Cybersecurity Optimization and Training for Enhanced Resilience in Finance

D6.3 – Training Modules Compilation (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	Eva-Maria Griesbacher, Uni Graz
	eva.griesbacher@uni-graz.at
Other Contributors	Martin Griesbacher, RISE
	Paul Rabel, Uni Graz
	Robin Renwick, TRI (Review)

Due Date	28.02.2020/31.03.2020 (after amendment)
Delivery Date	31.03.2020
Type	Report
Dissemination level	PU = Public

Keywords	Competence Training, Cybersecurity, Finance, Training Methodology, Training Modules

Document History

Version	Date	Description	Reason for Change	Distribution
V1.0	07.01.2020	Outline	External Review (TRI)	14.01.2020
V1.1	15.01.2020	Draft V1	Local Document	02.03.2020
V1.2	03.03.2020	Draft V2	SharePoint Document	20.03.2020
V1.3	23.03.2020	Draft V3	Internal Review 1	23.03.2020
V1.4	24.03.2020	Review Version	Internal Review 2	24.03.2020
V1.5	25.03.2020	Reviewed Version	External Review (TRI)	25.03.2020
V1.6	26.03.2020	Final Review V.	Internal Review 3	26.03.2020
V1.7	26.03.2020	Final Version	External Review (TRI)	31.03.2020

Abstract

D6.3 presents the state of the art of cybersecurity training within the finance sector, based on a comprehensive literature review of current scientific knowledge on organisational cybersecurity training. For this purpose, cybersecurity trainings conducted in finance and adjacent sectors that focused on assessment, awareness building and gamification, were analysed. Secondly, the paper extends to the analysis of cybersecurity trainings performed in other sectors. Here, an overview of the broader field of Security Education, Training and Awareness (SETA) approaches is provided. Furthermore, cybersecurity training approaches that focus on competence or skill development and gamification are discussed. Concluding the paper, lessons learned from all these previous cybersecurity training approaches are presented that will be crucial for the development of the SOTER training modules in D6.4. Trainings in cybersecurity for employees should thus focus on implementing a multi-channelled training regime, customizing trainings to organisations and to groups of comparable individuals, promoting problem-oriented solution behaviour, building up motivation to learn and to perform learned skills and knowledge in trainings, integrating management in training actions and building up cyclic evaluation and assessment mechanisms.

2 Table of contents

Executive summary

D6.3 presents the state of the art of cybersecurity training within the finance sector, based on a comprehensive literature review of current scientific knowledge on organisational cybersecurity training.

Based on a multifaceted understanding of cybersecurity and on the Central-European definition of competence, cybersecurity competence is defined as the capability, willingness/motivation and agency of persons to solve cybersecurity problems individually or in cooperation with others based on their ability to recognize cybersecurity incidents and to react accordingly based on their knowledge, skills and proficiency in a way that the organisational integrity (technical, social, legal, ethical) and the physical, mental, material, social, ethical and legal integrity of the individuals involved is safeguarded. According to the proposed definition of cybersecurity competence, cybersecurity competence training needs to address every single point of this definition, with the idea of multifaceted integrity (physical, mental, material, social, ethical and legal integrity) as its overarching principle. For this purpose, we developed a Cyber Security Competence Training (CSCT)-Framework applicable for organisations.

To be applicable to the finance sector, this framework must be customized. Therefore, previously conducted cybersecurity trainings in the finance sector – or comparable interventions –are reviewed in this deliverable. Since cybersecurity trainings conducted in sectors other than finance may provide valuable insight as well, another section is devoted to a brief analysis of these interventions. Within the third section of the deliverable, the focus is on addressing the lessons learned from training actions in finance and other sectors. To attain an overview of the cybersecurity training landscape for employees in the finance sector and beyond, an interdisciplinary literature review was conducted.

Concluding the paper, lessons learned from all these previous cybersecurity training approaches are presented that will be crucial for the development of the SOTER training modules in D6.4. Trainings in cybersecurity for employees should thus focus on implementing a multi-channelled training regime, customizing trainings to organisation and groups of comparable individuals, promoting problem-oriented solution behaviour, building up motivation to learn and to perform learned skills and knowledge in trainings, integrating management in training actions and building up cyclic evaluation and assessment mechanisms.

List of figures

List of tables

List of acronyms/abbreviations

Abbreviation	Explanation
CDA	Cybersecurity Competence Development and Assessment Framework
CDX	Cybersecurity Defence Exercise
CSCT	Cyber Security Competence Training
CSI	Cybersecurity Skills Index
GDPR	General Data Protection Regulation
HAIS-Q	Human Aspects of Information Security Questionnaire
HRM	Human Resource Management
ICT	Information and Communication Technology
ICS	Information and Communication Systems
IF	Interactive, First-person
IoT	Internet of Things
IS	Information Security
ISC	Information Security Compliance
ISCA	Information Security Culture Assessment
ISP	Information Security Policy
IT	Information Technology
LMS	Learning Management System
NIS	Network and Information Systems
OSN	Online Social Networks
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PMT	Protection Motivation Theory
RM	Resource Management
SBT	Social Bond Theory

SCPT	Situational Crime Prevention Theory
SETA	Security Education, Training and Awareness
SOTER	cyberSecurity Optimization and Training for Enhanced Resilience in finance
TTAT	Technology Threat Avoidance Theory

Table 1 List of acronyms/abbreviations

1 Cybersecurity Training in Finance – Introduction

The goal of work package 6 is to enhance cybersecurity competences of employees in the finance sector through a set of training activities. For this purpose, training modules based on the competence catalogue drafted in D6.1 and D6.2. (general and platform specific competences) will be created. D6.3 presents the state of the art of cybersecurity trainings in the finance sector, informed by the broader field of organisational cybersecurity trainings. It also gives an overview of training requirements in the finance sector based on an analysis of sector-specific cybersecurity frameworks and regulations. D6.4 will then expand on D6.3, setting the theoretical and methodological framework for cybersecurity trainings in the finance sector. Following the structure of the competence catalogue, D6.4 will then focus on the training of general cybersecurity competencies needed in the finance sector as well as the SOTER-platform-specific training modules.

1.1 Definitions

1.1.1 Competence

For the training modules, the continental-European definition of *competence* in Empirical Educational Research and Personnel Development has been adopted, since it is interdisciplinary and covers nearly all aspects we deem necessary for effective training actions. Within this context, competence is defined as the general capability of individuals to act and solve problems independently in a given situation based on their abilities, knowledge, skills, proficiency and personality (Müller-Frommeyer 2017, 308; Arnold et al. 2010, 173; Kaufhold 2006, 21-25). While many definitions in Empirical Educational Research attribute the realization of competence merely to the individual (Kurtz 2010, 8), we want to add a genuine social 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 (ibid.). Individuals not only need the capability to act competent, they also need agency to do so (Pfadenhauer 2010). But not just that: they must be motivated to perform their competences in a given situation, too (ibid.). In consideration of these additional aspects of the realization of competences, competence is hereafter defined as the general capability, willingness/motivation and agency of a person to act and solve problems independently or in cooperation with others in a given situation based on their abilities, knowledge, skills, proficiency and personality.

1.1.2 Cybersecurity

As Schatz et al. discussed in their article in 2017, Cybersecurity has become a frequently used, but ill-defined term over the past decade (Schatz et al. 2017, 53), increasingly replacing common terms like “Computer Security”, “IT Security” and “Information Security” (ibid., 54). Based on a semantic analysis of a wide scope of existing definitions in industry, government and academia, Schatz et al. propose the following definition: Cybersecurity comprises “the approach and actions associated with *security risk management processes* followed by organisations and states to protect confidentiality, integrity and availability of *data* and *assets* used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its *users*." (Schatz et al. 2017, 64, emphasis added).

So, the main concern of cybersecurity is the integrity, security, and control of digital assets and their associated access rules. But it must be emphasized that corresponding losses of integrity caused by security incidents can be the cause of further damages to an organisations' integrity (e.g. undue loss of financial or reputational assets). Due to the continually increasing regulation in the digital domain (e.g. GDPR, NIS directive) and the growing issue of online disinformation (see Martens et al. 2018) cyber risks also concern the ethical/reputational and legal layer of an organisation. To prevent losses of integrity, cybersecurity therefore must be addressed on different organisational layers (technical, social, legal & ethical).

For a systematic approach on vulnerabilities it is useful to consider the interfaces of an organisation to its digital assets. Ganin et al. (2017) identify three main domains, the physical (hardware), information (software) and social (personnel) domain. Most of the vulnerabilities associated with the information domain have to be covered by specialized IT security personnel, and are therefore not in the focus of the cybersecurity trainings in SOTER (the only exemption are basic insights into technology-based attacks as a question of cybersecurity awareness). We focus here on vulnerabilities associated with human factor-based cybersecurity issues. This implies, that the vulnerability is at least to a certain extend directly connected to human behaviour. For the case of incidents in the physical domain this could mean an employee giving an intruder access to hardware or in the information domain using IT with insufficient technical security settings. But the main concern here are vulnerabilities directly located in the social domain. This, for example, includes most prominently social engineering attacks but also negligent or malevolent behaviour within an organisation. All domains must be secured with targeted security measures. Loss of Integrity within one layer might bypass security measures on other layers (e.g. strong encryption as technical measure bypassed by via social engineering attacks stolen passwords, or decryption keys, from employees).

Additionally, it should be considered that many incidents (esp. those based on criminal/malevolent intent) have a multi-stage structure. For example, a successful social engineering attack opens the door to data theft which is used to gain financial resources through cyber fraud. In such cases, it is useful to start securing the first link in the chain of events to prevent loss of integrity. In more and more situations, this first link is in the social domain – especially since the technical security in the finance sector is continually improving. Finally, we need to extend the understanding of cybersecurity in the context of European values and norms (esp. regarding fundamental rights). As many incidents not only concern the integrity of an organisation, cybersecurity should also target to protect the integrity of any individual involved in an incident (e.g. in the case of theft of customer data). Accordingly, we can define security as a situational attribute, where the probability of damage to the physical, mental, material, social, ethical and legal integrity of all involved individuals is as low as possible. Keeping this extended understanding in mind, organisations can define cybersecurity as the task to create an overall trustworthy digital environment.

