Jemina Lakka-Kolari

PEDAGOGICAL ASPECTS IN CYBER SECURITY TRAININGS OFFERED BY PRIVATE COMPANIES

MASTER’S THESIS

TIIVISTELMÄ

Lakka-Kolari, Jemina
Pedagogiset aspektit yksityisten yritysten tarjoamissa kyberturvallisuuskoulutuksissa
Jyväskylä: Jyväskylän yliopisto, 2021, 59 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Yritykset ja organisaatiot ovat yhä häikäilemättömämpien kyberiskujen kohteena. Moni yritys onkin huomioinut tämän kasvavan riskin, ja tästä syystä panostanut turvallisuuden lisäämiseen. Heikoimpana lenkkinä kyberturvallisuudessa on tunnetusti ollut ihminen. Tästä syystä yritykset ja organisaatiot ostavatkin koulutuksia valistaakseen työntekijöitään minimoidakseen omia riskejään. Vastauksena tähän kysyntään moni yksityinen yritys on alkanut tarjoamaan maksullisia kyberturvallisuuteen liittyviä koulutuksia. Tässä tutkielmassa käsiteltiin yksityisten yritysten tarjoamia kyberturvallisuuskoulutuksia. Ilmiötä lähestyttiin pedagogiikan kautta, ja tarkoituksena oli tunnistaa yrityksien käyttämiä pedagogisia aspekteja. Näitä aspekteja reflektoitiin kyberturvallisuuskoulutuksen sekä aikuiskoulutuksen viitekehyksiin, jotta saatiin kattava käsitys näiden aspektien sopivuudesta kyberturvallisuuden alalle sekä aikuisten kouluttamiseen. Empiirinen aineisto kerättiin viideltä yritykseltä verkkokyselyllä. Ainoa kriteeri yritykselle oli, että he tarjoavat kyberturvallisuuskoulutusta Suomessa. Muilla tekijöillä, kuten yrityksen koolla tai koulutuksen sisällöllä, ei ollut merkitystä. Kysely toteutettiin hyödyntäen sekä laadullisia että määrällisiä kysymyksiä, jotta kyettiin saamaan kattava käsitys yrityksien koulutusten pedagogiikasta. Täten tutkimus toteutettiin mixed method-tyylillä. Tutkimuksessa selvisi, että yritykset lähestyivät koulutuksia kolmesta eri näkökulmasta: (1) opiskelijalähtöisyys, (2) sisältölähtöisyys, sekä (3) ostajalähtöisyys. Tämän lisäksi yritykset hyödynsivät monenlaisia menetelmiä opetuksessa. Nämä metodit sekä lähestymistavat sopivat hyvin sekä kyberturvallisuuden että aikuiskasvatuksen viitekehyksiin. Asioita, jotka tunnistettiin olevan ristiriidassa määriteltyjen viitekehysten kanssa, olivat mm. kouluttajan rooli oppimisprosessissa sekä koulutuksen tehokkuuden mittaristo. Tutkimusta ei suoraan voida nähdä validioivan yksityisten yritysten koulutuksien tehokkuutta, mutta sitä voidaan hyödyntää tulevaisuudessa tällaista tehokkuutta mittaavan tutkimuksen teossa.

Asiasanat: kyberturvallisuuskoulutus, aikuiskasvatus, tietoturva, pedagogiikka

ABSTRACT

Lakka-Kolari, Jemina
Pedagogical Aspects in Cyber Security Trainings Offered by Private Companies
Jyväskylä: University of Jyväskylä, 2021, 59 p.
Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

Companies and organizations are increasingly subject to unscrupulous cyber threats. Many companies have acknowledged this growing risk, as well as invested in increasing safety. The weakest link in this security has identified to be humans. For this reason, companies and organizations are willing to train their employees to minimize their own risks. This has been noted as a business opportunity and many private companies are now offering paid cybersecurity trainings. This dissertation dealt with cybersecurity training provided by private companies. The phenomenon was approached through pedagogy, with the aim of identifying the pedagogical aspects used by companies. These aspects were reflected on the frameworks of cybersecurity education and adult education in order to gain a comprehensive understanding of aspects' suitability to teach in the field of cyber security as well as adults. Empirical data was collected from five companies through an online survey. The only criterion for the company was that they offer cyber security training in Finland. Other factors, such as the size of the company or the content of the training, were not taken into consideration. The survey was conducted using both qualitative and quantitative questions in order to gain a comprehensive understanding of the pedagogy used by the companies. Thus, the study was conducted as a mixed method research. The study found that companies approached training from three different angles: (1) student-oriented, (2) content-oriented, and (3) customer-oriented. In addition to this, companies utilized a wide variety of methods in teaching. These methods and approaches fit well into the frameworks of both cybersecurity and adult education. Issues that were seen to be contradicted to the defined frameworks included the role of the educator in the learning process and the metrics for the effectiveness of the education. The research cannot be directly seen to validate the effectiveness of private company training, but it can be used in the future to conduct research measuring such effectiveness.

