Cybersecurity Optimization and Training for Enhanced Resilience in Finance

D6.1 – Competence Catalogue (I)

[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	Schmidt Nico, Uni GRAZ
	nico.schmidt@uni-graz.at
Other Contributors	Christina Schwarzenbacher, Uni GRAZ
	Eva Griesbacher, Uni GRAZ
	Martin Griesbacher, Uni GRAZ
	Tina Ehrke-Rabel, Uni GRAZ
	Robin Renwick, Trilaterl research
	Charlotte Kelly, InAuth

Due Date	30.11.2019
Delivery Date	29.11.2019
Type	Report
Dissemination level	PU = Public

Keywords	Cybersecurity, competence catalogue, human factor

Document History

Version	Date	Description	Reason for Change	Distribution
V0.0.1	20.09.2019	Draft		20.09.2019
V0.0.2	30.09.2019	Harmonising comments	First comments from Uni GRAZ, new template	
V0.0.5	10.10.2019	First feedback round	Complete first feedback round	13.10.2019
V0.0.6	25.10.2019	Second feedback round	Finalization of Uni Graz feedback	25.10.2019
V0.0.7	15.11.2019	Third feedback round	Finalization of feedback Trilateral, Rise & InAuth	17.11.2019

Abstract

The following Competence Catalogue is a non-exhaustive list of Cybersecurity Competencies that is supposed to provide a starting point and orientation for cybersecurity trainings. It specifically focuses on the human factor in cybersecurity.

The Competence Catalogue is based on research of current best practices, the legal context and cybersecurity considerations. Each competence is described in a fashion that contains an element of awareness, of comprehension and of projection – a common way to describe competences.

In the broader context of the SOTER project, the Competence Catalogue represents the entry point to how companies can increase their cyber resilience and promote the long-term development of a cybersecurity culture.

The current version of the deliverable is only the first part and will be updated in course of the SOTER project. The final deliverable will also include a connection to tangible cybersecurity risks that financial institutions currently face, as well as a deeper look at the legal and social context of cybersecurity competences.

Table of Contents

Executive summary

The SOTER project is a European Commission H2020 funded project entitled "Cybersecurity Optimization and Training for Enhanced Resilience in Finance". This deliverable is part of work package 6 – "Cybersecurity training in finance". The work package intends to provide a set of tools that financial institutions can use to improve their cybersecurity resilience. The basis of the work package is the present document, the "Competence Catalogue". This catalogue will describe a list of competences that financial institutions should aim to build in their employees, with a focus on the human factor in cybersecurity.

Of course, every competence is connected to a specific cybersecurity threat that it is trying to reduce. Therefore, the Competence Catalogue will always have to build on first the current cybersecurity threats that financial institutions face which will be researched in task 2.1 of the SOTER project: "Mapping and understanding human factors in effective cyber-security".

The current version of the Competence Catalogue is only the first version of the deliverable and is currently only including industry agnostic cybersecurity threats. As soon as specific threats of financial institutions have been analysed as part of the SOTER project, the Competence Catalogue will be adapted.

The catalogue starts of by explaining why the human factor in cybersecurity has recently been neglected or is at least often underrepresented in threat analysis. Recent examples show that most large breaches in the past could indeed be interpreted as connected to the human factor. Security breaches have cost companies' large amounts of money in fines as well as reputation losses. Additionally, companies not only should try to avoid costs but also possess some public responsibility, as e.g. described in the EU Charter of Fundamental Rights.

The main part of this document describes what can be done to decrease these vulnerabilities, specifically which competencies can be built up in employees to increase the resilience against cybersecurity attacks. According to current research, competencies are often described as a combination of awareness, comprehension and projection. This Competence Catalogue will work with this understanding and describe competencies in the following way:

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
Leak of confidential digital information to unauthorized individuals	Social engineering attack	Attackers try to manipulate employees in phone calls or E-mails by spreading the sense that they have some sort of connection with the company. Common variants are the impersonation of suppliers or business partners. After targets are persuaded, attackers will try to trigger invoices or the distribution of sensitive data.	Employees should be aware that there might be more information available on the internet (e.g. in message boards, social media or even through data leaks) then they assume. By using such information, attackers can create a sense of affiliation or authority.	Employees should try to steer the conversation in order to find out if the counterpart is who he pretends to be. Social engineering attackers commonly try to steer conversations which should be fought against. Simple questions about proof of e.g. company affiliation might already help to bust attackers.

Preventing malware via non-secure Websites or software

Bob is browsing the internet for a solution that helps him track his currently open tasks. Bob stumbles upon a website that offers a free software that claims to provide a pinboard-like feature where users can digitally save notes and directly link them to their calendar. The software is also available for Bob's phone. Bob reads the description of the software and is pleased by the advertisement. He remembers that he was asked in a training to refrain from installing third party software on his work phone without checking with the IT department first. Therefore, Bob sends an Email to his IT colleagues with the request to check if he can use the application. The IT department researches for a bit and finds out that the app contains a malicious feature that collects all information that is stored in it by users. The IT department suspects malicious intends behind this feature and asks Bob not to use the software. Bob is happy that he asked his colleagues before he started using the application and avoided the stealing of his notes.

How these competences can be built is part of a different SOTER deliverable, namely D6.3 "Training modules compilation".

List of tables

List of acronyms/abbreviations

Table 1, List of acronyms/abbreviations

Abbreviation	Explanation
EU	European Union
SOTER	Cybersecurity Optimization and Training for Enhanced Resilience in Finance

1. Introduction

The financial sector is facing considerable cybersecurity threats. Financial institutions manage large amounts of sensitive customers' data and offer an entry point to personal accounts. Companies in the financial sector face risks of data breaches and direct financial losses. Additionally, they have to deal with new regulations. This attack angle poses a large challenge, especially for newcomers in the financial sector. Conventional market players often maintain expansive dedicated departments in charge of cybersecurity, but e.g. start-ups sometimes neglect the importance of security measures or struggle with keeping their systems security up to date while dealing with rapid company growth, fast-changing applications and complex IT infrastructure. However, by far traditional banks are not safe either, large scale user data breaches become public regularly[1].

Financial institutions must assess cybersecurity risks very closely and take countermeasures. Risk mitigation efforts can vary from improvements in the technical infrastructure like patching vulnerabilities to training employees. A holistic cybersecurity strategy can only succeed as a combination of both. Therefore, the SOTER project aims to deliver a technical component that directly supports sensitive core banking processes (like customer authentication) as well as comprehensive training activities for financial employees. Together, both shall increase the resilience towards cybersecurity attacks for financial institutions.

An important commonality in many security breaches seems to be the human factor. In fact, a large part of past attacks might have been prevented by well-trained staff[2]. Hence, cybersecurity competencies should be part of every employee's job profile in the best interest of a financial institution.