1.1.3 Cybersecurity Competence

Bringing the aforementioned definitions of Competence and Cybersecurity together, Cybersecurity competence is the capability, willingness/motivation and agency of persons to solve cybersecurity problems individually or in cooperation with others based on their ability to recognize cybersecurity incidents and to react accordingly based on their knowledge, skills and proficiency in a way that the organisational integrity (technical, social, legal, ethical) and the physical, mental, material, social, ethical and legal integrity of the individuals involved is safeguarded.

1.2 Basic Cyber Security Competence Training Framework

According to the proposed definition of cybersecurity competence, cybersecurity competence trainings must address every single point of this definition (see Figure 1) – with the idea of multifaceted integrity (physical, mental, material, social, ethical and legal integrity) as its overarching principle. For this purpose, we developed a Cyber Security Competence Training (CSCT)-Framework applicable for organisations.

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. In this context, the knowledge base as well as what is considered appropriate behaviour should be guided by the idea of multifaceted integrity. Building on that knowledge, the corresponding job-function-oriented skills must be acquired and practiced until employees reach proficiency in performing these skills. This learning process should be accompanied by personality development to increase employees' feeling of self-efficacy and to enable them to work as a team when critical cybersecurity situations occur. Through this process, employees are enabled to acquire a fundamental situational capability to tackle critical cybersecurity situations, while safeguarding the integrity of all entities involved.

Since having the situational capability to do something does not necessarily imply that this capability is in fact realized, cybersecurity competence trainings must also motivate and empower employees. Within the SOTER trainings, storytelling and gamification methods will be used to ensure a high degree of motivation, but also to approximate the learning experience to real-world situations as close as possible. Because of these trainings, employees should experience growing levels of proficiency in tackling critical cybersecurity situations in a context that enables high levels of individual agency. Game contexts usually are such contexts. Due to the close connection of games to real-world situations, employees may make use of their sense of empowerment and motivation in their jobs.

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 competencies.

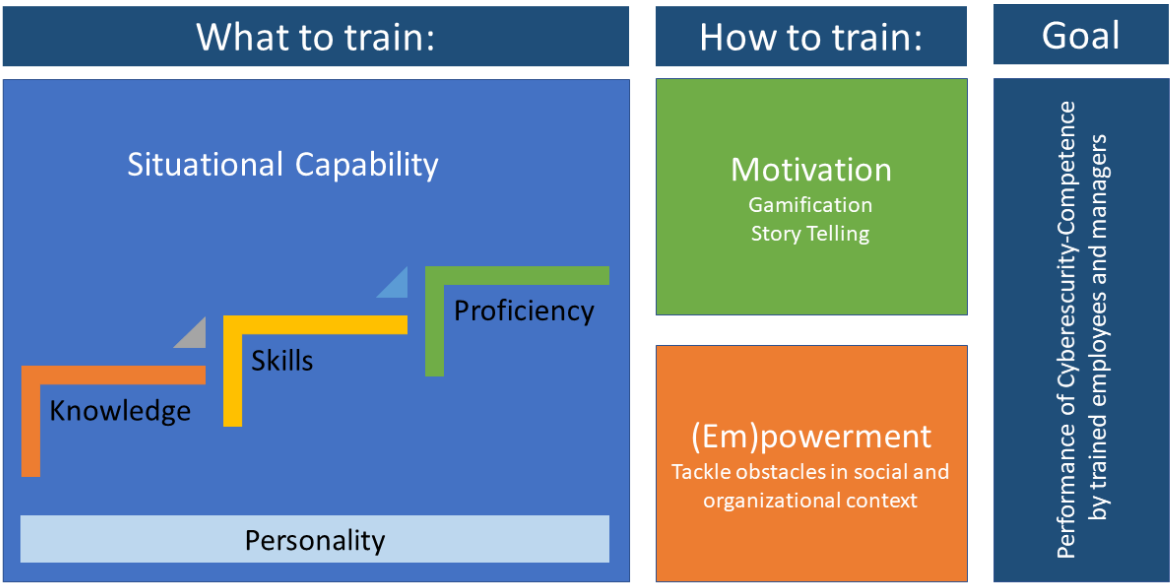


Figure 1: Competence Training Framework

Note that the prior section about the presented Cybersecurity Competence Training (CSCT) Framework constitutes merely a rough outline of the training and method. To be applicable to the finance sector, this framework must be customized. Therefore, in the following section previously conducted cybersecurity trainings in the finance sector – or comparable interventions – will be reviewed in more detail. Since cybersecurity trainings conducted in sectors other than finance may provide valuable insight as well, another section will be devoted to a brief analysis of these interventions. Within the third section of the deliverable, the focus will be on addressing the lessons learned from training actions in finance and other sectors, which will inform the development of the training modules in D6.4.

To attain an overview of the cybersecurity training landscape for employees in the finance sector and beyond, an interdisciplinary literature review was conducted. To ensure a comprehensive sample containing as many relevant sources as possible, a keyword catalogue comprising all relevant terms was deployed and forward as well as backward reference checking was performed. The review covers literature from information security, information systems security and human resources research that is concerned with the question of cybersecurity training for employees in the finance sector. Because of the limited results for the search terms bank* and financ*, the search was extended to other sectors, too. The literature search provided 65 articles for analysis, eight of those focusing on the finance sector.

The articles were analysed according to the following questions:

- What is or should be trained?
- Which methods are used to deliver the trainings?
- Which techniques are used in these methods to shape the behaviour of the employees?
- What determined the effectiveness of the performed cybersecurity trainings?

2 Previous Cyber Security Training Approaches in Banks

Cybersecurity Trainings in banks were primarily focusing on information security awareness, information security policy compliance, and information security behaviour. The most academically renowned training framework in the finance sector is the implementation of trainings and interventions based on Information Security Culture Assessment (ISCA), created by Adéle da Veiga and Jan H. P. Eloff (2010). ISCA was initially defined as an instrument to assess, cultivate and monitor information security culture in organisations. The aim of the instrument is to establish the level of information security culture in the [analysed] organisation, to identify necessary improvements and to benchmark the data from one assessment to the next to monitor changes and identify trends in its information security culture (da Veiga/Martins 2015, 165). Firstly, ISCA assesses whether the level of information security culture in the analysed institution is "adequate to protect the confidentiality, integrity and availability of information from an employee perspective" (Da Veiga/Martins 2015, 166), measuring it quantitatively by using an information security culture questionnaire developed in previous research by Da Veiga et al. 2007 and Da Veiga/Eloff 2010. The rationale of the questionnaire is that employees who agree to the statements in the questionnaire also have higher information security awareness, and thus show better information security compliance behaviour (Da Veiga/Martins 2015, 166). Based on the results of this assessment, interventions were planned and conducted with special focus on areas in which employees exhibited a lack of awareness. In the next iteration of the survey, trends in the information security culture of the analysed organisation were identified, improvements measured, and further necessary improvements defined.

As a similar assessment-based study of cybersecurity trainings within banks notes, information security culture-oriented approaches show a striking proximity to some concepts of competence due to their focus on the development of a security-supportive social context (Fagade/Tryfonas 2016, 133). This is important to consider given the prior acknowledgement of addressing the socio-cultural domain of cybersecurity within organisations.

2.1 Assessment-based Cybersecurity Trainings in finance

2.1.1 ISCA-Framework

In their 2015 paper, Da Veiga and Martins discuss whether the security culture in an international financial institution may be influenced positively by assessment-based information security awareness training actions (da Veiga/Martins 2015). The authors focus on improving information security culture because they perceive it as a strong influencing factor on information security compliant behaviour: employees process data and information based on their attitudes, assumptions, beliefs, values and knowledge constitutes an information security culture, which in turn influences information security behaviour (Da Veiga/Martins 2015, Da Veiga/Eloff 2010). This view indicates that information security culture may either support compliant information security behaviour because compliant behaviour becomes the norm (Da Veiga/Martins 2015, 166), or, if non-compliant behaviour becomes the norm, this diminishes overall information security (Da Veiga/Martins 2015, 163). In order to influence information security culture to encourage compliant behaviour of employees, da Veiga and Martins recommend awareness-training and monitoring activities in accordance with previous research on the topic from outside the finance industry (Ifinedo 2014, ISO/IEC 27002:2013, Herold 2011, Parsons et al. 2010, Herath/Rao 2009, Thomson et al. 2006, Von Solms/Von Solms 2004, Vroom/Von Solms 2004 , Nosworthy 2000, Gaunt 2000).

Da Veiga and Martins conducted a longitudinal case study in an international financial institution to assess whether information security culture improved due to their developmental interventions. The goal of their interventions was to induce “a culture in which information is governed and protected by all employees at all times in accordance with organisational policy and regulatory requirements” within this financial institution (da Veiga/Martins 2015, 163). For this purpose, they employed information security culture assessment (ISCA) based awareness trainings with pre- and post-intervention-questionnaires four times over the course of eight years.

The first assessment was conducted in 2006 with a sample size of 1941 employees, followed by an assessment in 2007 with 1571 respondents. The third assessment was held in 2010 and received 2320 responses, followed by the last assessment in 2013 with 2159 employees. The rising numbers of responses is mainly due to the growth of the company, which had about 4000 employees in 2006, but more than 8000 in 2013[1], while respondent rates were relatively stable between 28% to 40%. The majority of respondents were employees in the country headquarters of the organisation in South Africa, Australia and the United Kingdom.

In sum, the assessments covered nine dimensions of information security culture on the perceptional level (da Veiga/Martins 2015, 167):

1. Protection of information assets
2. Management’s perception of information security management
3. Change and willingness of users to change in order to protect information
4. User awareness and training regarding information protection requirements
5. Employees’ understanding of the information security policy
6. Effectiveness of investing in information security resources
7. Trust of employees in privacy and secure communication within the organisation
8. Information security governance (such as monitoring)
9. Additional needs for information security training

[1] We rounded the exact numbers of employees to the next thousand to ensure anonymity of the institution.

The results of the assessments of da Veiga and Martins show that after the ISCA-assessment based trainings, “employees had a more positive attitude towards information security” and their knowledge about information security improved (da Veiga/Martins 2015, 169).