Keywords: cyber security training, adult education, information security, pedagogy

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

As digitalization is becoming to effect more and more ordinary peoples' everyday lives, the risks related to it are also becoming more acknowledged. The acknowledgement itself has been noted to be insufficient as companies and organizations, regardless of their operating field, are becoming to be the targets of different types of cyberattacks. This has led to the phenomenon of private companies offering different types of cyber security trainings. The trainings are meant to target the weakest link in cyber security, which is perceived to be the humans (Puhakainen, 2006). Still, some studies suggested that 1 out of 5 fell for phising emails even after going through security training (C, Ruth 2020).

In Finland, the supervising organization for cybersecurity on national level is National Cyber Security Center, which operates under Finnish Transport and Communication Agency. Their tasks include providing situational awareness on cyber security and monitoring the security of communication networks. One of the services they provide is in regards to cyber security trainings and exercises. They provide a list of companies operating in Finland that are able to train the target company on cyber security. To be able to get to the provider list, there are no special requirements. The Center only checks that the company is a "known expert" on cyber security based in Finland and that they have some sort of training materials. There are no stated pedagogical requirements or requirements for the providing company to prove that their training is, in fact, efficient in either skills or knowledge building regarding cyber security.

It is the contention of the thesis that such lack of requirements is problematic. The trainings do not have any official guidelines or standards that they should meet in order for them to be proved to be efficient. When no real evaluation criterion is given as to what counts as good or bad training, the trainings could be insufficient in teaching skills and knowledge about cyber security. This lack of requirements might not be a problem now, but as more actors are coming to the training industry, the need for requirements is relevant. In addition to the lack of stated requirements for good training, cyber security trainings offered by private companies may also lack evidence on their effectiveness. This lack of research and surveillance is something that the European Union Agency for Network and Information Security has already addressed in 2015 (ENISA 2015).

This research will examine the phenomenon of private companies' cyber security trainings, and it will do it from the perspective of pedagogy. This will give the understanding of what is happening at the training field without any pedagogical requirements. The main research questions are:

1) What pedagogical aspects can be found from the private companies' cyber security trainings?
2) How these aspects fit in with the frameworks of cyber security education and adult pedagogy?

With these questions, the goal is to understand how training companies approach the trainings and what pedagogical methods are in use. Pedagogical aspects were chosen as the main interest point, as they can reveal how the companies perceive training, the training content, and the learner. These are important to identify as they will then help to understand the phenomenon of private companies offering training from the teaching and learning perspective. These identified pedagogical aspects will then be reflected upon the frameworks of cyber security education and adult pedagogy. This will give a better understanding of the phenomenon in relation to previous research.

The intention is to use this understanding in the future to study more on the effectiveness of the trainings and help in forming requirements regarding training methods. Thus, this research will not answer the questions whether these trainings are efficient or how the answered companies rate against each other. For the answered companies, this research will give the chance to see how the used methods reflect to the frameworks and possibly introduce new methods to take into practice.

The reason why both of adult education and cyber security training frameworks were chosen is due to the fact that together they will give a better understanding of the phenomenon. The reflection of the aspects to only one of those frameworks could lead to a bias. Cyber security framework was chosen as the field of training is cyber security. On the other hand, ss the provided trainings studied in this research are targeted for other companies and organization, adult education was chosen to be the other framework. It will give better understanding of teaching adults in organizational context. Also, as the field of cyber security can be seen as relevantly new, adult education framework might include some aspects that are not present in cyber security. With the use of both frameworks, the possibility of missing out something relevant, is minimized.

First this research will identify the frameworks of cyber security training and adult education. As cyber security as a field can be seen as relevantly new, research on information security training has also been used to build the framework. Information security and its trainings have been actively researched for few decades. Still, the field is noted to lack in research where both theory and empirical evidence are incorporated. Because of this lacking, this research will mainly only focus on research that has both of these present. The studies of Puhakainen (2006) *"A Design Theory For Information Security Awareness"* and Karjalainen (2011) *"Improving Employees' Information Systems (IS) Security Behavior Toward A Meta-Theory of IS Security Training And A New Framework For Understanding Emploees' Is Security Behavior"* are presented as the most relevant research, which will be used as the basis for the cyber security framework. In addition to using academic research to build this framework, different guidelines will also be used to broaden the understanding.

Also, in cyber security framework, the distinction between cyber security training and cyber security exercises was made. This was due to the fact that exercises can be perceived to have different pedagogical requirements. Also, doing and organizing exercises can be seen to need resources that not all companies are capable to have. Thus, this research will only focus on trainings in the empirical part. Still, as the exercises can also be identified to have a crucial role in teaching cyber security, they will also be introduced in the framework. This distinction can be seen to be relevant especially in possible future research.

In adult education framework, andragogy and self-directed learner theories are used first to identify the adult learner. Then two learning theories, transformative learning and experiential learning, are showcased. The reason why these two learning theories were chosen, is due to the fact that they are the most popular when explaining adult learning and they have also been used in the context of cyber security. Thus, they can be seen proper to explain whether the aspects found in the empirical part are relevant. In addition, learning at workplace will also be introduced.