But specifically, what skills should employees in the financial sector build up in order to increase their employer's cybersecurity resilience? The following catalogue will define a set of competencies that

[1] Sandler, "Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested"; NG, "How the Equifax Hack Happened, and What Still Needs to Be Done - CNET"; CISA U.S. Department of Homeland Scurity, "Apache Software Foundation Projects"; Collier, "Alleged Hacker May Have Hit Other Targets - CNN". See also: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ for an interactive visualisation

[2] Ponemon, "Separating the Truths from the Myths in Cybersecurity - Independently Conducted by Ponemon Institute LLC".

tries to answer exactly this question. It is intended to provide a solid basis for the SOTER training activities that will be carried out as part of the project.

The goal of this document is to provide a first draft of a cohesive cybersecurity competence catalogue. The described competences are relevant for employers of financial institutions. This catalogue defines the competencies that an employee should have in order to identify threats and to deal with them in the best interest of his employer. This catalogue lists competencies for employees and not citizens who might have different needs e.g. in order to protect their privacy. Finally, the implementation of the competence catalogue in cybersecurity trainings contributes to decrease the cybersecurity risks of financial institutions, specifically those that are connected to the human factor. Even though, the competencies are intended to increase the resilience against cybersecurity threats, it will also generally increase the awareness and skills of employees which supports them not only in their role as an employee but also as a citizen.

As this document is the first part of the actual deliverable, it will always retain the status of a draft and might be subjected to further rework. Additionally, the goal for the second part of the deliverable is to include specific cybersecurity aspects that are directly connected to the infrastructure that is created with the SOTER project.

2. Cyberthreats and public responsibility

This chapter points to a twofold problem in that financial institutions currently face: a high frequency and caused damage through cybersecurity attacks and an increase in demand for trustworthy companies, based on regulation and public demand. As mentioned, this document will provide a basis for the human factor in cybersecurity, however, there is of course the technical factor as well. Technical cybersecurity threats for financial institution will be analysed in more details in the technical part of the SOTER project.

2.1 Cybersecurity Attacks and the human factor

At the time of writing there were several major cybersecurity breaches in the recent past[3]. Two of the largest and most interesting breaches in the financial sector include the Equifax hack of 2017 and in 2019 the Capitol One and UniCredit hack[4].

In July 2019, Capital One confirmed that sensitive financial information such as social security numbers, bank account numbers, names and addresses were stolen from more than 100 million people. The information was extracted from application forms, meaning that not all leaked information were Capitol One customers but even having applied for a Capitol One credit card in the past could have led to someone's financial information being stolen. The hack was conducted by a former employee of a cloud computing provider who worked as an external for Capitol One and gained access to the company's cloud servers. While the hack took place in March, Capitol One only knew about it four months later[5].

The Equifax hack used a slightly different attack angle. Between May and July 2017 hackers stole names, social security numbers, credit card numbers, birth dates and even driver's license numbers

[3] An interactive visualisation of the latest breaches can be found here: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[4] Kumar, "UniCredit Bank Suffers 'Data Incident' Exposing 3 Million Italian Customer Records"; Collier, "Alleged Hacker May Have Hit Other Targets - CNN"; NG, "How the Equifax Hack Happened, and What Still Needs to Be Done - CNET".

[5] Sandler, "Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested".

of more than 145 million American consumers. The hackers still have not been identified[6]. The way they proceeded was looking for servers with vulnerabilities that were already publicly available[7]. They were not buying 0-day vulnerabilities[8] or searching for vulnerabilities on their own, they merely looked for officially logged vulnerabilities, and companies that did not update their systems fast enough.

The two examples therefore are similar in some ways and differ in others. Both share a similar matter that was stolen: personal information including social security numbers, addresses and sometimes even credit card data. The damage for the affected was therefore quite similar and seems to be characteristic for the financial sector. Both hacks do not seem to be addressed at the hacked company specifically, yet they proved to be attractive targets, in the case of Equifax by having a public vulnerability in its server structure. It can be assumed that the Equifax hackers simply might have kept on searching for different companies that had the same vulnerability if they had not found Equifax. In the case of Capitol One, the attack angle was not as agnostic, yet it seems there was no motive of retribution[9], but the hacker simply exploited vulnerabilities she was aware of. Regarding the preventability of the Equifax breach, as the Equifax hackers were exploiting publicly known vulnerabilities, it seems obvious that the breach resulted out of carelessness to sufficiently secure running systems. So far there has not been any notice about internal sources in the hack, therefore the lack of action on Equifax side seems to lie in employee's negligence. In case of Capital One, it is still unclear how exactly the hacker obtained knowledge about the vulnerability and if it was directly connected to her job. If she acted out of the position of an employee, it would surely be an action out of malicious intent[10]. In this case she must be categorised as an external attacker, not enough is known yet to qualify if the vulnerability on Capitol One's side resulted out of an accident or negligence.

The above examples show that currently, financial institutions are facing threats from different angles. What both have in common is a human component. They both show a similar vulnerability that is referred to as *the human factor* of cybersecurity[11]. Specifically, this means, the risk through human

---

[6] NG, "How the Equifax Hack Happened, and What Still Needs to Be Done - CNET".

[7] CISA U.S. Department of Homeland Scurity, "Apache Software Foundation Projects".

[8] Armin, Foti, and Cremonini, "0-Day Vulnerabilities and Cybercrime".

[9] Collier, "Alleged Hacker May Have Hit Other Targets - CNN".

[10] Sandler, "Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested".

[11] Carlton, Levy, and Ramim, "Mitigating Cyber Attacks through the Measurement of Non-IT Professionals' Cybersecurity Skills".

actions for financial institutions (with humans being employees)[12]. Institutions need to consider psychological, personal and social factors of the behaviour of their employees[13]. By contrast, the technological factor of cybersecurity focuses on risks through ill-designed infrastructure, insufficient maintenance tasks or the use of insecure components (software or hardware).

There are three different types of threats that result through the human component in cybersecurity systems: actions out of maliciousness, negligence or accidents[14]. All three motives can result in the same damage for companies but can be avoided by different measures, e.g. denying certain access rights to an employee might prevent all three of the threats. However, in case an employee loses his mobile phone, a company could have a safety plan installed that wipes the device so a potential finder cannot abuse the stored data. Therefore, the employee's negligent behaviour could be compensated by a prepared company.

Cybersecurity breaches in the financial sector which are connected to the human factor pose a considerable challenge. Thus, this part of the SOTER project will try to contribute to lessen this threat, while the technical component of SOTER will reduce technical cybersecurity vulnerabilities.

A more detailed discussion of the actual weaknesses of humans in the handling of applications will following the final version of the Cybersecurity Competence Catalogue. It will be closely linked to the definitions and findings of deliverable 2.1 ("Mapping of human behaviour related threats and mitigation measures") of the SOTER project.

2.2 Public responsibility and trust

Financial institutions face not only cyber risks, they also have responsibilities through regulation[15]. As described in the EU Charter of Fundamental Rights, European citizens have a right to

- the Protection of personal data,
- respect for private and family life

[12] Of course, customers can also be considered as risk factors. As the scope of this report is providing an base for employee trainings, customers will not be addressed closer in this context.