The percentage of employees receiving information security training increased from 23,8% in 2006 to 72,8% in 2013. Those who received information security training showed a significantly stronger information security culture than those who did not receive any trainings; however, this only holds true for the years 2006 and 2013 (da Veiga/Martins 2015, 171):

- training actions until 2010 were not suited to improve ISC of employees with prior training and their perception of the need for further trainings receded slightly
- training actions until 2010 improved ISC of employees without prior training merely marginally
- training actions after 2010 only improved ISC of employees with prior training significantly, but for employees without prior training only marginally
- About two-thirds of the employees felt the need for additional training after the ISCA-process

In 2013, ongoing developmental areas were identified:

- Password sharing practices
- Incident awareness
- Incident reporting
- Knowledge about the ISP (Information Security Policy) in place (location of physical copy, content, influence of changes on employees)
- Protection of organisational data in regard to third parties
- Capability of the banks to continue their daily operations in the face of a cybersecurity incident

These results suggest that the performed training actions were not particularly suited for the employees’ needs to learn about information security. The authors did not provide a comparative multivariate analysis of the development of the security culture in the assessed institution over the eight years observed, thus the results are mainly based on bivariate analysis which cannot control for intervening variables.

The article does not list all the used methods or techniques to deliver the training actions. However, the authors mention that the most preferred method for receiving information security information were face-to-face-presentations, followed by web-based training and e-mail instructions (da Veiga/Martins 2015, 171).

Da Veiga and Martins (2015, 175) conclude that their ISCA framework did improve awareness for cybersecurity risks and expected compliant behaviour. However, further research is necessary to determine whether the measured perceptions of employees in an ISCA correspond with actual compliant behaviour. The authors strongly recommend employing a managerial perspective on change management, training and awareness programmes to improve information security policy compliant behaviour, with the goal of creating a culture of information security (ibid., 172). The effectiveness of the ISCA-framework, for instance, could be determined by measuring the difference between self-reported and objectively recorded behaviour of employees (e.g. Employees' perception on incident reporting and actual incidents reported) (ibid., 175).

In 2016, Tesleem Fagade and Theo Tryfonas applied an adaption of da Veiga and Eloff's ICSA framework to four Nigerian banks (Fagade/Tryfonas 2016). They also provided strong arguments for the implementation of a security culture: In their assessment they found that security could not be achieved purely by communicating the expectation towards employees to act compliant, as is often the practice during quick certification processes (ibid., 133). However, instead of proposing more bottom-up training activities, they suggest a top-down approach in which management enforces compliant behaviour by incorporating security requirements within operational system architecture, therefore making it part of the job function. Thus, employees might not need "extra motivation, reward or punishment to perform those functions" any more (ibid., 136) – provided they were well-educated on these new job functions in the first place.

To the contrary, Wong et al (2019) state that "sufficient training and proper education" (ibid., 1258) is necessary to "inoculate" security consciousness into employees and thus induce a security conscious culture. But they do not distinguish further between different forms of trainings. Another study from Terlizzi et al (2017) identified training actions as being central to the development of cybersecurity cultures in Brazilian banks, but did not elaborate on the concrete training actions either.

2.1.2 HAIS-Q

A recent comparative study among 189 bank employees and 500 employees from other sectors in Australia found that bank employees show significantly higher information security awareness than other employees (Pattinson et al. 2017, 184). Based on another assessment instrument, the Human Aspects of Information Security Questionnaire (HAIS-Q) originally developed by Parsons et al. (2014), they found that this difference in awareness was not based on the amount of formal information security education the respective employee groups received (Pattinson et al. 2017, 186). Far more influential were information security trainings performed during working hours at their workplace (ibid., 186). However, it was not the frequency of these trainings that increased information security awareness, but the *type* of training the employees received (ibid., 187). Therefore, a "multi-channelled InfoSec training regime" incorporating all learning styles has proven to be particularly advantageous for building up information security awareness (ibid.). Incorporated in this regime is a *mix of* *platforms and media* including intranet and e-mail communication reporting recent security incidents and techniques for appropriate behaviour, online videos with actual employees from upper management using message framing and emphasizing the importance of secure behaviour in regard to data, information and systems as well as posters and flyers on the topic (ibid.).

2.2 Awareness-based Cybersecurity Trainings in Finance

In a recent study Stefan Bauer, Edward Bernroider and Katharina Chudzikowski evaluated the use of Information Security Awareness Programmes in three Central and Eastern European banks (Bauer et al. 2017). They compared three different approaches in delivering awareness interventions:

- Interaction approach: IS-department interacts intensely with all employees via intranet and a variety of training actions on a regular basis (Bauer et al 2017, 149). High user involvement fosters feedback cycles about acceptance and effectiveness of IS interventions to IS professionals (Bauer et al. 2017, 154).

- Incident related approach: incidents covered by media are reported to the employees on a regular basis (Bauer et al. 2017, 150), which increases the accuracy of risk perception of employees (Bauer et al. 2017, 154).

- Accountability Approach: a strong focus is put on compliance and its enforcement through regulation (Bauer et al 2017, 150). When implemented correctly, this approach may increase the sense of responsibility for IS among all employee groups (Bauer et al. 2017, 154)

2.3 Gamified training approaches in finance and adjacent sectors

Gamification is a method to enhance motivation in computer-based learning processes and has been steadily gaining popularity during the last decade (Jin et al. 2018, 151). Different formats, from virtual reality and web-based games to massive multiplayer online games and simulations, are applied in game-based learning. By means of gamification, students may be enabled to choose their actions and learn from the consequences of their actions as well as make mistakes and experiments in a risk-free environment. Therefore, they are enabled to actively learn to solve problems according to their age (ibid.). Gamification was theorized to overcome learning barriers such as lack of attention, engagement or interest (Conolly et al. 2012) and to improve learning through enjoyment and novelty-experience (Pekrun/Linnenbrink-Garcia 2012; Novak 2014). In addition, gamification was assumed to facilitate context-oriented learning processes through the close replication of real-world situations in narrative-based storylines (Hamari et al. 2014).

Jin et al. found that until 2018, game-based learning was applied only limitedly to cybersecurity education (Jin et al. 2018, 151). Within the literature review conducted for this draft, no scientific studies concerning gamified cybersecurity trainings conducted in the finance sector were identified. However, as with any literature review, some publications may have eluded our systematics. Nevertheless, the literature review yielded a few studies closely related to cybersecurity trainings in banks. The first relevant article found was an evaluation of minimalistically gamified training actions, conducted within a bank on a topic highly related to cybersecurity: anti-corruption (Baxter et al. 2016). The second article highly relevant to our work did not focus on banks in detail, but discussed issues of cybersecurity training in the wider field of critical infrastructure – of which financial institutions are a vital part of (Brilingaitė et al. 2020).

2.3.1 Minimalistic Gamification

Baxter et al. (2016) evaluated the application of gamification to anti-corruption trainings in a large multinational bank. For this purpose, software of a commercial provider of gamified trainings was used, namely True Office. The trainings were "minimalistically" gamified, meaning that trainings were visually animated, narrative-based storytelling was applied and interactive engagement was required. However, the trainings were not completely gamified down to every detail (ibid., 2). At the beginning, the learning objectives were set. Participants then had to complete a set of tasks and at the end of the training, they had to take a quiz. The training took place within a realistic animation of familiar work-related settings (ibid., 8).

The authors found that their minimalistically gamified training actions improved the acceptance of the training program compared to previous, non-gamified interventions, because the gamified training was "more enjoyable, fun, interesting, and informative" (Baxter et al. 2016, 2). Many of the 127 employees participating in these trainings expressed a strong preference for the conducted gamified training in comparison to other formats, such as online-training using only written material or traditional in-person lectures (ibid., 12). In terms of actual knowledge gain, the trainings only proved to be effective for certain subgroups of employees (mainly younger or less experienced employees, ibid., 3). The authors' findings are consistent with other literature on the topic of effectiveness of gamification, indicating some gain in learning and motivation (Devers/Gurung 2015; Connoly et al. 2012, 671).

2.3.2 CDX – Cybersecurity Defence Exercises in Critical Infrastructure

One way of completely gamifying cybersecurity trainings is conducting Cybersecurity Defence Exercises (CDX) (Furtună et al. 2010, Brilingaitė et al. 2020). Basically, in a CDX two teams play against each other in a replicated real-world ICT setting: The attackers (usually called the Red Team), who try to compromise the security of the systems set up, and the defenders (usually called Blue Team), whose goal is to defend the systems to the best of their abilities. In some CDXs, additional teams take part in the game to facilitate proper conduct and to provide an even more realistic experience for the players. They are labelled EXCON (Exercise

Coordination) Teams, White, Black, Grey, Green or Gold Teams; however, their labelling is not consistent regarding the roles these teams assume during a CDX (Brilingaitė et al. 2020, 3). Usually, CDX participants are IT professionals, from entry level positions such as student or trainee to specialist.

2.3.2.1 Integration of non-technical staff into CDX – Hybrid CDX

Brilingaitė et al. (2020) evaluated the possibility to extend Cybersecurity defence exercises to a broader group of participants, namely non-technical staff. Hence, they conducted a case study with more than 70 participants in a joint military-civilian cybersecurity exercise focused on critical infrastructure. The exercises' goal was to defend critical infrastructure against different cyber threats (Brilingaitė et al. 2020, 3). In addition to Red and Blue Teams for the attackers and defenders of the replicated critical infrastructures, the authors introduced Purple Teams to the CDX, making it a hybrid CDX. Purple Teams represented employees of a simulated organisation owning the critical infrastructures, as well as business end-users interacting with this organisation. Thus, the Purple Teams created close to real world data flows by performing routine daily operations, such as communicating with clients as well as purchasing and selling on virtual marketplaces using networked services, IoT and ICS (Brilingaitė et al. 2020, 3-4).

2.3.2.2 Conduction of Hybrid CDX – Cybersecurity Competence development and assessment (CDA) framework

Concluding their research, Brilingaitė et al. (2020, 9-11) propose a Cybersecurity Competence Development and Assessment (CDA) Framework. The CDA structures the sequence of activities performed in a CDX to enable the systematic involvement of non-technical participants, as well as to allow for proper evaluation of the process at the individual level. Therefore, they distinguish between four crucial phases of hybrid CDX:

1.) Identify: Pre-exercise assessment of the training audience (gathering participant profiles) and design of the learning objectives (compile competence map)
2.) Plan: Scenario, Environment/Range, Attack vectors; Pre-exercise training of teams and individuals (learning material, courses or lectures), define group and individual tasks and roles; Without pre-exercise training, the start of the CDX can be quite confusing, especially for ad-hoc teams that did not know each other before; it is crucial for team development (collaboration, coordination and communication, task distribution)
3.) Conduct: Pre-trained teams play against each other within a set timeline
4.) Evaluate: Post-exercise assessment of competencies of individual participants via self-reflection

2.3.2.3 Effectiveness of Hybrid CDX

As previous research did not provide objective evidence of the usefulness of CDX, Brilingaitė et al. (2020) put particular emphasis on the evaluation of the learning experience of their hybrid CDX setup. They placed observers within each team to collect data on team collaboration, information sharing, learning curves and obstacles to the learning experience of the participants. Additionally, they performed assessments of the competence level of each participant, before and after the exercise. The assessments were semi-structured questionnaires based on self-reflection (Brilingaitė et al. 2020, 5).