The empirical data was collected from five different companies providing their services in Finland. The companies vary in size and in their training offering. The companies answered an online questionnaire that was sent to them by email. The questionnaire had 20 questions, and they were both open-ended and close-ended. As the aim of the research is to understand the training phenomenon, mixed method research was used as the main methodology. This will allow to fully study the phenomenon from both qualitative and quantitative perspectives, and the perspectives give validation for each other in the analysis. The main focus was on the open-ended questions, thus qualitative analysis will be emphasized. Still, as the answers were analyzed at the same time, the research can be identified as mixed method. The open-ended questions were analyzed with content analysis method with theory-guided approach.

The pedagogical aspects were perceived from three different perspectives: learning principles, learning situation and after learning. The research found that many of the companies used and approached learning from pedagogical aspects that could be found from both cyber security and adult education frameworks. One aspect that was not found from either cyber security framework or the empirical data was the enhanced role of facilitator, which is emphasized in adult education framework.

In regards to the structure of this research, first the frameworks of cyber security training and adult education will be introduced. After these, the empirical data and the methodology will be showcased and explained. This will follow a section where the results from the empirical data will be reflected on the frameworks presented at the beginning. A discussion part will finish this research, where the reliability and validity are deliberated. Also, future research implications will be presented there.

2 LEARNING CYBER SECURITY

This chapter’s purpose is to introduce the framework of cyber security training. It will answer the questions on what cyber security training is, why it is important and how it is guided. To answer these questions, extensive literature review has been done. Literature review was chosen as the method for this section, as it gives the possibility to systematically collect and synthesize previous research. It is an effective method in regards to fragmented study fields, where knowledge production is forming at an accelerated speed. Literature review also gives the possibility to answer research questions with knowledge deriving from multiple studies rather than just one. Thus, the answers can then be seen as more valid. (Snyder, 2019)

2.1 Security in Cyber Domain

Cyberattacks can be divided into three different categories depending on the target. Physical cyberattacks target physical aspects such as physical power sources, synthetic cyberattacks focus on computer logic, and sematic cyberattacks target the human interface. Sematic attacks are perceived to be the most dangerous attacks, as humans are seen to be the weakest link in security. For that reason, training is needed. (Aaltola & Taitto, 2019)

When studying cyber security trainings and their essence, information security field can be seen to have a major impact on it. Even though the term “cyber security” is relatively new, information security has been researched upon for decades. Decades of research on information security is generally relevant also for cyber security.

Assets can be seen as the main difference between these two fields. In information security, the asset is information, and the main goal is to secure it from possible harm. In cyber security, it is not that straightforward as the protection regards cyberspace itself, those who function in cyberspace, and any assets that could be reached via cyberspace. This is visible also in that, in information security, humans can be seen as a threat and a vulnerability. In comparison, in cyber security the perception is that humans are an asset needing protection. (Reid & Van Niekerk, 2014) Thus, information security can be seen as part of cyber security when asset is information, and it is accessible via cyber space.

Another difference between these two fields is about the security culture. Information security culture can be seen to form around the organization's culture, when the context is organizational. This means that it is relatively well-controlled environment with predictable user behavior and profile. In cyber security, the culture can be seen to be formed societally, and the users cannot be profiled in the same way as in information security. (Reid & Van Niekerk, 2014; Siponen, 2001)

As the empirical part of this research will focus on cyber security trainings targeted for organizations, cyber security can be perceived to have many of the same aspects as information security, such as the security culture forming around the organization's culture and the main security concern being the organization's assets, which are most likely information. For this reason, information security will play a crucial role in understanding cyber security trainings. Nevertheless, it is good to acknowledge that in other contexts, such as in cyber security exercises and trainings targeted for private people, another approach could be more useful.

2.2 The Purpose of Training

The concept of training is a debatable aspect both in the field of cyber security as well as in information security. It visible in the way terms such as education, training, awareness, and exercises are used overlappingly.

Institute of Standard (NIST) has published two guidelines *NIST SP 800-16* (1998) and *NIST SP 800-50* (2003), which assess how to build an efficient information security training model. Guideline 800-16 is the first to differentiate between awareness, training and education. Awareness is seen as a prerequisite to training, and education is seen as reserved only for IT specialists to fulfill their job requirements. Training, in the middle, is defined to strive to produce relevant and needed security skills and competences to other than IT security specialists. Learning is defined to be the action needed to move from one phase to another. (NIST SP 800-16, 1998). Also, guideline SP 800-50 differentiates awareness and training, as awareness could be seen to be guided with "What behavior do we want to reinforce?" and training "What skill or skills do we want the audience to learn and apply?". (NIST SP 800-50, 2003)

European Union Agency for Cyber Security (ENISA) was formed in 2004, with the goal of establishing high level cyber security across Europe. One way it promotes this is by supporting and organizing cyber exercises as well as promoting cyber security education. In 2012, it published a report on raising security awareness, which is mostly based on above mentioned NIST guidelines.

In the report, ENISA defined awareness to be the first component of an education strategy. Awareness is stated to consist of set of activities, and it occurs on an ongoing basis. According to ENISA, how awareness differs from training is that awareness campaigns are less formal and shorter. Training component relies on the skills built in awareness campaigns, and training as an event is more organized and seeks to teach participants. That is the reason why training programs need to be based on organization's learning objectives. (ENISA 2010).