[13] Juanito, "Cyber Security Culture in Organisations".

[14] Antonucci and Durbin, "Identifying, Analyzing, and Evaluating Cyber Risks".

[15] The second version of this deliverable will have a more detailed look at the legal context, specifically the implications of GDPR and PSD2.

- Freedom of expression and information
- Non-discrimination and
- Consumer protection.[16]

The possibility of infringing these fundamental rights must be considered closely when designing applications and database systems. System design can already prevent multiple possible rights violations by e.g. preventing employee's access to sensitive data. However, not everything can be anticipated and prevented by accurate system design. Daily operations must recognize their responsibility as well. According to this twofold challenge, the SOTER project contains both, a technical solution as well as trainings for operational employees.

According to the TRUSSEC[17] project the most common issues citizens have with service providers are loss of control over one's personal data, consent problems (lack of informed consent), security breaches, lack of transparency in company's use of users' data, informational asymmetry between users and providers and data-based discrimination[18]. This is the second component of the human factor. Not only is the human factor referring to a possible source of error, it also describes an important benchmark of the design of applications and IT-Security-Solutions: how to support human processes and activities. The EU charter of fundamental rights, as well as citizens across Europe demand from companies to carefully design and operate their applications in order to prevent data breaches and respectfully take up the task of managing user data. This should be seen as a considerable task for financial institutions.

New market participants and fintech's recognize this paradigm shift (and it's potential) and challenge traditional financial institutions exactly from this angle. Companies try to provide trustless services, promise their customers secure data storage or even build fully decentralised networks where no central company oversees user data. New competitors learn out of the public notion that privacy is a factor that citizens do care about. However, not all new competitors build on the notion of trust.

[16] European Union, "Charter of Fundamental Rights of the European Union (2000)".

[17] TRUESSEC is a European Comission H2020 project which focuses the development of criteria that promote trustworthiness in ICT. More information on TRUESSEC can be found on the project website: https://truessec.eu/

[18] We will assume here that general concerns regarding ICTs are similar to financial institutions which often have access to similar data.

Companies that have received bad press[19] in the past exactly about trust and privacy issues such as Facebook also try to challenge the financial sector with their introduction of its own digital currency – Libra. It has yet to be seen if Libra is to succeed but it can already be said that it could be a re-defining moment for the financial sector especially considering retail banking and instant payments. With the current political backlash[20], it might very well be that Libra will never be used in public, but even then, similar applications will most likely be pushed forward shortly after with high tech companies such as Tencent, Alipay, Telegram[21] or even Amazon potentially working on similar solutions[22].

Summing up, creating a trustworthy institution that is compliant with current regulation and public opinions is a considerable challenge for current market participants as well as fintech.

3. A holistic cybersecurity competence framework

The last chapter stated that financial institutions currently face a twofold problem: A predominant threat of cybersecurity attacks as well as a public demand for trustworthy companies, which is also increasingly backed by EU regulation[23]. This chapter will describe a clear outline on what financial institutions can do in order to increase their cybersecurity and increase trustworthiness[24]. As shown, both challenges contain the human factor.

By building up cybersecurity competencies, employees will strengthen their ability to identify and respond so cyber threats. Additionally, an increase in cybersecurity combined with the commitment

[19] Doffman, "1.5m Users Hit By New Facebook Privacy Breach As Extent Of Data Misuse Exposed".

[20] Nystrom, "Demystifying the Facebook Libra Congress Hearings".

[21] Baydakova, "Telegram Finally Confirms It's Behind TON Blockchain".

[22] As a side note it should be mentioned that currently none of these market challengers are resident in the European Unions which might be either a symptom for European Regulation or an opportunity for a new native company to fill the void.

[23] Which can be seen for example in the EU Cybersecurity act: European Commission, "The EU Cybersecurity Act".

[24] Oltramari et al., "Towards a Human Factors Ontology for Cyber Security".

to properly manage user data will increase public trust in financial institutions. The following sections will explain the components that will help to shape this transformation[25].

Cybersecurity competences are an additional responsibility of employees: they describe how to act in specific situations and must be seen as an important part of every job profile. Employees cannot simply be held accountable for actions they were not trained for, which do not fall under required diligence in the workspace or can be categorised under common knowledge. Therefore, it should be clearly communicated that employees receive additional responsibilities in the form of cybersecurity competencies, yet they must be prepared sufficiently simultaneously. It seems to be very important that this relation is clear. Otherwise, staff might react negatively to changes in their daily work. They might perceive new cybersecurity measures as an unjustified burden, or they have problems with weighing their business responsibilities with cybersecurity aligned behaviour. This could result in employees trying to bypass new cybersecurity requirements, which could even lead to a decrease of an organization's overall cybersecurity resilience.[26]

It also must be mentioned that not only internal factors such as awareness and expertise of employees will lead to a resilient cybersecurity system. External factors such as external stress through workload, general staff motivation or even physical health will affect the ability of employees to act in a secure way, just like they affect the general working behaviour[27]. This competence catalogue will not start to describe how to run a healthy operation but companies should keep in mind that e.g. even if their staff receives the highest standard of cybersecurity trainings and the most up to date infrastructure, an over-worked employee can threaten the security of the whole system by falling for a social engineering attack. When talking about system security, a system can only be as strong as its weakest part[28].

3.1 Awareness

How can a successful competence training look like and what should it contain? First of all, companies as well as employees have to become aware of the current context in which they act. It is a useful

[25] Ibid.

[26] Juanito, "Cyber Security Culture in Organisations".

[27] Oltramari et al., "Towards a Human Factors Ontology for Cyber Security".

[28] Partida and Andina, *IT Security Management : IT Securiteers - Setting up an IT Security Function*.

approach[29] to understand awareness as a mix of three different categories: Perception, Comprehension and Projection. Perception describes the process of identifying threats and attacks. It is the basis for a successful cybersecurity strategy. In order to identify threats, first a stocktaking exercise must be performed. An institution must be aware of its asset, to be able to know what is at risk. Otherwise, it will not be able to protect itself. However, defining what is at risk is inherently not possible without knowing attack schemes. Therefore, both must be mapped against each other. That is the comprehension component of awareness. Comprehending current attack angles and threats helps to realise which assets are threatened and by what. The combination of understanding possible threats as well as what is at stake allows to create projections: forecasting where the biggest risks of a future attack could be, and which vulnerabilities hackers could abuse. Projecting allows to build a cohesive strategy to develop a company in a certain way. It is the ability to be able to describe how the company should look like in the future.

It also must be noted here that awareness is an ongoing process. In the ever-changing environment of cybersecurity, knowledge must be re-assessed continuously, and competencies have to be renewed and nurtured. Even though others[30] assume that the continuous improvement of staff competencies happens automatically, we strongly advise proactive competence development.

3.1.1 Perception: Awareness of assets

To become aware of the assets at stake for financial institutions, companies have to critically asses their internal infrastructure, applications and data storage systems.