The assessments of the hybrid CDX showed that a large proportion of participants – though quite self-confident about their expertise at the beginning of the CDX – identified knowledge gaps and lack of skills in different areas of cybersecurity competence after the exercise (Brilingaitė et al. 2020, 6). Thus, hybrid CDX may be applied to raise awareness of knowledge gaps and lacking skills.

During the hybrid CDX, several skills as well as knowledge of the participants were developed further (Brilingaitė et al. 2020, 7-8):

- The knowledge about attacks and their impact on the system
- Technical skills
- Psychological understanding of the opponent
- Making new connections
- Improved critical thinking
- Using soft skills
- Providing user support
- Time Management

The hybrid CDX conducted by Brilingaitė et al. (2020) was quite effective at developing of team competencies. Participants acquired competence in their abilities of task distribution, external and internal team collaboration, as well as coordination, teamwork and meeting new people (ibid., 7). Most teams were able to overcome problems of miscommunication and information sharing due to integration problems, and succeeded in creating a fun, friendly atmosphere in which it was possible to express oneself.

The results of Brilingaitė et al. show that the non-technical participants also acquired knowledge and skills about cybersecurity during the hybrid CDX, and wanted to be even more actively involved (Brilingaitė et al. 2020, 8). Non-technical participants perceived that they learned a lot about attacks and their potential impact on the system. Therefore, the integration of non-technical staff not only helps to create a more realistic replication of a real-world context for the exercises, it also provides considerable benefits to the cybersecurity learning experience of the participating non-technicians. Since their behaviour may be crucial for cybersecurity in many organisations, their integration into CDX appears to be promising.

2.3.2.4 Hindrances for Hybrid CDX

The widespread implementation of CDX in organisations of any size is particularly impeded by their high cost (of money and time) and high effort required (Brilingaitė et al. 2020, 11).

Additionally, the purely competitive character of the CDX does not suit all types of learners (Brilingaitė et al. 2020, 12). As a solution, they suggest integrating several assessments into the CDX, in which all participants have the opportunity to step out of the competitive, stressful mode, and instead have time to analyse, report and reflect on attacks within their teams (ibid.).

2.3.2.5 Challenges of gamification for cybersecurity competence trainings

An evaluation of a game-based cybersecurity training intervention with US-American students conducted by Jin et al. (2018) showed that there are considerable gender differences regarding the enjoyability of gamified cybersecurity education interventions. The results suggest that male participants found the game-based learning activities more enjoyable and interesting than female participants did. Moreover, male students indicated that they had learned something more often than female students did (Jin et al. 2018, 156). This indicates slight variances in both the reception and effectiveness of gamification-based tasks across genders, and is something to consider if gamified training actions are proposed.

3 Selected previous Training Approaches in other sectors

In this section, several cybersecurity, information security or compliance training approaches, that have been applied and scientifically studied outside of banking and finance, will be discussed. Since banks and other financial institutions share many commonalities with other enterprises, such as being an organisation or being threatened by similar cyber threats, findings from trainings outside the financial sector can be in part transferred to training actions in banks and fintech.

Most scientifically assessed training actions conducted in organisations focus on the development of information security compliance, awareness, behaviour or culture. The term "cybersecurity training" is hardly used by anyone, and the few trainings performed in the name of cybersecurity are targeted at information security.

Cybersecurity Compliance trainings as such are rare, because of the notion that compliance has to be ensured by cybersecurity governance methods from the "command & control" spectrum, such as enforcement, monitoring, deterrence, social control and punishment (i.a. Cheng et al. 2013, Aurigemma/Mattson 2014), fear appeals (Johnston et al 2015) or persuasion (Barlow et al. 2013).

The first branch of cybersecurity compliance trainings focused heavily on deterrence and later awareness building (Barlow et al. 2013, 146). Employees were informed about cybersecurity policies and consequences of not acting according to them (sanctions). However, employees often applied neutralisation techniques to rationalise non-compliant behaviour (ibid.). Even when threatened with serious sanctions, employees often chose not to act in a compliant manner because they thought to have a compelling reason not to, such as choosing the more comfortable way because nobody would get harmed anyway, believing to have no other acceptable choice, or allowing for the occasional deviation from cybersecurity policies because of being a good employee at large (ibid., 148-149). Barlow et al. argue that cybersecurity policy compliance training programmes may heavily benefit from addressing these neutralization techniques as well (ibid., 154; Siponen et al. 2020). In recent years, cybersecurity compliance training approaches developed that focused increasingly on education and empowerment (Choi/Yoo 2014, Talib/Dhillon 2015).

Within information security, the field of study concerned with behaviour modification expands on the aforementioned concept by inducing information security (conscious care) behaviour (Protection Motivation Theory, PMT) (Safa et al. 2015, Mamonov/Benbunan-Fich 2018) or threat avoidance behaviour (Technology Threat Avoidance Theory, TTAT) (Arachchilage/Love 2014), using a variety of interventions. These approaches aim to incentivize employees to act in compliance with ISP programs, by reducing opportunities to act in a non-compliant manner (Situational Crime Prevention Theory, SCPT), and by motivating them to act in compliance by means of social bonds produced in shared information security activities on the other hand (Social Bond Theory, SBT) (Safa et al. 2015).

During the last decade, a new field of study has developed, namely Security Education, Training and Awareness (SETA) (Vasileiuo/Furnell 2019, xvi). Scholars within this field of study are concerned with security education programmes, which integrate awareness-raising activities, skill acquisition and competency training into a common knowledge body aimed at improving employees' cybersecurity behaviour (ibid.).

3.1 Security Education, Training, and Awareness (SETA) Approach

Albert Caballero (2017) provides a comprehensive overview of the framework as well as of elements and contents of a SETA programme to be implemented in organisations. In principle, SETA programmes start with general education and training activities for all users and relevant job functions; subsequently refining training and education efforts to fit the role of each individual or group (ibid., 497).

Following this approach, the first step of a SETA programme is an extensive information security awareness training action targeting all personnel, regardless of their IT usage, position and job function (ibid., 497). Because of these general trainings in information security awareness, all personnel should gain increased awareness of potential risks and threats as well as an understanding of the importance of information security for the organisation in general (ibid., 449). All personnel should be aware of the need to protect people, assets and resources within the organisation (ibid., 504) Due to the integration of all personnel into this general training action the foundations for a positive information security culture are being established (ibid.).

The next step of a SETA Programme is training for all personnel involved with organisational IT systems, wherein information security basics are taught, and information security literacy is developed (ibid., 497). These awareness trainings should encourage everyone using IT systems in an organisation to make information security part of their routine, and to report incidents immediately and correctly (ibid., 499). After this training step, all employees should be aware of the following topics (ibid., 501):

- Password security
- Email phishing
- Social engineering
- Mobile device security
- Sensitive data security
- Business communications security

After these general training actions, further trainings may be customized for different groups according to their functional roles and responsibilities regarding their use of IT systems (functional training) and their level of proficiency in information security (skill-based training) (ibid., 497; role definitions based on PCI-DSS, 2014). Through functional training, every specific role in an organisation develops the skills and knowledge necessary to perform their job function (ibid., 504). They should be enabled to recognize their accountability and obligations regarding information security, to learn to handle processes that are included in their job function securely, and to recommend best practice on their own initiative. In these functional training actions, all personnel performing management roles should learn to set and communicate security expectations, encourage and re-enforce security awareness in staff by holding employees accountable for their security-related actions (ibid., 499 and 504). Due to skill-based adaption of these functional trainings, the current skill level of individuals is considered to optimize the learning effects (ibid., 498).

IT Security specialists and professionals are integrated into the training process both as trainees and as instructors (ibid., 497). They are receiving functional and skill-based training to perform their job functions securely and are encouraged to share their education and experience within other parts of the company, in order to generate spillover effects onto employees with different, often specialized roles.

To be able to customize the whole training process to the special needs of an organisation and its personnel, assessment and evaluation procedures have to be built in (ibid.).

Caballero recommends using a combination of different training delivery techniques (ibid., 501):

- Computer-based training
- E-Mails
- Video campaigns
- Posters and banners
- Lectures and conferences
- Regular newsletters
- Brochures and flyers
- Corporate events

To be effective, Caballero states that it is important to design the trainings in a way that they are easy to use, scalable to the size of the organisation and fitting the industry requirements (ibid., 502). Additionally, it is important to provide trainings on topics that are perceived as personally useful for the target audience to foster motivation (ibid., 504).

3.2 Cybersecurity Competence Training Approaches

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

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

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

Nevertheless, there are studies that provide a comprehensive analyses of notions prerequisite to competence, such as skills. In the following section, the most promising study regarding cybersecurity competence development (and its evaluation) shall be reviewed.

3.2.1 Cybersecurity Skills Index (CSI)

The study conducted by Carlton et al. (2019) develops a cybersecurity skills index (CSI) comprised of nine platform-independent cybersecurity skills for non-IT professionals. The skills were identified by a panel of cybersecurity experts and based on top 12-list of cybersecurity incidents in 2014 (see Table 2). The authors define cybersecurity skill as "an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security to mitigate cyber-attacks (ibid. 2019, 102; Carlton et al. 2016).

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

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

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

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

As Carlton et al. (2019, 102) stated, previous research suggests that the "use of observable hands-on skills provides unbiased evidence of competence" (see also D'Arcy et al. 2009, Hu et al, 2011).