So, these guidelines perceive that training is based on awareness, and the transition between these two stages is done by learning. Training is defined as an organized event, where skills and competences are built. In comparison to awareness, training is only for certain employees. Education is at the top of the pyramid, with only being relevant to IT professionals. Figure 1 illustrates this continuum.

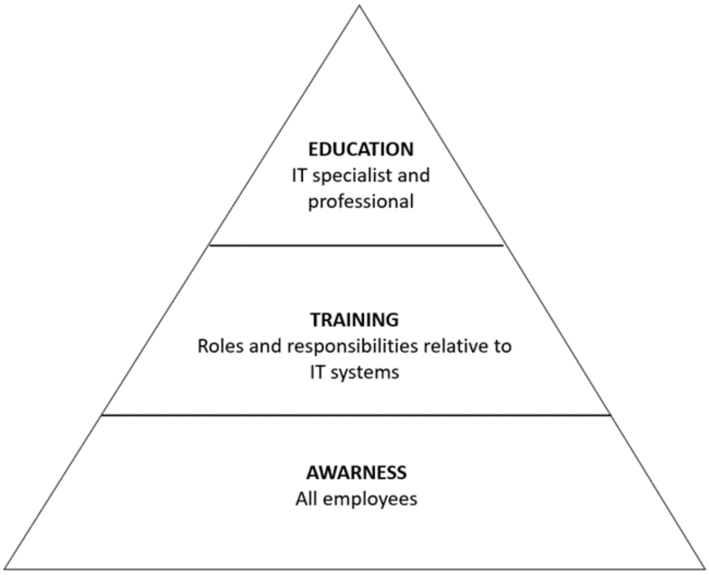

EDUCATION
IT specialist and professional
TRAINING
Roles and responsibilities relative to IT systems
AWARNESS
All employees

Figure 1 Learning Continuum based on NIST 800-16 (National Institute of Standards and Technology, 1998).

In academic research, Amankwa, Loock & Kritzinger (2014) have done an in-depth conceptual analysis on the differences between awareness, training and education. They found the core differences to be on the concepts' focus, purpose and methods of delivery. Training was defined by them to be any action that is taken to make sure that every employee is equipped with the necessary information security skills and knowledge. (Amankwa, Loock, & Kritzinger, 2014).

Karjalainen (2011), on the other hand, has found, based on Siponen et al. (2006), that information security training is persuasive and non-cognitive. She also states that IS security trainings have three existentialistic features, which are crucial for the training to be needed. These features are (1) existence of security-sensitive organizational asset, (2) threat towards them, and (3) different technical, social, and organizational mechanisms for protecting the organizations assets. (Karjalainen, 2011)

Another approach in using the concepts comes from Puhakainen (2006), who uses the term awareness training in his research. There awareness training is stated to be action intended to improve employees' information security behavior to comply with IS security policies and instructions. (Puhakainen 2006) Nykänen's (2011) definition can be seen to be in between these two definitions, as he does not use the term awareness training, but defined information security training to be action, in which the users' motivation, behavior, attitudes, and awareness regarding information security is improved and guided towards organizational security policies. (Nykänen, 2011)

As is visible, the usage of concepts is not clear, especially with awareness and training. Rather than making a clear distinction between these two, Puhakainen and Nykänen are combining awareness and training. This combination can be justified with the fact that in 1998 when NIST SP 800-16 was published, IT was still relevantly new aspect at workplace. This could then be the reason why only certain people who worked with IT needed to be trained instead of just being aware. Nowadays, IT is inevitably interlinked with all parts of work, and for that reason all employees can be perceived to have the need to be trained to have necessary skills regarding cyber security to secure assets.

In addition to awareness, training and education deriving from information security research, cyber security learning also consists of exercises. It is widely recognized that training and exercises are different approaches, but how they differ is debated. Aalto and Taitto (2019) have done a distinction between cyber security education, training and exercises. Education is, by them, perceived to be a phase, where basic understanding and knowledge is gained, which can then be used to develop skills. After education comes training, where skills are formed to gain certain competencies. Exercises are defined to be distinctly separate events, where organizations test their readiness for cyberattacks.(Aaltola & Taitto, 2019) Thus in this definition, exercises are seen as separate events, which are not directly linked to any learning continuum.

Hazivasilis, Ioannidis, Smyrlis et al. (2020) have formed another type of differentiation between cyber security trainings and exercises, where exercises are seen as more advanced level in the learning continuum. In their research, they make a distinction between basic training and advanced training. Basic training is defined to consist of lectures, awareness videos, tutorials and other educational material, which should be targeted for the general public. Advanced training uses emulated and/or simulated scenarios as teaching tools targeted for security experts Their division is based on Bloom's taxonomy knowledge pyramid. The first three steps, including third step applying, should be the goal in basic training. Then the three top steps are preserved for advanced training. (Hatzivasilis, Ioannidis, Smyrlis, et al., 2020).