As already elaborated, cybersecurity competencies are always connected directly to specific vulnerabilities. If we regard cybersecurity vulnerabilities as such, they vary depending on the sector: Health companies or hospitals manage highly sensitive data and additionally face the risk of device manipulation. Devices that are connected to the internet can be corrupted: hackers can change the temperature in refrigerators that store blood; change the dosages of drug infusion pumps or prevent defibrillators from giving shocks.[31] [32] Self-driving cars can be hijacked: Hackers can honk, control the

[29] Oltramari et al., “Towards a Human Factors Ontology for Cyber Security”.

[30] Carlton, Levy, and Ramim, “Mitigating Cyber Attacks through the Measurement of Non-IT Professionals’ Cybersecurity Skills”.

[31] Reel and Robertson, “Hospital Gear Could Save Your Life Or Hack Your Identity - Bloomberg Business”.

[32] Zetter, “It’s Insanely Easy to Hack Hospital Equipment | WIRED”.

media system or sometimes even stop the engine[33]. Regarding data breaches in the financial sector, abusers can gain access to extremely sensitive information. Financial institutions manage data that contains information about customers debt or assets, their monthly income and expenses as well as account statements that might lead to more concrete profiles. Customer's whose data is stolen might e.g. face extortion about publishing their finances or the data might be sold directly which is an extremely liquid market with lots of prospective buyers[34].

The theft of customers' balances might even be on a similar level as health records. They are both containing information about a person that cannot be revoked. If a database of user password combinations is stolen, in the first place, no damage has been done if e.g. all user accounts are frozen. While customers might not be able to log in for a certain period until the company sends them new log-in credentials via email, the lost data could be of no direct value to the thief. However, if the stolen data does contain information as described in the paragraph above, it can be replicated and used and there is no way to contain it. Once the attacker knows that Bob does have an allergy to peanuts or a debt of 100.000€ with a bank, this information cannot be captured again. Therefore, the loss of such data is *irreversible* and therefore demands special attention. It seems like health conditions are more sensitive in a way that they are more permanent than financial records and people might perceive them as more personal. However, the structure of personal information in both seems to be similar.

Maybe the most obvious example of loss through a cyber risk is hackers gaining access to personal online-banking services and directly executing remittances. Such an attack could happen e.g. through social engineering, or phishing directed at the customer, but even happen through breaches in the customer databases of financial institutions. Often it could happen as a combination of both, with breached data, hackers can start more elaborated and sophisticated phishing or social engineering attacks.

However, remittances can be reversed in some cases. Therefore, even if maybe counter-intuitive they might present lower costs for a company to level out. The structure of an unauthorised remittance is completely different to the leak of e.g. someone's annual income.

Coming back to the earlier introduced notion of resilience, in the case of unauthorised remittances, it is extremely important to have working recovery mechanisms in place. If these are well defined and

[33] Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED".

[34] Armin, Foti, and Cremonini, "0-Day Vulnerabilities and Cybercrime".

intact, an attack can sometimes even be fully reversed and cause no actual damage (apart from the work that is needed to reverse the wrong remittance). In case of breached information, the loss might not be able to be reversed. Therefore, recovery mechanisms might not be as effective but additional effort should be placed in creating a robust system that cannot be breached as easily. When creating cybersecurity defence mechanisms this distinction should be kept in mind in order to be able to secure the asset at risk in an efficient way.

3.1.2 Comprehension: Threat awareness

The follow common attack schemes that can currently be found in the financial sector: Different forms of Social Engineering attacks, (distributed) denial of service attacks, Advanced social Engineering attacks targeting operators secretaries[35], Attacks on mobile banking for business users[36], attacks on Physical devices connected to the internal network[37], Bypass login by brute force Invalidated redirects and forwards, Bypass login by brute force or DNS login attack, Compromise security via Trojan-malware, Client-server protocol manipulation, Session hijacking[38] [39]. Additionally, we will discuss unconventional attacks such as image and integrity attacks where hackers spread e.g. false information about companies or manipulate external data sets in order to erode public trust. One might argue that there is nothing the company can do about it as other channels are publishing wrong information, but internal full integrity and transparency can be a working countermeasure. We will also point at the current development that hackers seem to focus on the weakest links: Hackers attack small companies in a Supply Chain to gain access to others[40]. The following nine cybersecurity skills have been identified as the most prevalent to be used against the above mentioned threats:

1. Preventing the leaking of confidential digital information to unauthorized individuals
2. Preventing malware via non-secure Websites
3. Preventing personally identifiable information (PII) theft via access to non-secure networks
4. Preventing PII theft via e-mail phishing
5. Preventing malware via e-mail

[35] Namestnikov and Bestuzhev, “Cyberthreats to Financial Institutions 2019: Overview and Predictions”.

[36] Ibid.

[37] Ibid.

[38] Gencer and Atle, “Cyber Risk Patterns”.

[39] Armin, Foti, and Cremonini, “0-Day Vulnerabilities and Cybercrime”.

[40] Namestnikov and Bestuzhev, “Cyberthreats to Financial Institutions 2019: Overview and Predictions”.

6. Preventing information system compromise via USB or storage drive/device exploitations
7. Preventing unauthorized information system access via password exploitations
8. Preventing PII theft via social networks[41]

In addition to external threats, there can also be vulnerabilities that are directly connected to employee behaviour.

3.1.3 Projection: Creating a resilient system.

If a company is aware of its assets and risks, it is enabled to draw out its cybersecurity strategy and steer towards increasing security.

Cybersecurity resilience is lined out as a characteristic of a system. A system can show different qualities such as robustness or recovery. Image a bridge, an object that is notoriously bad at self-recovery. When constructing a bridge, it is normal to design it strong enough that it can withstand two or three times the predicted maximal load[42]. A bridge is an example of a system that is very robust but incapable of recovering. Cybersecurity resilience includes first, the level of actual security in the sense that a system with higher security is harder to be breached. Additionally, resilience covers the ability of a system to recover after a successful attack, meaning the time until the initial security before the breach is reached again. Lastly, a resilient system includes the capability to grow by stress. This means that systems that have been successfully attacked in the past are capable to learn from these attacks in order to not only recover to the same level of security but even increase its overall security. Summing up, in this paper we will consider the ability to recover, to withstand attacks and to learn from attacks[43].

The paragraph above defined the characteristics of a resilient cybersecurity system but what should the system be resilient against? It has to be analysed first what are the assets at stake such as customers credit card information, biometric data, physical hardware, logical software, market information just to name a few.[44] All these different assets might be attacked through different schemes but generally information technology risks are categorised in three main categories: loss of

[41] Carlton, Levy, and Ramim, "Mitigating Cyber Attacks through the Measurement of Non-IT Professionals' Cybersecurity Skills".

[42] Hansson, "Risk".

[43] Carlton, Levy, and Ramim, "Mitigating Cyber Attacks through the Measurement of Non-IT Professionals' Cybersecurity Skills".