3.3 Cybersecurity Training Gamification Approaches

During the last decade, several cybersecurity training initiatives gamified their approaches to increase the interest and motivation of trainees in their training actions. Gamification is defined as the "use of game design elements in non-game-contexts" (Deterding et al 2011, 9). In the context of information security or cybersecurity training, gamification means the design of training actions on these topics to provide training experience similar to those created by games (Koivisto/Hamari 2019, 193). By making a mundane, purpose-driven training action engaging and exciting, enabling the experience of mastery, competence, immersion and flow through a set of game elements, the objectives of the training action should be achieved with more ease and more efficiently than it would be in conventional trainings (ibid., 192). Gamification is widely used for various topics and contexts, but has still been rarely applied to topics related to cybersecurity in organisations (Koivisto/Hamari 2019: 204-205). Particularly when used in business contexts, gamification is frequently applied as so-called Serious Game. Clark C. Abt, a pioneer in this field of pedagogical research, defined Serious Games as follows:

“The oxymoron of *Serious Games* unites the seriousness of thought and problems that require it with the experimental and emotional freedom of play. Serious Games combine the analytic and questioning concentration of the scientific viewpoint with the intuitive freedom and rewards of imaginative, artistic acts.” (Abt 1987, 11-12)

As business contexts are mostly perceived as demanding *serious* thought about solving *serious* problems, the concept of Serious Games is highly applicable. The difference between gamification and serious games is that serious games additionally incorporate pedagogic elements that are not necessarily part of all gamification attempts (Le Compte et al. 2015, 3). Le Compte et al. (2015, 11-12) present an overview of learning mechanics (Table 3) and game mechanisms (Table 4) that can be implemented into serious games:

Behavioural Momentum	Role Play		
Cooperation	Collaboration	Goods/Information	
Selecting/Collecting	Tokens	Cut Scenes/Story	
	Cascading Information	Communal Discovery	
	Questions & Answers	Pareto Optimal	Appointment
Strategy/Planning	Resource Management	Infinite Gameplay	
Capture/Eliminate	Tiles/Grids	Levels	
Game Turns	Action Points	Feedback	
Time Pressure	Pavlovian Interactions	Meta-game	
	Protégé effects	Simulate/Response	Realism
Design/Editing	Movement		
Tutorial	Assessment		
	Competition		
Urgent Optimism	Ownership		
Rewards/Penalties	Status	Virality	

Table 3: Game mechanics (Le Compte et al. 2015, 11)

Instructional	Guidance	
Demonstration	Participation	Action/Task
Generalisation/ Discrimination	Observation	Feedback
	Question & Answer	
Explore	Identify	Discover
	Plan	Objectify
Hypothesis	Experimentation	
	Repetition	
	Reflect/Discuss	Analyse
	Imitation	Shadowing
Simulation	Modelling	
Tutorial	Assessment	
	Competition	
Motivation	Ownership	Accountability
	Responsibility	Incentive

Table 4: Learning Mechanics (Le Compte et al. 2015, 12)

The following gamification attempts presented in Table 5 in the field of information or systems security are a selection of serious games and applications of game elements to non-game contexts and do not claim to be exhaustive, particularly regarding commercial solutions. Most gamification attempts in cybersecurity training presented here were published in peer reviewed journals or presented at scientific or practitioner conferences. Table 6 summarizes the name of the game, the developing organisation, the type and setup of the game. The last column states the source who reviewed the respective game.

In the third column of the table, in which the type of the game is presented, we follow the systematics from Cone et al. (2007). They distinguish between two categories of games for enhancing cybersecurity: interactive first-person (IF) games and resource management (RM) simulations (Cone et al. 2007, 64). In an interactive first-person game, players interact directly with different elements of a virtual environment from their own point of view, making consecutive decisions and experiencing the consequences of these decisions immediately. The most common example for interactive first-person games is the genre of first-person shooter games. By contrast, resource management simulations require the player to manage a set of limited resources within a virtual environment to achieve certain goals. These two general types of serious games can be further split up into cooperation vs. non-cooperation approaches (cooperation or opposition between players) with dynamic or static game elements (multiple stages or sequences vs. static setting) (Roy et al. 2010).

Title	**Developer**	**Type**	**Setup**	**Source**
CyberCIEGE	Naval Postgraduate School and Rivermind Inc.	IF simulation, non-cooperative, dynamic	Persona in an office scenario handles cybersecurity threats	Cone et al (2007)
HATCH	Technical University Munich, Goethe-University Frankfurt	IF simulation, non-cooperative, dynamic	Persona in an office scenario elicits social engineering attacks	Beckers et al. 2016
CyberNEXS (TM)	SAIC	IF simulation, CDX, dynamic	Exploring game design for cybersecurity training	Nagarajan et al. 2012
Anti-Phishing Phil (TM)	Wombat	IF game, static	Fish “eats” good links and rejects “bad” ones	
Scholar Compliance Training/ Scholar for Cybersecurity	True Office	Simulation, Storytelling, dynamic	Persona investigates an alleged wide-spread bribery at a large company	Baxter et al. 2016
CyberProtect (R)	Carnie Inc. (originally from: DoD – US Department of Defence)			DoD 1999
Carronade	US Military Academy (USMA)	IF Simulation, static	Detection exercise with simulated phishing mail	Dodge et al. 2007
SERUM		IF Simulation & embedded training, static	Exercise in detecting phishing mails	Jansson/Von Solms 2013
PenQuest	FH St. Pölten University of Applied	IF Simulation, Non-cooperative Roleplay	Attack modelling - combines attack semantics with	Luh et al. 2019

	Sciences, Austria		possible countermeasures	
What.Hack				Thornton/Francia III 2014
Brute Force				Thornton/Francia III 2014
Friend or Foe				Thornton/Francia III 2014
Data Security	Playgen	Simulation	new employee must identify security concerns	Le Compte et al. 2015, 4
Agent Surefire	Mavi Interactive	Simulation	Catch an insider threat, identify breaches and security issues	Le Compte et al. 2015, 4
Cyber Awareness Challenge	Carney Inc.	Simulation	Be a federal government agent and catch an unnamed hacker	Le Compte et al. 2015, 4
Cyber Security Investigation (CSI) Game	InfoSecure	Puzzle Game	Find the right combinations of events that lead to an IS incident	Le Compte et al. 2015, 4
Game of Threats	PwC	Resource Management, Card Game	Cybersecurity Risk simulation	Tioh et al. 2017
Social engineering game		3D, VR IF Simulation	Piggybacking, Tailgating, Mantrap	Jin et al. 2018
Cyber defense tower game		Resource Management	Defend virtual computer server from attacks by placing defensive structures	Jin et al. 2018

2D GenCyber Card Game	Nestler (2016)		digitalized version of the NSA GenCyber Card game: Understanding the 10 Cyber Security First Principles	Jin et al. 2018

Table 5: List of cybersecurity games from academic literature

Regarding the content of gamified cybersecurity trainings, Arachchilage/Love (2014, 706) have suggested that perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity and perceived susceptibility elements should be part of cybersecurity trainings focusing on the prevention of phishing attacks.

Nagarajan et al. (2012, 257) list the following training topics for cybersecurity gamification:

- Password use and Management
- Protection from malware and spam
- Patch management
- Social engineering phishing techniques awareness
- Compliance
- Implementation of new technology
- Data backup and storage procedures
- Incident response procedures
- Use of personal devices in work environment
- Manage host/network access control lists
- Individual responsibilities and accountability

Due to the growing body of literature on gamification during the last decade, various meta-analyses have been conducted.

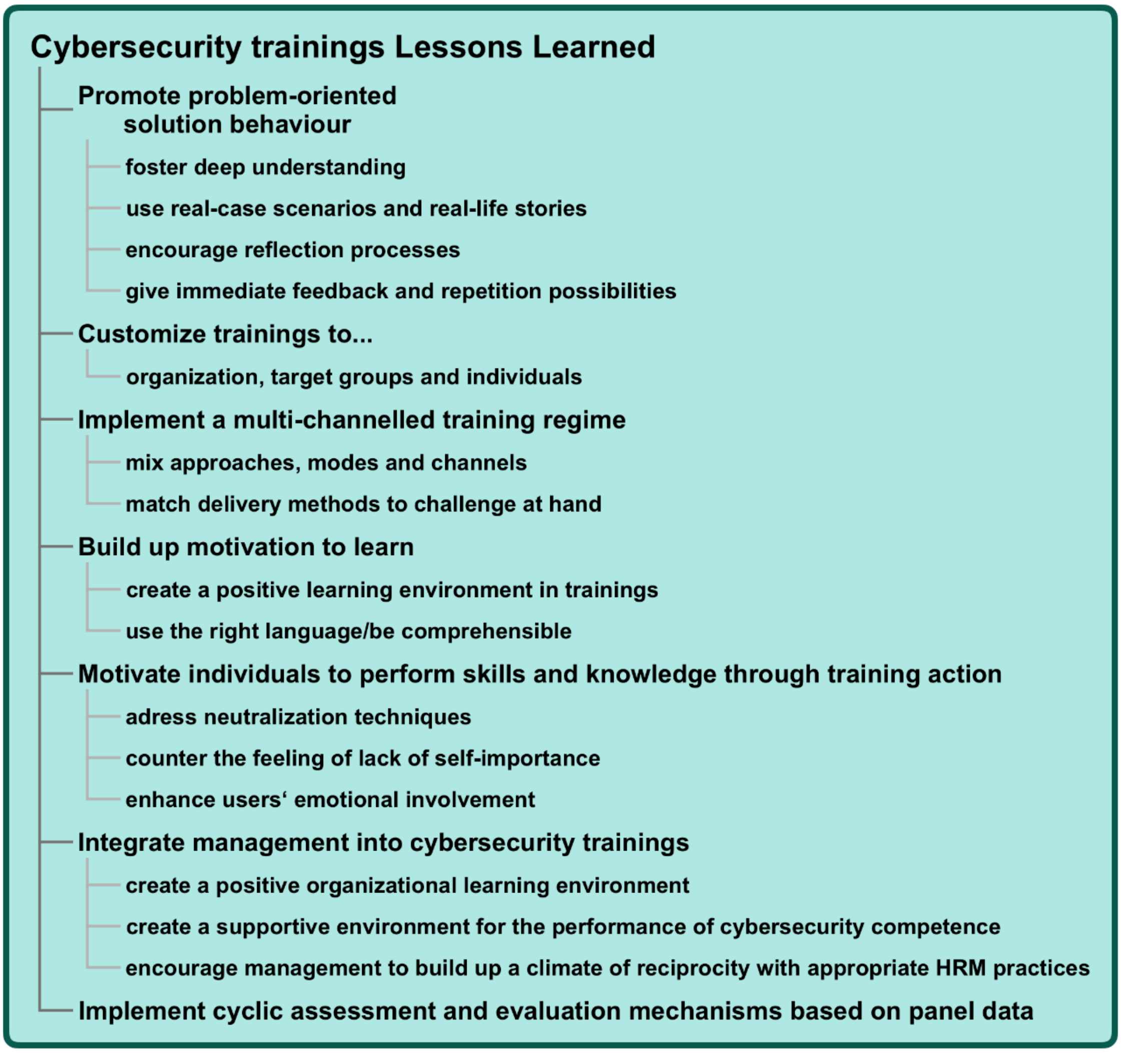
For instance, Sailer and Homner conducted a meta-analysis of gamification studies that showed significant positive effects of gamification on cognitive, motivational and behavioural learning outcomes (Sailer/Homner 2020, 106). The positive effect of gamification on cognitive learning outcomes in particular proved to be the most stable across studies (ibid.).

