 EBA Guidelines on ICT and Security Risk Management

Information security policy

The information security procedure required to be established under the Payment Services Directive[5] and the relevant national law transposing this directive should allocate the main roles and responsibilities of information security management, setting out requirements for both

1 Art 5 (1) lit j Directive (EU) 2015/2366.
2 Art 5 (1) subparagraph 2 Directive (EU) 2015/2366; EBA/GL/2019/04.
3 Art 14 Directive (EU) 2016/1148.
4 EBA/GL/2017/17, p. 12, which has now been repealed by EBA/GL/2019/04, but the importance of training and awareness is still stressed, EBA/GL/2019/04, p. 22.
5 Art 5 (1) lit f Directive (EU) 2015/2366.

staff and contractors of the financial institution.[6]

Based on this information security policy, financial institutions should implement security measures in order to mitigate ICT and security risks, including measures in regard to logical, physical and ICT operations security, security monitoring, information security reviews, assessment and testing as well as information security training and awareness.[7]

Information security training and awareness

Information security training and awareness is considered one of 7 key measures to mitigate ICT and security risks.[8] The other 6 are organisation and governance in accordance with paragraphs 10 and 11; logical security; physical security; ICT operations security; security monitoring; information security reviews, assessment and testing[9].

- Monitoring the threat landscape and situational awareness can be considered as a task to be fulfilled by dedicated IT security personnel.[10]
- According to EBA, PSPs "should establish periodic security awareness programmes" to ensure that staff and contractors "are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks"[11].
- Periodic security awareness programmes "should require PSP personnel to report any unusual activity and incidents."[12]
- PSPs should not only enhance the security awareness of their employees but also of payment service users on "security risks linked to the payment services by providing PSUs with assistance and guidance"[13]
- Training programmes should be established for all staff and contractors[14]
- According to EBA guidelines, "financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including information security"[15]
- Payment service providers "should establish a **training programme** for all staff to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures in order to reduce **human error, theft, fraud, misuse or loss**."[16]
- According to the EBA, training programmes should be provided annually or "more frequently if required"[17]. The guidelines do not specify in which cases more frequent trainings are required.
- Management "should ensure that the allocated budget is appropriate to fulfil the ICT operational needs and security risk

6 EBA/GL/2019/04, p. 18.
7 EBA/GL/2019/04, p. 18.
8 EBA/GL/2019/09, p. 18.
9 EBA/GL/2019/04, p. 18.
10 EBA/GL/2017/17, p. 23 and according to the revised EBA Guidelines on ICT and security risk management, regular threat monitoring is considered important as well, see: EBA, EBA/GL/2019/04, p. 17.
11 EBA/GL/2019/04, p. 22.
12 EBA, EBA/GL/2017/17, p. 24, the Guidelines in place currently also provide for the reporting of ICT and security risks, see: EBA, EBA/GL/2019/04, p. 15–16.
13 EBA, EBA/GL/2017/17, p. 24, the Guidelines in place currently also provide for the reporting of ICT and security risks, see: EBA, EBA/GL/2019/04, p. 28.
14 EBA/GL/2019/04, p. 22.
15 EBA/GL/2019/04, p. 14.
16 EBA/GL/2019/04, p. 22.
17 EBA/GL/2019/04, p. 14.

management processes on an ongoing basis.[18]

- Information sharing: Information sharing has been considered by the EBA as part of their guidelines for the implementation of PSD 2 but have been subsequently removed. The now repealed guideline from 2017 still *encouraged* participation in information sharing platforms with "other PSPs and relevant third parties such as operators of payment systems, industry associations, etc."[19]

4.2.2. Requirements from leading standards

The listed requirements in this sector complement the legal requirements for awareness and training discussed in section 2.4 and from sectoral guidelines (3.4.1).