[44] Armin, Foti, and Cremonini, "0-Day Vulnerabilities and Cybercrime".

confidentiality, loss of integrity or loss of availability. A loss of confidentiality could be created by a wrongly configured software program where employees have unnecessary reading rights on customers personal data. Confidentiality means that only the right people may see a certain data set. A data set shows integrity if the data cannot maliciously be changed. Availability is reached if an authorised person wants to access i.e. a website and can do so.[45]

This cybersecurity catalogue will not go into depth about risk management principles[46] as it is not concerned about weighing which risks are the most economical to try to avoid. However, such considerations will and should matter in a company's cybersecurity strategy. The presented work can help quantify such avoidance costs and therefore contribute to decision making processes in the cybersecurity landscape. As cyber competencies are always linked to risks, and risks are referring to possible events in the future, it can be quite sophisticated to calculate which risk avoidance measures are appropriate. The goal of this catalogue is therefore to describe a comprehensible list of possible countermeasures which financial institutions can use to pick and choose.

3.2 How can cybersecurity competences be described?

This section will define how specific cyber security competences can look like and which competencies financial institutions should aim to build in their staff. Cybersecurity competencies will differ for different types of employees in the financial sector. Every job profile demands different skills. A solution architect for a payment system in a new Fintech company will need other knowledge than a front-office position or a management assistant. However, we will assume for this version of the deliverable that the human factor in the core competencies will stay the same[47], although the different positions have a different risk exposure. This assumption will be reworked and completed in an iterative process with the results of SOTER deliverable 2.1 ("Mapping of human behaviour related threats and mitigation measures") in order to make sure that the same topics will be addressed throughout the SOTER project.

[45] Ibid.

[46] A possible reference for risk management principles is the ISO 31000

[47] Bowen, Devarajan, and Stolfo, "Measuring the Human Factor of Cyber Security".

In this document, a cybersecurity competence is defined as the ability to perform one's job in a way that averts cyber threats from the employee's financial institution.[48] [49]. The competence is always a link of identifying a threat as well as being able to respond correctly, it incorporates the elements of awareness that were described in the last section[50]. This chapter will lay the groundwork of how cybersecurity competences can be structured. The next chapter will use this method in order to describe predominant cybersecurity competences that can be found throughout literature. It will focus on threats that are directly connected to cybersecurity and not soft competencies such as general competences of entrepreneurial leadership, cooperation or organisation[51]. The following example illustrates how we can describe that an employee (Bob) has a certain competence. We can say that Bob has a cyber competence against phishing if

> *Bob possesses the capability of identifying a phishing attack that is carried out against him. He recognises a suspicious link in an Email that claims to be a link to reset his password, however he remembers that he did not request anything like it. Bob can respond correctly to the phishing attack. He marks the email for his system administrators to check if other employees have received a similar email. Bob's behaviour increases the cybersecurity resilience of his employer. He averts the attack and even helps others by creating awareness for the threat.*

As cybercrime is an ever-evolving field, new threats emerge nearly every day, therefore a catalogue of threats can never be exhaustive which follows the same for the identification of cyber risks[52]. Therefore, an additional challenge is training employees to being able to identify and respond to risks they are not explicitly aware of. The competency to react to unknown risks can be described in the following way. Let us therefore look at Bob's colleague Alice:

---

[48] Carlton, Levy, and Ramim, "Mitigating Cyber Attacks through the Measurement of Non-IT Professionals' Cybersecurity Skills".

[49] Prifti et al., "A Competency Model for 'Industrie 4.0' Employees".

[50] Ibid.

[51] Ibid.

[52] Although there are currently emerging initiatives such as https://www.owasp.org/index.php/Main_Page, an open form platform that e.g. tries to categorise attack angles and also provide open source tools for security checks in software development.

Alice was part of a cybersecurity training where she learned about the risk of social engineering attacks. The trainer mentioned that commonly, social engineering attacks try to manipulate individuals by sending fake invoices that mimic actual suppliers, therefore Alice is extra cautious with double-checking invoices. A year later, Alice receives an email by a market research institute that claims to create an overview for consumers in Alice's industrial sector. The Email just asks for a list of companies that are Alice's customers. Alice remembers the training and even though the inquiry does not directly resemble the social engineering attack she learned about; she suspects malicious intents. She informs her CISO and shares her concern. Later she finds out that the inquiry was part of a new attack scheme that looks for supplier/consumer relation information in order to create new large-scale social engineering attacks. Alice successfully applied her past learnings to a new situation and helped improve the resilience of her company.

The above two examples show how cybersecurity competencies will be approached in this catalogue. They both show an element of awareness – recognizing the phishing or social engineering attack – and expertise – responding in the correct way to avert risk from the company.

The next table proposes a framework how cybersecurity competencies can be described in a reduced and dense overview. The column "risk" contains the name of the cybersecurity risk. "Description" is describing the attack scheme of said risk. The "Awareness factor" describes how employees can be made aware of the risk and "expertise" describes how employees should respond if they become a target of the said risk.

Table 2, Cybersecurity Competences

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
PII theft via e-mail phishing	Phishing attack	Attackers try to "phish" for sensitive data like passwords by re-creating fake E-mails. These E-mails often look and sound increasingly credible and ask recipients to insert e.g. their log-in credentials on fake websites where they will be tapped.	Training through simulation. IT department may create their own fake phishing E-mails that can be sent to the staff for training purposes.	The user may not follow any links in fake E-mails and should make aware the IT department of her company in order to create the ability to recognise phishing attempts by checking certain parameter fields in emails such as the sender, use of specific nomenclature,

				recognition of viable authentication and secure channels and links.
Leak of confidential digital information to unauthorized individuals	Social engineering attack	Attackers try to manipulate employees in phone calls or E-mails by spreading the sense that they have some sort of connection with the company. Common variants are the impersonation of suppliers or business partners. After targets are persuaded, attackers will try to trigger invoices or the distribution of sensitive data.	Employees should be aware that there might be more information available on the internet (e.g. in message boards, social media or even through data leaks) than they assume. By using such information, attackers can create a sense of affiliation or authority.	Employees should try to steer the conversation in order to find out if the counterpart is who he pretends to be. Social engineering attackers commonly try to steer conversations which should be fought against. Simple questions about proof of e.g. company affiliation might already help to bust attackers.

This paper defines important cybersecurity competencies; however, the definition of such competencies cannot suddenly improve the cyber resilience[53] of financial institutions. Competencies must be built up through various trainings. Therefore, this catalogue tries to provide a sounds basis on which trainings can be developed. Every competence will be described in the form of a story and tabularly in order to be a solid base for companies' staff trainings. It will present a coherent framework.

3.3 Cybersecurity Culture

An institution cannot simply force employees to behave in a cyber-secure way. Therefore, a more holistic change of perspective is needed. The needed employee behaviour has to be adapted in every aspect of the working life; it must influence the working culture[54]. ENISA published a report how such a cybersecurity culture could look like with the following main pillars:

[53] Resilience is understood in a way that describes a system's capability to withstand external pressure and also regenerate in case of threat manifestation.