2015 ENISA report on national and international cyber security exercises also makes a distinction between exercises and trainings. ENISA's terminology on exercises and trainings was based on ISO-22398 standard. The standard states that exercises are *"process to train for, assess, practice, and improve performance in an organization"*. Training is defined as *"activities designed to facilitate the learning and development of knowledge, skills, and abilities, and to improve the performance of specific tasks or roles"*. (ENISA 2015; International Organization for Standardization, 2013)

So, when information security is perceived to be a crucial part of cyber security due to organizational context, cyber security training could be stated to be actions of awareness raising and knowledge development, behavior and motivational changing, and skill building. The key difference between cyber exercises and trainings is that exercises are stated to be more focused on implementing previously formed knowledge and skills regarding cyber security, whereas training is meant for developing those knowledges and skills. Exercises can also be seen to have more distinguished communal learning objectives as they are focusing on the performance on organizational level, in comparison to trainings which focus on performance of specific tasks and roles. This cyber security learning framework is presented in Figure 2.

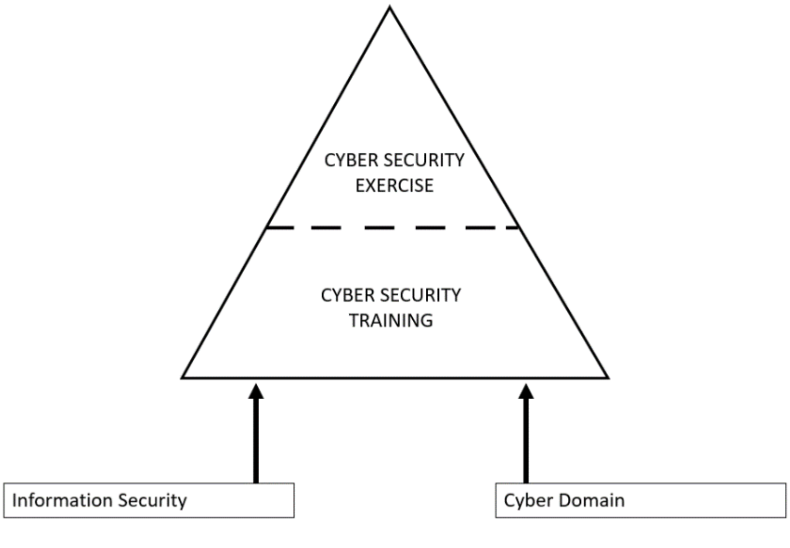


Figure 2 Cyber security training learning continuum

Now, even though cyber security exercises were left out on the empirical part, the concept and its methodologies will be introduced in the next sub-chapter, to give a better understanding of the whole cyber security learning process.

2.3 Cyber Security Exercises

Cyber exercises can be defined as: *"a planned event during which an organization simulates a cyber-disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption"* (Aaltola & Taitto, 2019). These exercises have mainly been seen and used as part of military training, but now more public and private organizations are using them to strengthen and build resilience towards cyberattacks. One reason for exercises' popularity growing, is the fact there are some indications that traditional training methods such as classroom lectures, home assignments and lab environment are not efficient enough to teach cyber security. The reason for this is that those methods do not showcase the full quantity and complexity of cyber domains. (Hautamäki, Karjalainen, Hämäläinen, & Häkkinen, 2019; Karjalainen, & Kokkonen, 2020)

There are many different types of methods to implement an exercise. On the basis of ISO-22398, different exercise methodologies have been introduced, and methods such as capture the flag, discussion-based game, red team blue team, seminar, simulation, tabletop and workshop are commonly known (Hautamäki, Karjalainen, Hämäläinen, & Häkkinen, 2019). The pedagogy in exercises is usually based on collaboration and simulation of real-life events. Simulation is a game pedagogy genre, where students are players with pre-set goals that need to be achieved. The game models either natural or man-made system or phenomena. (Karjalainen, & Kokkonen, 2020) Other types of games are also being used in the exercises, but it has been noted that most of the developed games were designed to be finished over a short period of time and in one session. This can be seen problematic, if one of the learning outcomes should be behavioral change. (Hendrix, Al-Sharbaz & Bloom, 2016)

The research in the area of cyber security exercises is also lacking the measurable effects of the learning outcomes. Especially regarding exercises targeted for security professionals. (Hendrix, Al-Sharbaz & Bloom, 2016) One suggestion to assess the learning outcomes of exercises were introduced by Karjalainen and Kokkonen (2020) who used Kirkpatrick's four level assessment framework to assess the exercises: (i) reaction, (ii) learning, (iii) behavior, and (iv) results. (Karjalainen, & Kokkonen, 2020)

Cyber security exercises are identified to have three distinct phases: (1) planning the scope and the objectives, (2) implementation, and (3) evaluation/feedback. In all the phases, pedagogical objectives should be taken into consideration. During the planning phase, the trainer specifies the pedagogical methods used based on the scope of the exercise and the involved security aspects. Also the elements, which will be simulated, will be defined in this phase. In regards to pedagogy, this is the most crucial phase as it determines the used platform. If the platform is not properly constructed to fulfill the learning needs, then rest of the phases will not be effective. (Hatzivasilis, Ioannidis, Smyrlis et al., 2020; Karjalainen, & Kokkonen, 2020).