Education and determination of competence: According to ISO 27001, an "organization shall

- determine the necessary competence of person(s) doing work under its control that affects its information security performance;
- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- retain appropriate documented information as evidence of competence."[20]

Cybersecurity Awareness and Training:

ISO 27000 considers the following as a critical success factor for information security management: "an effective information security awareness, training and education programme, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards, etc., and motivating them to act accordingly."[21]

ISO 27001: "Employee training to understand the problem of social engineering and to recognize situations that might be an indicator of, or precursor to, a social engineering attack and understand how to apply company policy procedures to social engineering attacks for protection information".[22]

According to ISO 27001, personnel "shall be aware of:

- the information security policy
- their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
- the implications of not conforming to the information security management system requirements."[23]

Awareness should also be enhanced in regard to "detection, prevention and recovery controls to protect appropriate against malware".[24]

"All employees of the organisation and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function"[25]

18 EBA/GL/2019/04, p. 14.
19 EBA/GL/2017/17, p. 94; although this encouragement is no longer included in the most recent version of the Guidelines (EBA/GL/2019/04), it nevertheless shows that such topics continue to be discussed and might become again relevant in future recommendations or guidelines.
20 ISO/IEC 27001:2017, Section 7.2.
21 ISO/IEC 27000:2019, section 4.6.
22 Humphreys, E. (2016). Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House, p. 112
23 EN ISO/IEC 27001:2017 section 7.3.
24 EN ISO/IEC 27001:2017 section 12.2.1.
25 EN ISO/IEC 27001:2017 Annex A.7.2.2.

Cybersecurity and recruiting:

ISO 27001 provides some guidance on aspects of recruitment, in order to ensure that the human resources employed in an organisation do not negatively impact on the cybersecurity levels of the organisation. This includes the conducting of background checks. Prior employment history, screening and clear outlining of roles and responsibilities. It is all deemed as part of the Information Security Management System (ISMS), and is contained within *Annex A.7 - Human Security Management*.

Involvement of Management

ISO 27000 also proposes that both support and commitment should be sought from all levels of management, especially those at the top of the management tree. This is considered a critical success factor for information security management systems, and an integral part of any organisation's human factor-based security strategy.[26]

Personnel security controls

The SANS Institute identifies four "personnel security controls"[27] (SANS 2008) defined as such:

- Background checks and screening
- Confidentiality, nondisclosure, authorized use agreements
- Job descriptions
- Training in security awareness and compliance

26 ISO/IEC 27000:2019, section 4.6.

27 SANS 2020: Security Assessment Guidelines for Financial Institutions, https://www.sans.org/reading-room/whitepapers/auditing/security-assessment-guidelines-financial-institutions-993, accessed 2021-07-22.

5

References

Abawajy, J. (2014) User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* **33** (3), 237-248.

Aldawood, H. & Skinner, G. (2019) Reviewing Cyber Security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues. *Future Internet* **11** (3), 73.

Bauer, K. N., Orvis, K. A., Ely, K. & Surface, E. A. (2016) Re-examination of Motivation in Learning Contexts: Meta-analytically Investigating the Role Type of Motivation Plays in the Prediction of Key Training Outcomes. *Journal of Business and Psychology* **31** (1), 33-50.

Briggs, P., Jeske, D. & Coventry, L. (2017) Behavior Change Interventions for Cybersecurity. In: Behavior Change Research and Theory. Elsevier, 115–136.

Dodge, R. C., Carver, C. & Ferguson, A. J. (2007) Phishing for user security awareness. Computers & Security 26 (1), 73–80.

Lin, T.C.W (2016) Compliance, Technology, and Modern Finace. Brooklyn Journal of Corporate, Financial Commercial Law 11(1), 159-182.

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

Kurtz, T. & Pfadenhauer, M. (eds.) (2010) *Soziologie der Kompetenz,* 1. Aufl. VS Verlag für Sozialwissenschaften, Wiesbaden.

Müller-Frommeyer, L. C., Aymans, S. C., Bargmann, C., Kauffeld, S. & Herrmann, C. (2017) Introducing Competency Models as a Tool for Holistic Competency Development in Learning Factories: Challenges, Example and Future Application. *Procedia Manufacturing* 9, 307–314.

Pfadenhauer, M. (2010) Kompetenz als Qualität sozialen Handelns. In: Kurtz, T. & Pfadenhauer, M. (eds.) *Soziologie der Kompetenz*, 1. Aufl. VS Verlag für Sozialwissenschaften, Wiesbaden, 149–172.