[54] Antonucci and Durbin, "Identifying, Analyzing, and Evaluating Cyber Risks".

> *"• Stay relevant – both with regard to new threats, as well as employee and organisational changes. All necessary knowledge for different staff should be encompassed, along with management's vision for roles and responsibilities.*
>
> *• Plan for natural learning– sufficient time should be set aside for training. The programme should positively influence the knowledge, the attitude and the behaviour of participants.*
>
> *• Involve the entire organisation – open communication and awareness throughout the organisation allows for internal consistency and feedback for improvements.*
>
> *• Share the enthusiasm - a creative, varied and tailored education programme may achieve more. Methods depend on the organisation's wishes and budget but may include one or more of games, stories, films and case studies, workshops and crisis exercises."* [55]

ENISA claims that these cornerstones need to be fulfilled to create a sustainable and resilient culture that helps to lower cybersecurity threats. However, ENISA builds on the following assumption.

> *"To convince people to change, three parallel processes must take place: (1) there must be dissatisfaction with the current situation; (2) this dissatisfaction must cause anxiety and/or guilt; and (3) employees must be able to adopt new behaviour in a safe environment without compromising their identity or integrity. To "unfreeze" the existing culture, its shortcomings must be identified and communicated, after which the new culture can be instilled by changing knowledge and behaviour"*[56]

Surely, dissatisfaction can be a strong catalyst for innovation and evolution, however it does not seem to be a necessary condition. The same is true for (2) and (3). ENISA describes one way how cultural changes might occur but misses to explain why other approaches to change a company's culture cannot succeed. It seems to be quite unlikely that every change in company culture was based on reaching a specific negative tipping point that caused a considerable amount of guilt or anxiety. Cultural change can also happen in a step-by-step manner[57]. This competence catalogue follows the idea that cultural changes can happen in an active and not only reactive way. Consequently, it tries to

[55] Juanito, "Cyber Security Culture in Organisations".

[56] Ibid.

[57] S. Cameron and E. Quinn, *Diagnosing Changing Organization Culture Based on the Competing Values Framework [PDF File]*.

complement a company's cybersecurity culture strategy by providing a basis for trainings and using illustrative examples or stories to easily describe complex circumstances.

Moreover, one might argue that as ENISA describes that dissatisfaction and subsequent guilt or anxiety seem to be effective catalysts to change, following that trainings could try to artificially recreate such a situation. We strongly advise here that training through threat should not be endorsed for a healthy company climate. Even if a rise in cyber resilience could be achieved in such a way, there surely would be a considerable downside in employee satisfaction levels.

A company's cybersecurity strategy should therefore encompass the strengthening of cyber security competencies and the creation of a cybersecurity culture. By doing so, they can mitigate the threat of costly data breaches and hacks and improve public trust.

4. Cybersecurity Competence Catalogue

The following chapter currently represents an early draft of the cybersecurity competencies that will be discussed during the duration of the SOTER project. Task 2.1 of the SOTER project is concerned with identifying and recognising vulnerabilities and threats that are directly connected to human factors in cyber-security. As soon as first findings of this research are available, the cybersecurity competence catalogue will be updated and aligned accordingly. Hence, the following paragraphs are an agnostic first outlook on how cybersecurity competencies will look like in the future. Once more vulnerabilities are identified, more competencies will be added.

This chapter will discuss different important cybersecurity competencies and describe them in a way so they can be used for trainings. Cybersecurity competencies will contain an element of awareness and expertise, as mentioned before. Awareness will be looked at from a very specific angle: Awareness regarding specific cybersecurity risks that financial institutions face. The described expertise are the needed skills to tackle the relating threats[58].

Preventing the leaking of confidential digital information to unauthorized individuals

Alice was part of a cybersecurity training where she learned about the risk of social engineering attacks. The trainer mentioned that commonly, social engineering attacks try to manipulate individuals by sending fake invoices that mimic actual suppliers, therefore Alice is extra cautious with double-

[58] Coppolino et al., "How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project".

checking invoices. A year later, Alice receives an email by a market research institute that claims to create an overview for consumers in Alice's industrial sector. The Email just asks for a list of companies that are Alice's customers. Alice remembers the training and even though the inquiry does not directly resemble the social engineering attack she learned about; she suspects malicious intents. She informs her CISO and shares her concern. Later she finds out that the inquiry was part of a new attack scheme that looks for supplier/consumer relation information in order to create new large-scale social engineering attacks. Alice successfully applied her past learnings to a new situation and helped improve the resilience of her company.

Table 3, Competence example: Social engineering

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
Leak of confidential digital information to unauthorized individuals	Social engineering attack	Attackers try to manipulate employees in phone calls or E-mails by spreading the sense that they have some sort of connection with the company. Common variants are the impersonation of suppliers or business partners. After targets are persuaded, attackers will try to trigger invoices or the distribution of sensitive data.	Employees should be aware that there might be more information available on the internet (e.g. in message boards, social media or even through data leaks) then they assume. By using such information, attackers can create a sense of affiliation or authority.	Employees should try to steer the conversation in order to find out if the counterpart is who he pretends to be. Social engineering attackers commonly try to steer conversations which should be fought against. Simple questions about proof of e.g. company affiliation might already help to bust attackers.

Preventing malware via non-secure Websites or software

Bob is browsing the internet for a solution that helps him track his currently open tasks. Bob stumbles upon a website that offers a free software that claims to provide a pinboard-like feature where users can digitally save notes and directly link them to their calendar. The software is also available for Bob's phone. Bob reads the description of the software and is pleased by the advertisement. He remembers that he was asked in a training to refrain from installing third party software on his work phone without checking with the IT department first. Therefore, Bob sends an Email to his IT colleagues with the request to check if he can use the application. The IT department researches for a bit and finds out that the app contains a malicious feature that collects all information that is stored in it by users. The IT department suspects malicious intends behind this feature and asks Bob not to use the software. Bob

is happy that he asked his colleagues before he started using the application and avoided the stealing of his notes.

Table 4, Competence example: Malware

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
Malware via non-secure Websites or software	Becoming a victim of malware through accessing a non-secure website.	Malware can be applications that run on websites or downloadable applications that harms users. Hackers abuse open redirects or log-in files to plant malicious content. Users should be aware of the files they download and install as well as of the websites they access. If search engines or their IT department issues a warning against accessing a specific website it should always be followed.	Simulating what malware can do. Malware can e.g. be an executable file that affects browser settings in a way that private information and passwords are collected and leaked.	Users should be aware of the dangers of downloading and executing flies from unknown websites. Users should refrain from accessing websites that they were warned about. Users should not download and execute files from unknown sources without asking their IT department's assessment.