In the implementation phase, the students try to manage through all the learning goals with the help of the trainer. The trainer's task is also to monitor the students and handle events and incidents. The implementation usually consists of problem solving, decision-making, analysis skills and situational awareness. At the end, the feedback phase is used to go through all the main exercise elements. In this phase, the students can reflect on their learnings and can ask questions. It is also important to distribute the training material afterwards to enhance post-practice learning. (Aaltola & Taitto, 2019; Hatzivasilis, Ioannidis, Smyrlis et al., 2020; Karjalainen, & Kokkonen, 2020)

The exercise platform, or cyber range, is proclaimed to be a crucial component in making exercises effective. When used and supervised properly, it can give safe environment to practice real-life intrusions and penetrations. Cyber domains are becoming increasingly complex, and for that reason forming proper platforms to practice on can be a challenge. Also, if the purpose of the training is on the competence building of the trainees, then choosing the right learning platform is crucial as too complex platforms can negatively impact the learning situation. (Hautamäki, Karjalainen, Hämäläinen, & Häkkinen, 2019) Different analyzing tools have been created to be used on the exercise platforms, which can measure human cognition or decision making based on eye tracking or use of mouse or keyboard. These measures can be used to indicate human performance and are usually used with quantitative methods and measures. (Aaltola & Taitto, 2019)

As one of the main essences of cyber security exercises is not only in training cyber security skills individually, but in giving organizations the chance to showcase how effective their procedures are in protecting their critical information, services and assets, these also need to be taken into consideration when evaluating the exercises' efficiency. (Hautamäki, Karjalainen, Hämäläinen, & Häkkinen, 2019) Exercises also encourage organizational management to test different tactics, so the evaluation needs to take this type of communal learning into account. For this reason, formative assessment should be used as the evaluation of learning activities that guide the exercises and help to see whether learning goals have been meat. (Aaltola & Taitto, 2019; Karjalainen, & Kokkonen, 2020)

There are different international guidelines made on exercises such as ENISA 2015. Also national guidelines have been formed, and example of this is Finland's National Cyber Security Center's guidelines. For example, the Center has published a guide for organizations regarding cyber exercises. It defines exercise to be a controlled situation where processes are evaluated. The guide showcases different cyber exercises and explains what different steps are needed to implement them efficiently. The exercise form is based on the report on a three stage model: (1) plan, (2) implement, and (3) analyze. The guideline also suggests that multiple small-scale exercises should be organized during the year as it can be easier than to organize one massive exercise once a year. Getting an outsider to organize the exercise is encouraged, as the guideline states that the planning phase can otherwise take too much of the employees time. (Traficom, 2019)

2.4 Formation & Delivery

In the academic field, for example Karjalainen (2011) and Puhakainen (2006) have done extensive literature review regarding information security training studies. These reviews showcased how differently trainings have been studied and viewed. Karjalainen identified seven different contextual approaches used in the literature. These approaches were: (1) Psychological training approach, (2) Training approaches based on learning theories, (3) Security awareness program approaches, (4) Process approaches, (5) Situational approaches, (6) Social engineering preventive approaches, and (7) Computer-based training approaches. (Karjalainen, 2011) Puhakainen found in his study that previous research could be divided into two categories depending on how they perceived user behavior could be influenced. The two categories identified were cognitive approaches and behavioral approaches. (Puhakainen, 2006) Both of them acknowledged that previous research could not be used to answer the question on how to form an effective training, due to different reasons such as lack of empirical evidence or the lack of proper usage of the theories.

The question of how to build an effective cyber security training is not a simple one, due to training's complex nature with goals of knowledge and skill building to behavioral change. The problem is also in the lack of proper academic research done on the matter, both in information and cyber security fields. Many of the research studies done are either only solely based on empirical evidence, lacking theory or only based on theory without empirical validation (Puhakainen, 2006). Especially the lack of pedagogical theories used to explain the effectiveness has been noted (Puhakainen & Siponen, 2010). The problem has also been, that the studies are done on many different levels ranging from meta-theories to practical guides.

Because of the disunity of the field, this sub-chapter will first introduce different guidelines regarding training designing. After that, two academic studies will be introduced. These academic studies represent different perspectives on the forming of effective trainings, and they are both empirically confirmed as well as theoretically supported. Thus, they should give a reliable and broad understanding on how to form effective trainings, with all the training goals taken into account.