Baptista and Oliveira conducted a meta-analysis of literature on the topic in 2019. They identified the following factors and interdependencies for the effectiveness of gamification and serious games: Ease of use, learning opportunities and social aspects of the game result in an increasing perception of usefulness of the game. Further, the perception of usefulness combined with the right level of “hedonic” value (fun, pleasure, excitement), enjoyment and the user’s evaluation as favourable or unfavourable affect the intention to perform specific security-relevant behaviour in the future (Baptista/Oliveira 2019, 310).

While the attributes of the game seem to influence its effectiveness, it also depends on who is playing the game. Baxter et al. 2016 investigated the effects of gamification on compliance training in banks. They found that less experienced employees, supposedly being younger and more familiar with games, enjoyed gamified training actions and learned more than employees with more occupational experience (Baxter et al. 2016). This age-related variance should be considered alongside the previously identified gender-based differences as potential limitations of game-based approaches.

4 Conclusion: Lessons Learned from previous Approaches

Many of the approaches discussed in the previous sections discussed some issues to be learned from their approaches. Section 4 of this deliverable is devoted to collect these lessons learned for D6.4. The following list summarizes these lessons learned from previous cybersecurity training approaches in finance and other sectors (figure 2):



Cybersecurity trainings Lessons Learned

- Promote problem-oriented solution behaviour
  - foster deep understanding
  - use real-case scenarios and real-life stories
  - encourage reflection processes
  - give immediate feedback and repetition possibilities
- Customize trainings to...
  - organization, target groups and individuals
- Implement a multi-channelled training regime
  - mix approaches, modes and channels
  - match delivery methods to challenge at hand
- Build up motivation to learn
  - create a positive learning environment in trainings
  - use the right language/be comprehensible
- Motivate individuals to perform skills and knowledge through training action
  - adress neutralization techniques
  - counter the feeling of lack of self-importance
  - enhance users‘ emotional involvement
- Integrate management into cybersecurity trainings
  - create a positive organizational learning environment
  - create a supportive environment for the performance of cybersecurity competence
  - encourage management to build up a climate of reciprocity with appropriate HRM practices
- Implement cyclic assessment and evaluation mechanisms based on panel data

Figure 2: Cybersecurity training lessons learned from previous approaches

4.1 Promote problem-oriented solution behaviour

One lesion to be learned from previous cybersecurity training approaches in finance and beyond is to focus on the development of problem-oriented solution behaviour based on a deep understanding of problematic cybersecurity situations and their solution.

The basis for problem-oriented solution behaviour is a deep understanding of problematic cybersecurity situations. Ideally, all users as well as the IS staff understand the importance and the reasoning behind cybersecurity procedures reacting to these problematic situations

(Bauer et al. 2017, 152). Ideally, all users as well as IS staff understand the importance and the reasoning behind IS procedures (Bauer et al. 2017, 152). This is only possible, if all actors gain knowledge about certain concepts that might seem counter-intuitive for non-IT professionals:

- The impact of cybersecurity breaches is often not physically visible and/or its consequences are intangible (De Bruin/Janssen 2017, 3)
- The complexity of the interaction between humans and systems in cybersecurity situations is “beyond the understanding of most people” (De Bruin/Janssen 2917, 4)
- Cybersecurity risks are not remote. Cybersecurity incidents can happen to anyone despite the best security measures (De Bruin/Janssen 2017, 4)

One way to achieve deep understanding is to make cybersecurity a real-life topic through using real-case scenarios and real-life stories. Since trainings on the job have proved to be more effective than formal courses (Pattinson et al. 2017, 186), simulated trainings could profit from the use real-case scenarios and case studies in trainings (Aldawood/Skinner 2019, 11). To encourage increasing user involvement, simple and engaging real-life stories should be used for illustration purposes (Bauer et al. 2017, 154).

Additionally, encouragement of reflection processes, immediate feedback and repetition cycles seem to foster learning and problem-oriented solution behaviour. Albrechtsen/Hovden (2010) found that collective dialogues and group work processes were appropriate means to encourage reflection processes. Immediate feedback and repetition in game-based approaches increased participants’ capacity to identify phishing websites accurately (Abawaji 2014, 245).

4.2 Customize trainings to organisation, group and person

For the trainings to be effective, several publications found customization of trainings to the targeted organisation, group and individual highly important. First, the trainings must be customized to the organisations needs resulting from their branch, size and organisational specifics. On the side of organisational specifics, Aldawood and Skinner (2019, 4) recommended the customization of cybersecurity trainings to business needs, market pressures, degree of digitalization of business, budget available to the firm.

Second, trainings should be customized to target groups within the organisation at hand.
Bauer et al. (2017, 150) suggested tailoring trainings for different groups of employees, because they face different IS risks, awareness levels and behaviours:

- User Groups:
    - Headquarter Employees (general management sections of banks)
    - Branch employees (interaction with clients directly)
- IS managers

Bauer et al state, that headquarter employees perceive mostly threats from outside the organisation, while they do not see their own behaviour as crucial for ensuring IS. Headquarter staff is usually also not aware of the risk of a malicious insider. Branch employees report high awareness of data leakage risks and increasing social engineering attacks (Bauer et al. 2017, 152). At the same time, branch users reported struggling with safe identification processes like logging on and off from their computers with safe passwords the most (Bauer et al. 2017, 154). Hence, what these two user groups have in common is the lack of recognizing their own responsibilities for IS, while assigning these responsibilities almost exclusively to the IS department instead (Bauer et al. 2017, 154).

Third, trainings should be customized to groups of individuals. Pattinson et al. (2017, 187) found it crucial for cybersecurity trainings to be customized to different learning styles. Trainings should also be customized to the skill level of groups of individuals (Ghafir et al 2018, 4992, Caballero). Also, the personality of the individuals to be trained should be taken into consideration. For instance, Abawaji (2014, 247) stated that there is a certain proportion of people that are not willing to learn any game mechanics at all, and therefor gamification is not suitable for all employees.

4.3 Implement a Multi-Channelled Training Regime

Since customizing cybersecurity programmes at all of these levels might not be possible without overarching effort, the implementation of a multi-channeled training regime with a comprehensive mix of approaches, delivery modes and channels is recommended to meet different and even conflicting needs (Bauer et al. 2017, Abawaji 2014, Aldawood/Skinner 2019). Bauer et al. (2017, 154) suggest for ISA programmes to incorporate a comprehensive mix of interventions with a long-term goal in mind. This mix should integrate high density of interactions of IS staff with all user groups with real-world IS incident examples used for interventions like courses, presentations and assessments, while putting a reasonable amount of energy into accountability building without inducing mistrust of employees by being too directive (ibid.). Accountability building activities could comprise cybersecurity events, campaigns, guides, manuals and policies.

Through the use of media richness monotony of training actions should be reduced. For that, a multimodal delivery approach could be applied that uses a broad spectrum of text, video and game elements (Abawaji 2014, 242, 246-247). The training content can be made additionally engaging through graphics, assessments and animations (Abawaji 2014, 242) or by using interactive content (Aldawood/Skinner 2019, 4; Dodge 2007). Bauer et al. report good experience with videos visualizing IS risks and threats (Bauer et al. 2017, 154). Further, they found self-assessment techniques to support user involvement and allow for feedback (Bauer et al. 2017, 155). The most preferred delivery methods by employees were face-to-face-presentations, followed by web-based training and e-mail instructions (da Veiga/Martins 2015, 171).

Pattinson et al (2017, 187): "multi-channelled InfoSec training regime" has proven to be particularly advantageous for building up information security awareness. Incorporated in this regime is a *mix of platforms and media,* such as intranet and e-mail communication reporting recent security incidents and techniques for appropriate behaviour, online videos with actual employees from upper management using message framing and emphasizing the importance of secure behaviour in regard to data, information and systems as well as posters and flyers on the topic (ibid.)

Another study on the use of Online Social Networks (OSN) in Brazilian banks also came to the conclusion that trainings should be delivered employing a variety of activities, covering, e-learning, face-to-face-trainings, events, campaigns, guides, manuals and the intranet (Terlizzi et al. 2017, 241). They analysed five of the biggest banks in Brazil, of which only three offered information security courses, trainings and interventions. One bank conducted a formal course covering the "Fundamentals of Information Security" with additional focus on anti-kidnapping intelligence, anti-money-laundering, anti-corruption, crisis management and business continuity in light of a cyber incident (ibid., 242). The other two banks launched training actions, e-learning courses and campaigns to foster an appropriate risk and control culture, with one bank putting strong emphasis on current examples of cyberattacks and electronic fraud (ibid., 243).

Abawaji (2014, 238-241) found, that matching delivery methods to concrete problems at hand is also important for effective training programmes. Thus, he suggests to use delivery channels like E-Mails and screen savers to address time-sensitive cybersecurity problems that need immediate acknowledgement, while web based training via mobile learning platforms is well suited for targeting geographically diverse audiences.

4.4 Build up motivation to learn

To build up motivation to learn for trainees, it is important to create a positive learning environment in training sessions. One component of a positive learning enviroment is the way in which learning objectives are communicated. Common, non-technical language as well as non-technocratic, two-way communication proved to be most effective at raising IS compliant behaviour (Bauer et al. 2017,153). Directive messages, however, fostered mistrust and detachment from employees regarding IS activities (Bauer et al. 2017, 155).

The language used in trainings should also be comprehensible for as many trainees as possible. For that, it should be adapted to the skill level of trainees. Since most of the cybersecurity or information security trainings in organisations are developed by IT professionals, some suffer from lacking technical knowledge of non-IT employees and thus from a lack of comprehensibility (Aldawood/Skinner 2019). The language used should be concise and easy to comprehend for non-technical users, while not frustrating technical users (Abawaji 2014, 243).