Preventing personally identifiable information (PII) theft via access to non-secure networks

Alice is on a work trip and wants to access her e-mails from her hotel room at the BusinessHotel this evening. She opens her laptop and tries to connect to a nearby Wi-Fi. She sees that three networks are nearby: Two secure networks, called "Hotel_WiFi" and "BusinessHotelWifi" and one public network under the name "FREE_WIFI_FOR_ALL". Alice remembers that public networks should not be used, especially when accessing her work emails. She wonders which of the secure networks is indeed the official hotel Wi-Fi- network and therefore can be trusted. She quickly calls the reception and asks the person at the desk who informs her that "BusinessHotelWifi" is their official network. Alice connects to "BusinessHotelWifi" and accesses her e-mails.

Table 5, Competence example: PII theft

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
PII theft via access to non-secure networks	Using a honeypot Wi-Fi	Attackers try to create honeypot Wi-Fi networks that intercept log-in credentials or data in general. All data that is sent without encryption on a public spoof Wi-Fi, such as E-Mails or instant messages might be accessed by hackers. Log-in credentials that are transmitted via insecure protocols might be collected.	Recognizing the dangers of public Wi-Fi networks as well as seemingly secure spoof networks.	The user will not connect to possibly malicious public Wi-Fi networks and take measures to make sure that seemingly secure networks are indeed trustworthy.

Preventing PII theft via e-mail phishing

Bob possesses the capability of identifying a phishing attack that is carried out against him. He recognises a suspicious link in an Email that claims to be a link to reset his password, however he remembers that he did not request anything like it. Bob can respond correctly to the phishing attack. He marks the email for his system administrators to check if other employees have received a similar email. Bob's behaviour increases the cybersecurity resilience of his employer. He averts the attack and even helps others by creating awareness for the threat.

Table 6, Competence example: Phishing

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
Leak of confidential digital information to unauthorized individuals	Phishing attack	Attackers try to "phish" for sensitive data like passwords by re-creating fake E-mails. These E-mails often look and sound increasingly credible and ask recipients to insert e.g. their log-in credentials on fake websites where they will be tapped.	Training through simulation. IT department may create their own fake phishing E-mails that can be sent to the staff for training purposes.	The user may not follow any links in fake E-mails and should make aware the IT department of her company in order to create awareness of the attack in case other employees might be affected.

Preventing malware via e-mail

Alice works in accounting and receives an e-mail by a company that offers a product which claims to support the management account of small companies. The e-mail says that in an attached .zip file the recipient can find more information about the offer and the product. Alice regards the offer and thinks it might be interesting for her company but is aware that an attached .zip file might be dangerous to open. She decides to quickly call the company to check whether the offer is legitimate. Alice calls the number that is mentioned in the e-mails and receives an out-of-service notice. Alice realises that the offer probably is fake and notifies her IT department about the e-mail. The IT department researches a bit and finds out the e-mail is indeed malicious, and the e-mail attachment contained a virus.

Table 7, Competence example: malicious attachment

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
Malware via e-mail	Becoming a victim of malware by opening a malicious attachment from an email.	Attackers try to send emails with malicious attachments that, once opened, infect machine or even the network of the user. Through the technological progress, anti-virus software malware attacks via e-mail have been declining rapidly.	Being aware of the dangers malware that is sent via e-mails. Executable files can contain viruses, trojan applications or ransomware. Most malware attacks via e-mail use executable file formats such as .exe, .html or .zip.	If possible, users should try to double-check if the received file is malicious. This can be as easy as calling the sender. Additionally, the warning of anti-virus software should be followed and in any suspicious case, IT departments should be consulted who can open files in contained environments.

Preventing information system compromise via USB or storage drive/device exploitations

Bob went to a conference on automotive design last week to expand his network among other automotive designers. In an after-conference event he meets a gentleman that is claiming to be a vivid student of Bob's work. He continues to talk about his admiration for Bob and asks him if he can give him some of his own blueprints and if Bob can have a look at them. Bob feels flattered and agrees, thereafter the admirer hands over an USB stick. The week, back in the office, Bob remembers the USB stick and thinks about having a look at the blueprints. He remembers a past training, where he was told that USB sticks might contain malicious software and harm his company. Therefore, Bob decides

to ask his IT department to check the USB stick first. The IT department does indeed find malicious code on the USB stick and Bob feels ashamed that he has fallen for a flattering pretender but is happy that he remembered to be cautious enough to prevent anything worse from happening.

Table 8, Competence example: Malware (external device)

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
Information system compromise via USB or storage drive/device exploitations	Becoming a victim of malware by using a USB stick.	USB sticks might contain malicious code that, once plugged into a system, infect the machine or a whole network.	Being aware of the dangers of using USB sticks received from third parties.	The user may not use any USB stick that was received from an unknown source without consulting his IT department first, to check the content of the USB stick.

Preventing unauthorized information system access via password exploitations

Alice wakes up on a Saturday morning and checks the news. One of the headlines is a new data breach in a social network Alice often users. The article claims that even username and password combinations have been stolen. Alice is shocked and quickly takes steps to recover her social network account and then starts to think if there could be any other consequences through the leak. Luckily, last week she has been in an IT Security training where she learned the importance of strong passwords. The training mentioned that not only do passwords have to be strong individually, users should also avoid using the same password for different services. This information was new for Alice who until then used the same – very strong – password for all websites and applications, even for her work accounts. Right after the training she decided to change all her passwords. By doing so she dodged that the password that was stolen from her social media account could be used by hackers to gain access to Alice's profiles for other websites and even her work accounts.

Table 9, Competence example: Password theft

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
Unauthorized information system access via password exploitations	Cracking or theft of passwords	User passwords might either be stolen e.g. from the databases of old websites or services that use weak	Users should be aware of the dangers of using the same passwords for multiple websites	Users will choose passwords that are strong against brute force attacks and

		encryption techniques and security. If users use the same passwords for multiple services, attackers can get access to critical systems. Additionally, weak passwords can be guessed by brute force attacks. Brute force attacks become more dominant with a rise in computation power and are especially efficient against short and weak passwords.	or services. Users should know what makes a password strong and secure, namely length, use of numbers, symbols, capital letters and refraining from encyclopaedic components.	guessing. Users will not use the same password for multiple services.

Preventing PII (Personal identifying information) - theft via social networks

Bob is feeling exhausted after a long day at work and really looking forward to his boss taking his short vacation next week so that Bob can start out slower for a few days. After work he takes a selfie and wants to upload it to Instagram with the caption "That's the face looking forward to your vacation on the Bahamas, boss!" Just before sending the message he remembers a training he had, were the trainer told a story about an enterprise being afflicted by a severe case of CEO-Fraud, because public information about the CEO being on vacation was exploited by criminals. Besides, maybe his boss wouldn't find his post funny neither, if he read it. He decides that the post might not be a good idea after all and closes the application.

Table 10, Competence example: Social engineering attack

Threat and Asset at risk	Risk	Description	Awareness factor	Expertise
PII theft via social networks	Social engineering attacks	Attackers try to befriend victims on social networks in order to steal PII. By gathering information about victims, attackers can collect important information that can later be used maliciously. Many services use security questions such as "Name of a pet?". Answers to such	Users should be aware about the dangers of posting certain information on social media. Information that can be used to impersonate the user should not be publicly available for attackers.	Users shall not publish any restricted information that could lead to successful impersonation on social networks. The same is true for sensitive information about their workspace.

		questions can be deducted through information available on social media.		