2.4.1 Guidelines

Different guidelines have been made to give practical instructions on how effective trainings should be formed. The oldest, NIST SP 800-16 (1998), bases its training effectiveness on andragogy, where adult learners' uniqueness regarding values, beliefs and opinions are noted. It also proclaims that using the suggested type of training will be intermediate in regards to impact timeframe. The guideline states that the trainees job functions and different levels of knowledge are aspects that need to be taken into consideration when planning and executing the training. The learning objectives should be learning new skills and answering the question "How". Example teaching methods introduced were practical instructions such as lectures, case studies and hands-on practices. (NIST SP 800-16, 1998)

The approach also distinguishes that training should be divided into three levels, depending on the difficulty level and content. These levels should be linked to job roles and responsibilities, where not everyone needs for example advanced training. Three behavioral objectives for trainings were also identified: (1) conditions of activity, (2) activity to be performed, and (3) level of success. Test measures should be things that put the learner to apply the learned, such as problem solving. To evaluate the effectiveness of the training student satisfaction, learning effectiveness and teaching effectiveness, performance effectiveness, and training program effectiveness should be taken into account. (NIST SP 800-16, 1998)

NIST SP 800-50 (2003) focuses on designing an awareness and training program, but does not explicitly state on what theoretical framework it is basing its claims. As most of its content is based on SP 800-16, the assumption is that andragogy is also used in this guideline as the theoretical base. This SP 800-50 identifies three steps in the development of training, where first is the designing the program. After this comes the developing of the awareness and training materials, which is followed by the implementation. (NIST SP 800-50, 2003)

The SP 800-50 (2003) guideline also states that the design must fit the organizational needs, as users need to feel the relevance of the subject. This can be done with conducting a needs assessment before designing. The guideline brings up the notion of outsourcing the training, but guides that the organization should understand its training needs beforehand to be able to determine whether the prospective vendor's training material is suitable for them. Suggested methods in the guideline are interactive video training, web-based training, non-web computer-based training and onsite instructor-led training. (NIST SP 800-50, 2003)

ENISA has not published any guidelines on effectual trainings yet (if exercises are not taken into account), but it has identified in a 2012 report a three-step process for developing an effective information security awareness program. The steps are to first plan, assess and design, then execute and manage, and last evaluate and adjust. The report also proclaims that the main principles of change managements should be used to ensure that the objectives of an awareness campaign are met. To ensure that the awareness campaign effects behavior and culture, the report suggests using training as a support. Even though the report talks about awareness campaigns, it is included in this study as in the end it states that the guidelines can also be used in trainings. For this reason, it is also included in this research.

2.4.2 A Design Theory

To overcome the shortcomings of previous research, Puhakainen's study *A Design Theory for Information Security Awarness* (2006) uses the universal constructive instructional theory (UCIT) and the elaboration likelihood model to explain informaiton security trainings. The use of multiple theories is argued by Puhakainen to bring more understanding to the phenomena, as one theory cannot explain everything. In this study, the behavioral and attitudinal change of the user is seen as crucial, as the user may not follow security measures even though they are aware for them. Thus, learning is perceived as persistent change in the learner's behavior. (Puhakainen, 2006)

UCIT is used to trying in explaining the learning situations complexity. It is a framework used to help design situational instructional theories, which are used for creating customized instructions. It is seen especially efficient in organizational instruction formation. UCIT consists of (i) functions, (ii) basic components and (iii) situated awareness/constrains systems. Functions can be acquisition, storage, and use of knowledge. Basic components are divided into the learning environment, the learning tasks, the learner, and the frame of reference. (Puhakainen, 2006)

The learner's attitudinal change is explained with the elaboration likelihood model, which sees cognitive processing and cues as routes to the change. The attitudinal change through cognitive processing happens in three parts, where first the recipient recognizes the persuasive arguments. Then the recipient tries to understand them in a meaningful way, and in the end makes an evaluation of the arguments. The recipient's motivation and ability effect on how they process these arguments. Recipients with high motivation are more likely to use cognitive processing to process the arguments, whereas recipients with low motivation rely more generally on cues. It is argued that change happening based on cognitive processing can be seen to be more predictable and long-lasting versus change based on interpreting cues. (Puhakainen, 2006)

The design of the training should be done based on UCIT, which has four different stages. In the first stage, the instructional tasks are defined. Then the learners' current knowledge and attitudes are defined. Third stage is about reconstructing the learning tasks and environment, and then in the last stage the effectiveness of the instructions are measured. (Puhakainen, 2006) This process is illustrated in Figure 3.

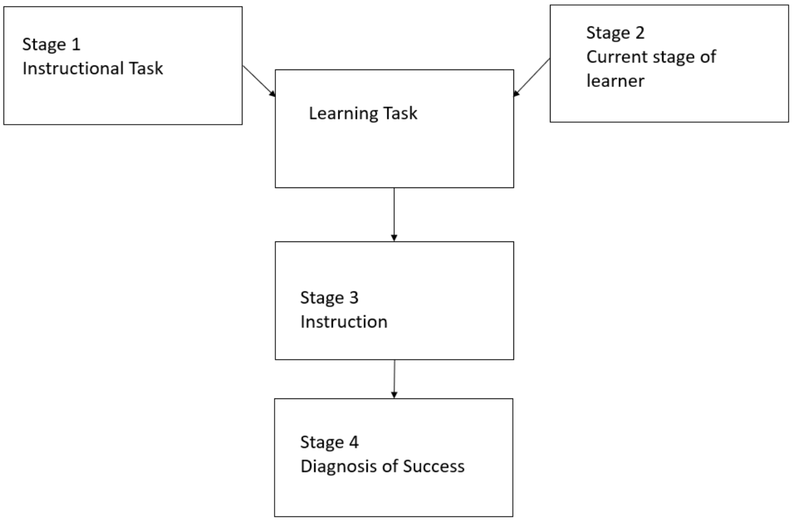


Figure 3 Design Theory modified (Puhakainen 2006, p.76)