4.5 Motivate individuals to perform skills and knowledge through training actions

Training actions should be designed in a way, that they foster trainees' motivation to perform the skills and knowledge they learn during trainings in real-life situations. For that, firstly neutralization techniques of employees must be addressed adequately. All users should be motivated not to use neutralization techniques like "appeal to higher loyalty" (other, potentially conflicting business objectives such as customer satisfaction are more important than cybersecurity), "defence of necessity" (cybersecurity behaviour is not possible because of high customer satisfaction priority and high workload) or "denial of injury" (believing that nobody will be harmed anyway, Bauer et al. 2017, 154).

Additionally, trainees often do not feel important enough for cybersecurity or simply are not emotionally engaged. For that, training actions should counter the feeling of lack of self-importance (Aldawood/Skinner 2019, 6) and enhance trainees' emotional involvement in IS activities through role plays, quizzes or informal training setting expansions (Bauer et al. 2017, 155).

4.6 Build in evaluation and assessment mechanisms

Aldawood and Skinner (2019, 9) emphasize the importance of integrating assessment mechanisms into cybersecurity trainings in organisations. Within these assessments, employees that pose a high risk for the cybersecurity of the organisation should be identified and specific training sessions should be designed for them (ibid.). As a result, the trainings can be specifically tailored to the needs of the organisation and its employees, which can help save training costs (ibid, 10).

Based on evaluations, improvements can be implemented regularly, whereby cycle models are favourable (Bauer et al. 2017, 153). Bauer et al. also propose evaluation possibilities like using honey pots to measure compliant or fraudulent behaviour or social engineering penetration tests (handling fake phishing mails, pace phone calls and face artefacts like USB sticks). We want to state though, that the latter evaluation techniques are problematic in some ways. If employees are made aware of being randomly exposed to fake incidents, they may start to believe that compliant behaviour is not all too important, since all is fake. Thus, they may not react to a real incident with care.

The ISCA from da Veiga and Martins (2015) shows that longitudinal cross-section assessments are not suited to the evaluation of progress in information security culture building. Assessing information security culture or behaviour via questionnaires as done by an ISCA-framework (da Veiga/Martins 2015, Da Veiga/Eloff 2010, Tryfonas/Fagade 2016) or the HAIS-Q (Pattinson et al. 2017, Parsons et al. 2014) might work well for assessing awareness, but an increased level of awareness does not necessarily result in increasing incidence of desirable cybersecurity behaviour. Perhaps employees have learned to fill out the questionnaires “properly”, so they would not be annoyed with further information security compliance interventions. Presumably, previous training might have taught employees to answer the questionnaire in such a way as to avoid further training.

Due to the survey design of da Veigas and Martins assessment (2015), using longitudinal cross-sectional data but not panel data, it could not be ensured that the same persons get assessed every year. Because of the rapid growth of the organisation it is highly likely that each sample after 2007 contains many new employees that did not complete the survey before. Thus, improvements may hardly be inferred from this data, as the inconsistent fluctuations in information security dimensions over time show (see da Veiga/Martins 2015, 170). However, regarding the privacy of the employees, the longitudinal non-panel-design is clearly favourable.

4.7 Integrate Management in Cybersecurity Trainings

Focussing training actions only on employees might not be effective, since management might not be aware of accurate workplace related conditions counteracting the performance of gained skills and knowledge. Youngkeun Choi and Tewjong Yoo (2014) found that employees’ compliance intentions in three Korean banks were significantly affected by Human Resource Management (HRM) practices. They argue that employees form their willingness to comply with an organisations Information Security Policy (ISP) based on their perception of the organisation as a social exchange partner, and based on the laws of reciprocity of interaction (Choi/Yoo 2014, 11). Depending on the treatment employees receive from their employer, their attitude towards the organisation is shaped. If they perceive their employer as acting benevolent, they are more likely to act benevolent in response and show ISP compliant behaviour (ibid.). Choi and Yoo (2014) emphasize the importance of reciprocity-enhancing HRM procedures around the implementation of these trainings. Trainings are not conducted in isolation, they happen within the context of the organisation and its HRM practices, such as the form of appraisal and reward structures. Most effective in supporting ISP compliance intentions were development-oriented appraisals, where employees’ performance was evaluated based on their achievements over a fixed period of time and future goals were derived from that evaluation, as well as just financial reward structures within the banks as well as in comparison to sector norms (Choi/Yoo 2014, 13). Among employees, these HRM practices fostered trust in reciprocity towards their employers and strengthened their positive attitude towards ISP compliance, even though they were not directly addressed in training actions. Thus, management should be encouraged to implement such commitment-based HRM practices rather than command-control-practices to establish a corporate culture in which cybersecurity trainings can unfold their effectiveness optimally (ibid., 14).

For our training actions, Choi and Yoo's findings have several implications. First, it is important to create a positive organisational environment for the performance of cybersecurity competence. For that, the recommendations for the formation of a cybersecurity culture can be applied. Like Knapp et al. already found in 2007, performing continuous training actions would be the means in place for that goal. Pattinson et al. (2014, 187) recommend establishing organisation wide cybersecurity learning practices in line with the setup of a learning and development division.

Second, people have to be made aware, that cybersecurity is a joint effort, not only an individual one. For that, Brilingaitė et al. (2020) proposed the enhancement of team building through the training setup, Aldawood and Skinner (2019, 10) recommend training people on collaborative incident response.

Third, workplace-related obstacles in performing cybersecurity competence have to be addressed. Management should have a look on workload, pressure and stress of their employees, since too much of these can counteract cybersecurity behaviour. People are frequently too stressed to perform learning activities in addition to their challenging job demands (work pressure, serious deadlines, workload, performance measures) (Aldawood/Skinner 2019, 5-6). If under pressure, employees suffer from a lack of attention towards the training action (ibid., 6). For effective trainings, workload, pressure and stress have to be reduced to a manageable level for employees, while at the same time keeping the time participants spend on training actions as short as possible (Abawaji 2014, 243). Since fear of change might pose a strong stressor to employees too, HRM practices might be used that reduce this stressing factor. Da Veiga and Martins (2015) strongly recommend employing a stress-conscious managerial perspective on change management, training and awareness programmes to improve information security policy compliant behaviour and thus induce a culture of information security (ibid., 172).

Last, as Cybersecurity trainings are usually conducted by HRM, the findings of Choi and Yoo point to the importance of trustworthiness of the implementation process of the trainings. The findings of Choi and Yoo suggest that sincerity and trustworthiness are the leading principles of the design and implementation of cybersecurity trainings, if they should at least influence the intentions of employees to perform secure behaviour positively. Lowry et al. (2015) also underline the importance of organisational trust and respectful communication in training actions against computer abuse. Monitoring employees for cybersecurity compliant behaviour could, if implemented incorrectly, invade their privacy (De Bruin/Janssen 2017, 4) and may be perceived as counteracting a positive cybersecurity culture that safeguards the civil rights of all actors involved.

5 References

Abt C.C., *Serious Games*, University Press of America, Lanham/London, 1987.

Albrechtsen E., Hovden J., ‘Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study’, *Computers & Security*, Vol. 29, 2010, P. 432-445.

Arachchilage N.A.G., Love S., ‘Security awareness of cumputer users: A phishing threat avoidance perspective’, *Computers in Human Behavior*, Vol. 28, 2014, p. 304-312.

Arnold, R., Nolda, S., Nuissl, E., ‘Kompetenz’, *Wörterbuch Erwachsenenbildung*, Klinkhardt, Bad Heilbrunn, 2010, 172-173.Ashenden D., Sasse A., ‘ CISOs and organisational culture: their own worst enemy? *Computers & Security*, Vol. 39, 2013, p. 396-405.

Aurigemma S., Mattson T., Deterrence and punishment experience impacts on ISP compliance attitudes’, *Information & Computer Security*, Vol. 25, No. 4, 2017, p. 421-436.

Baptista G., Oliveira T., ‘Gamification and serious games: A literature meta-analysis and integrative model’, *Computers in Human Behavior*, Vol 92, 2019, p. 306-315.

Bauer, S., Bernroider, E.W.N., Chudzikowski, K., ‘Prevention is better than cure! Designing information security awareness programs to overcome users’ non-compliance with information security policies in banks’, *Computers & Security*, Vol. 68, p. 145-159.

Barlow J.B., Warkentin M., Ormond D., Dennis A.R., ‘Don’t make excuses! Discouraging neutralization to reduce IT policy violation’, *Computers & Security*, Vol. 39, 2013, p. 145-159.

Baxter R.J., Holderness D.K.Jr., Wood D.A., *The effects of gamification on corporate compliance training: A field experiment of True Office Anti-Corruption Training Programmes*, preprint 2016, electronically available at: http://ssrn.com/abstract=2766683 (14.01.2020)

Beckers K., Pape S., Fries V., ‘HATCH: Hack And Trick Capricious Humans – A serious game on social engineering’, *Proceedings of British HCI Conference Fusion*, 2012, Bournemouth, UK.

Brilingaitė A., Bukauskas L., Juozapavičius A., ‘A framework for competence development and assessment in hybrid cybersecurity exercises’, *Computers & Security*, Vol. 88, p. 1-13.

Caballero A., ‘Security Education, Training and Awareness’, *Computer and Information Security Handbook*, Elsevier, 2017, p. 497-505.

Carlton M., Levy Y., Ramin M., ‘Mitigating cyber attacks through the measurement of non-IT professionals’cybersecurity skills’, *Information & Computer Security*, Vol. 27, No. 1, 2019, p. 101-121.

Carlton M., Levy Y., Ramin M., Terrell S., ‘Development of the MyCyberSkills TM iPad App: A scenario-based, hands-on measure of non-IT professionals’ cybersecurity skills’, *WISP 2015 Proceedings*, Association for Information Systems Electronic Library (AISeL), 2016.

Cheng L., Li Y., Li W., Holm E., Zhai Q., ‘Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory’, *Computers & Security*, Vol. 39, 2013, p. 447-459.

Cone B.D., Irvine C.E., Thompson M.F., Nguyen T.D., ‘A video game for cyber security training and awareness’, *Computers & Security*, Vol. 26, 2007, p. 63-72.

Connolly T.M., Boyle E.A. , MacArthur E., Hainey T., Boyle J.M., ‚A systematic literature review of empirical evidence on computer games and serious games‘, *Computers & Education*, Vol. 59, No. 2, 201, p.661 -686.