5. How to improve cybersecurity competences

How can financial institutions build up cybersecurity competences? How can a company decrease the risk of human errors among its employees? How can the previously described competences be promoted in a sustainable and long-lasting way? The past chapter described what an employee should strive to achieve in terms of cyber security competences. After the goal is set, it is equally important to sufficiently describe *how* it can be achieved. How cybersecurity competences can be strengthened specifically will be addressed in a different deliverable of the SOTER project, namely D6.3 "Training modules compilation". The training modules will encompass the story-telling fashion of the above-mentioned cybersecurity competences and will promote the ability to perceive, comprehend and project.

Additionally, the competence pattern can function as a benchmark to track meaningful cybersecurity KPI's. Companies can track the success of training actions and i.e. measure the improvement of threat awareness by implementation routine awareness tests.

6. Thought experiment: Employee liability

This chapter is a placeholder for the possible inclusion of a thought experiment on a liability between employees and employers. The idea is to draw out how a company structure could look like where employees possess full liability of their actions. Decentralized yet private applications in companies that provide full transparency on user behavior could lead to a shift of responsibility towards employees. A decentralization of companies could lead to more robust systems without a central single point of failure and shift responsibility and involvement closer to employees. The thought experiment is not intending to promote a new form of company but simply an exercise to explore different ways of organization and how they relate to cybersecurity.

7. References

Antonucci, Domenic, and Steve Durbin, "Identifying, Analyzing, and Evaluating Cyber Risks", *The Cyber Risk Handbook*, No. 2017, 2017, pp. 97–107.

Armin, Jart, Paolo Foti, and Marco Cremonini, "0-Day Vulnerabilities and Cybercrime", *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, 2015, pp. 711–718.

Baydakova, Ana, "Telegram Finally Confirms It's Behind TON Blockchain", *Coindesk*, 2019. https://www.coindesk.com/telegram-finally-confirms-its-behind-ton-blockchain.

Bowen, Brian M., Ramaswamy Devarajan, and Salvatore Stolfo, "Measuring the Human Factor of Cyber Security", *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, No. June, 2011, pp. 230–235.

Carlton, Melissa, Yair Levy, and Michelle Ramim, "Mitigating Cyber Attacks through the Measurement of Non-IT Professionals' Cybersecurity Skills", *Information and Computer Security*, Vol. 27, No. 1, 2019, pp. 101–121.

CISA U.S. Department of Homeland Scurity, "Apache Software Foundation Projects", *Apache Software Foundation Releases Security Updates*, 2017. https://apache.org/index.html#projects-list.

Collier, Kevin, "Alleged Hacker May Have Hit Other Targets - CNN", *CNN*, 2019. https://edition.cnn.com/2019/07/30/business/hack-targets-capital-one-hacker/index.html.

Coppolino, Luigi, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano, and Luigi Sgaglione, "How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project", *Proceedings - 32nd IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2018*, Vol. 2018-Janua, 2018, pp. 573–578.

Doffman, Zak, "1.5m Users Hit By New Facebook Privacy Breach As Extent Of Data Misuse Exposed", *Forbes*, 2019. https://www.forbes.com/sites/zakdoffman/2019/04/18/facebook-illegally-harvested-data-from-1-5m-users-as-it-leveraged-its-data-machine/#69edf97c6a2e.

European Commission, "The EU Cybersecurity Act", 2019. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

European Union, “Charter of Fundamental Rights of the European Union (2000)”, *Official Journal of the European Union*, 2012, pp. 391–407.

Gencer, Erdogan, and Refsdal Atle, “Cyber Risk Patterns”, Vol. 2016, No. 653321, 2016.

Greenberg, Andy, “Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED”, *Wired.Com*, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Hansson, Sven Ove, “Risk”, *The Standford Encyclopedia of Philosophy*, Edward N. Zalta, 2018. https://plato.stanford.edu/archives/fall2018/entries/risk/.

Juanito, Pandia Mamani, “Cyber Security Culture in Organisations”, *Anasthesiologie Und Intensivmedizin*, No. 6, 2018, pp. 1–193. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=emed10&NEWS=N&AN=40852808.

Kumar, Mohit, “UniCredit Bank Suffers ‘Data Incident’ Exposing 3 Million Italian Customer Records”, *The Hacker News*, 2019. https://thehackernews.com/2019/10/unicredit-bank-data-breach.html.

Namestnikov, Yury, and Dmitry Bestuzhev, “Cyberthreats to Financial Institutions 2019: Overview and Predictions”, *AO Kaspersky Lab.*, 2018. https://securelist.com/ksb-cyberthreats-to-financial-institutions-2019-overview-and-predictions/88944/.

NG, Alfred, “How the Equifax Hack Happened, and What Still Needs to Be Done - CNET”, *Cnet*, 2018. https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

Nystrom, Mason, “Demystifying the Facebook Libra Congress Hearings”, *Medium*, 2019. https://medium.com/swlh/demystifying-the-facebook-libra-senate-hearing-50d36a421e62.

Oltramari, Alessandro, Diane Henshel, Mariana Cains, and Blaine Hoffman, “Towards a Human Factors Ontology for Cyber Security”, *CEUR Workshop Proceedings*, Vol. 1523, 2015, pp. 26–33.

Partida, Alberto;, and Diego Andina, *IT Security Management : IT Securiteers - Setting up an IT Security Function*, Dordrecht : Springer Science+Business Media B.V., 2010.

Ponemon, “Separating the Truths from the Myths in Cybersecurity - Independently Conducted by Ponemon Institute LLC”, No. June, 2018. https://www.bmc.com/content/dam/bmc/collateral/third-party/Ponemon%2BReport.pdf.

Prifti, Loina, Marlene Knigge, Harald Kienegger, and Helmut Krcmar, "A Competency Model for 'Industrie 4.0' Employees", *Wirtschaftsinformatik*, 2017, pp. 46–60. https://www.wi2017.ch/images/wi2017-0262.pdf.

Reel, Monte, and Jordan Robertson, "Hospital Gear Could Save Your Life Or Hack Your Identity - Bloomberg Business", *Bloomberg Businessweek*, 2015. https://www.bloomberg.com/features/2015-hospital-hack/.

S. Cameron, Kim, and Robert E. Quinn, *Diagnosing Changing Organization Culture Based on the Competing Values Framework [PDF File]*, 2006.

Sandler, Rachel, "Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested", *Forbes*, 2019. https://www.forbes.com/sites/rachelsandler/2019/07/29/capital-one-says-hacker-breached-accounts-of-100-million-people-ex-amazon-employee-arrested/#1dd106641d20.

Zetter, Kim, "It's Insanely Easy to Hack Hospital Equipment | WIRED", *Wired*, 2014. http://www.wired.com/2014/04/hospital-equipment-vulnerable/.