Conte de Leon D., Goes C.E., Haney M.A., Krings A.W., ‘ADLES: Specifying, deploying, and sharing hands-on cyber-exercises’, *Comptuers & Security*, Vol 74, 2018, p. 12-40.

D’Arcy J., Hovav A., Galletta D., ‘User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach’, *Information Systems Research*, Vol. 20, No. 1, 2009, p. 79-98.

Da Bruin A., Eloff J.H.P., ‚An information security governance framework‘, *Information Systems Management*, Vol. 24, No. 4, 2007, p. 361-372.

Da Veiga A., Martins N., Eloff J.H.P., ‚Information security culture – validation of an assessment instrument‘, *Southern African Business Review*, Vol. 11, No. 1, 2007, p. 147-166.

Da Veiga A., Eloff J.H.P., ‚A framework and assessment instrument for Information Security Culture‘, *Computers & Security*, Vol. 29, 2010, p. 196-207.

Da Veiga A., Martins, N., ‘Improving the information security culture through monitoring and implementation actions illustrated through a case study’, *Computers & Security*, Vol. 49, 2015, p. 162-176.

De Bruin, H., Janssen, M., ‘Building cybersecurity awareness: The need for evidence-based framing strategies’, *Government Information Quarterly*, Vol. 34, 2017, p. 1-7.

Deterding S., Dixon D., Khaled R., Nacke L., ' From game design elements to gamefulness: Defining "gamification"'. Lugmayr A. (Ed.), *Proceedings of the 15th International Academic Mindtrek Conference: Envisioning Future Media Environments, ACM*, New York, p. 9-15.

Devers C.J., Gurung R.A., 'Critical perspective on gamification in education', *Gamification in Education and Business*, Springer, 2015, p. 417-430 .

DoD – US Department of Defense, Defense Information Systems Agency, *'CyberProtect'*, 1999.

Dodge Jr. R.C., Carver C., Ferguson A.J., 'Phishing for user security awareness', *Computers & Security*, Vol. 26, 2007, p. 73-80.

Eminağaoğlu M., UçE., Eren S., 'The positive outcomes of information security awareness training in companies – A case study', *Information Security Technical Report*, Vol. 14, No. 4, 2009, p. 223-229.

Fagade T., Tryfonas T., 'Security by compliance? A study of insider threat. Implications for Nigerian banks', *Tryfonas T. (Ed.), Human aspects of information security, privacy, and trust,* Springer, 2016, p. 128-139.

Furtună A.,Patriciu V.V., Bica I., 'A structured approach for implementing cyber security exercises', *8th International Conference on Communications, IEEE*, 2010, p. 415-418.

Ganin A. A., Quach P., Panwar M., Collier Z. A., Keisler J. M., Marchese D., Linkov I., 'Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management', Risk Analysis, September 2017, p. 1-27.

Gaunt N., ‚Practical approaches to creating a security culture', *International Journal of Medical Informatics*, Vol. 60, No. 2, 2000, p. 151-157.

Ghafir I., Saleem J., Hammoudeh M., Faour H., Prenosil V., Jaf S., Jabbar S., Baker T., 'Security threats to critical infrastructure: The human factor', Journal of Supercomputing, Vol 74, No. 10, 2018, p.4986-5002.

Hamari J., Koivisto J., Sarsa H., ‚Does gamification work? A literature review of empirical studies on gamification', *47th Hawaii International Conference on System Sciences*, Hawaii, USA, 2014.

Herath T., Rao H.R., ‚Encouraging information security behaviours in organizations: role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, Vol. 47, 2009, 154-165.

Herold R., *Managing an information security and privacy awareness and training program*, Boca Rotan, CRC Press, 2011.

Hu Q., Xu Z., Dinev T., Ling H., 'Does deterrence work in reducing information security policy abuse by employees?', *Communications of the ACM*, Vol. 54, No. 6, 2011, p. 54-60.

Ifinedo P,. 'Information systems security compliance: an empirical study of the effects of socialization, influence, and cognition', *Information and Management*, Vol. 51, 2014, p. 69-79.

ISO/IEC 27002:2013, *Information technology – security – techniques – code of practice for information security management*, 2013.

Jansson K., von Solms R., 'Phishing for phishing awareness', *Behaviour & Information Technology*, Vol. 32, No. 6., 2013, p. 584-593.

Jin G., Tu M., Kim T-H., Heffron J., White J., 'Evaluation of Game-Based Learning in Cybersecurity Education for High School Students', J*ournal of Education and Learning (EduLearn)*, Vol. 12, No. 1, 2018, p. 150-158.

Johnston A.C., Warkentin M., Siponen M., 'An enhanced fear appeal retorical framework: Leveraging threats to the human asset through sanctioning rhetoric', *Management Information System Quarterly*, Vol. 39, No. 1, 2015, p. 113-134.

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

Koivisto J., Hamari j., ‚The rise of motivational information systems: A review of gamification research', *International Journal of Information Management*, Vol.45, 2019, p 191-210.

Kurtz, T., 'Der Kompetenzbegriff in der Soziologie'. Kurtz, T., Pfadenhauer. M. (ed), *Soziologie der Kompetenz*, Verlag für Sozialwissenschaften, Wiesbaden, 2010, p. 7-28.

Le Compte A., Watson T., Elizondo D., 'A renewed approach to serious games for cyber security', 7th International Conference on Cyber Conflict: Architecture in Cyberspace, Maybaum M., Osula A.-M., Lindström L. (Eds.), *NATO CCD COE Publications*, Tallin, 2015.

Luh R., Temper M., Toja S., Schrittwieser S., Janicke H., ‚PenQuest: A gamified attackier/defender meta model for cyber security assessment and education', *Journal of Computer Virology and Hacking Techniques*, 2019, p. 1-43.

Mamonov S., Benbunan-Fich R., 'The impact of information security threat awareness on privacy-protective behaviors', *Computers in Human Behaviour*, Vol. 83, 2018, p. 32-44.

Martens B., Aguiar L., Gomez-Herrea E., Mueller-Langer F., The digital transformation of news media and the rise of disinformation and fake news, *JRC Digital Economy Working Paper 2018-02*, 2018, see https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf

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

Nagarajan A., Allbeck J.M., Sood A., Janssen T.L., 'Exploring game design for cybersecurity training', *Cyber Technology in Automation, Controll and Intelligent Systems (CYBER)*, 2012 IEEE International Conference proceedings, p. 256-262.

Nosworthy J.D., , Implementing information security in the 21st century – do you have the balancing factors?', *Computers & Security*, Vol. 19, No.4, 2000, p. 337-347.

Novak E., ‚Toward a mathematical model of motivation, violation, and performance', *Computers & Education*, Vol. 74, 2014, P. 73-80.

Parsons K., McCormac A., Butavicius M., Pattinson M., Jerram C., ‚Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, Vol. 42, 2014, p. 165-176.

Parsons K., McCormac A., Butavicius M., Ferguson L., *Command human factors and information security: individual, culture and security environment*. Control, Communications and Intelligence Division, Defence Science and Technology Organisation, 2010.

PCI DSS, Payment Card Industry Security Standards Council, *PCI Data Security Standard*, 2014.

Pekrun R., Linnenbrink-Garcia L., ‚Academic emotions and student engagement'. In: Christensen N.S.L., Reschly A.L., Wylie C. (eds.), *Handbook of Research on Student Engagement*, Springer, New York, p. 259-282.

Pfadenhauer, M., 'Kompetenz als Qualität sozialen Handelns'. Kurtz, T., Pfadenhauer. M. (ed), *Soziologie der Kompetenz*, Verlag für Sozialwissenschaften, Wiesbaden, 2010, p. 149-172.

Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V., Wu Q., 'A survey of game theory as applied to network security', *43rd Hawaii International Conference on System Science (HICSS)*, 2010, *IEEE*, p. 1-10.

Safa N.S.; Sookhak M., VonSolms R., Furnell S., Ghani N.A., Herawan T., 'Information security conscious care behavour formation in organizations', *Computers & Security*, Vol. 53, 2015, p. 65-78.

Sailer M., Homner L., 'The gamification of learning: A meta-analysis', *Educational Psychology Review*, Vol. 31, No. 1, 2020, p. 77-112.

Schatz D., Bashroush R., Wall J., 'Towards a more representative definition of Cyber Security', *The Journal of Digital Forensics, Security and Law*, Vol. 12, No. 2, 2017, p. 53-74.

Thomson K., Von Solms R., 'Information security obedience: a definition', *Computers & Security*, Vol 24, No. 1, 2005, p. 69-75.

Siponen M., Puhakainen P., Vance A., 'Can individuals' neutralization techniques be overcome? A field experiment on password policy', *Computers & Security*, Vol. 88, 2020, p. 1-12.

Talib Y.A., Dhillon G., 'Employee ISP compliance intentions: An empirical test of empowerment', *Proceedings of the International Conference on Information Systems*, Fort Worth, TX, December 12-16, 2015.

Terlizzi M.A., de Souza Meirelles F., Viegas Cortez da Cunha M.A., 'Behaviour of Brazilian bank employees on Facebook and the cybersecurity governance', *Journal of Applied Security Research*, Vol. 12, No. 2, 2017, p. 224-252.

Thio J.-N., Mina M., Jacobson D.W., 'Cyber security training a survey of serious games in cyber security', *IEEE Frontiers in Education Conference (FIE)*, 2017.

Thomson K., Von Solms R., Louw L., 'Cultivating an organisational information security culture. *Computer Fraud & Security*, October 2006, p.7-11.

Thornton D., Francia III G., 'Gamification of information systems and security training: issues and case studies', *Information Security Education Journal*, Vol 1, No. 1, 2014, p. 16-24.

Vasileiou I., Furnell S*., Cybersecurity Education for Awareness and Compliance*, IGI Global, Hershey, PA, 2019.

Von Solms R., Von Solms B., ‚From policies to culture‘, *Computers & Security*, Vol 23, 2004, p. 275-279.

Vroom C., Von Solms R., ‚Towards information security behavioural compliance‘, *Computers& Security*, Vol. 23, No. 3, 2004, p. 191-198.

Witman M.E., Mattord H.J., ‘Principals of information security’, *Cengage Learning*, Boston, MA, 2018.

Wong W.P., Tan H.C., Kim H., Tseng M.-L., ‘Human factors in information leakage: Mitigation strategies for information sharing integrity’, *IMDS*, Vol 119, No. 6, p. 1242-1267.