Applying these theories to information security training, Puhakainen recognizes four meta-requirements that IS security awareness training should have in order to be effective: (1) learner's previous knowledge should be taken into account, (2) possibilities and constrains cause by the instructional task, the learning environment, and the organizational setting should be taken into account, (3) systematic cognitive processing of information should be enabled, and (4) systematic cognitive processing of information should be motivated. (Puhakainen, 2006)

2.4.3 A Meta-Theory

Karjalainen has in her study *Improving Employees' Information Systems Security Behavior - Toward a Meta-Theory of IS Security Training and a new Framework for Understanding Employees' is Security Behavior* (2009) formed a meta-theory regarding IS security trainings. As a basis, she have used Hare's theory of three levels of thinking. The three levels are: (1) Meta-level, (2) Critical thinking level, and (3) Intuitive thinking level. When applied to IS security training, Meta-level consists of the nature and existentialistic features of IS security training. Critical thinking level is about the pedagogical requirements for IS security training and Intuitive thinking level is the practice of IS security training at organizations. (Karjalainen, 2009) Figure 4 illustrates this framework.

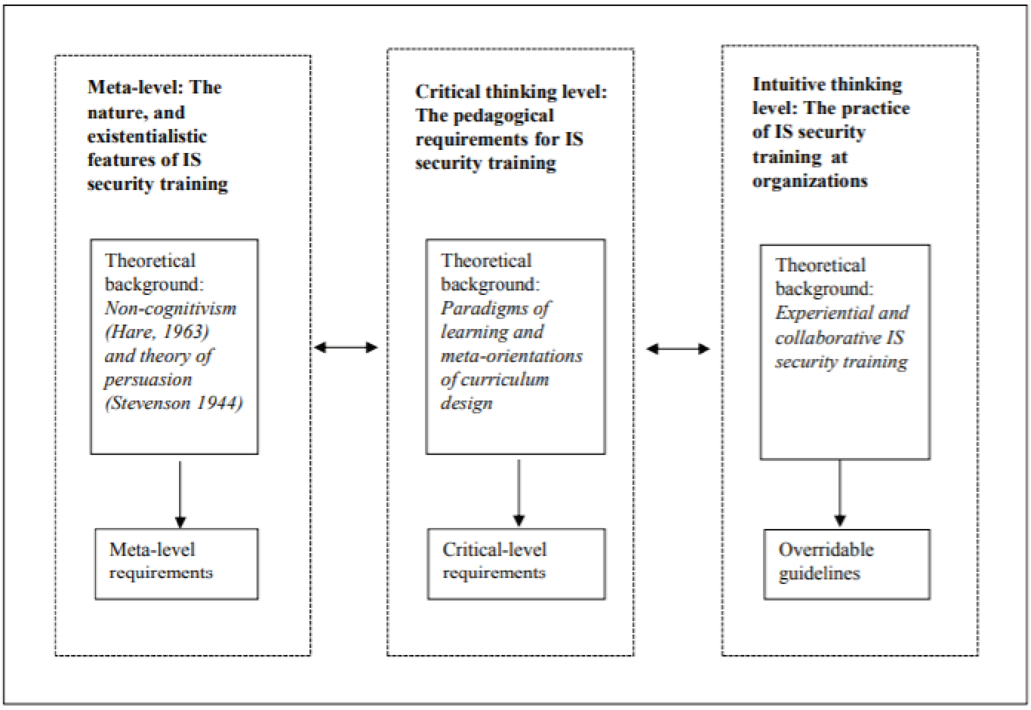

Meta-level: The nature, and existentialistic features of IS security training
Theoretical background: Non-cognitivism (Hare, 1963) and theory of persuasion (Stevenson 1944)
Meta-level requirements
Critical thinking level: The pedagogical requirements for IS security training
Theoretical background: Paradigms of learning and meta-orientations of curriculum design
Critical-level requirements
Intuitive thinking level: The practice of IS security training at organizations
Theoretical background: Experiential and collaborative IS security training
Overridable guidelines

Figure 4 A Framework to Design IS security training approaches (Karjalainen 2009, p.32)

Based on the formed meta-theory, Karjalainen suggest that the nature of IS security trainings differ from other types of trainings. On the Meta-level, she sees that the trainings are based on non-cognitivism and persuasion. This differs from other types of training in that it does not provide absolute scientific facts and tries to affect the learner's attitude and behavior. In addition to IS security being non-cognitive and persuasive, three existentialistic features can be identified on the meta-level: (1) an existence of security-sensitive organizational assets, (2) threats towards them, and (3) different technical, social, and organizational mechanisms for protecting the assets of the organization. (Karjalainen, 2011)

Transformation meta-orientation was deemed to be the most suitable for IS security training, based on the testing of meta-orientations. The general aims of transformation-oriented trainings are viewed coherently with personal perceptions and experiences. The ultimate goal of the learning process is in transforming predominant beliefs and actions. In the context of IS security training, the goal of the training is to transform IS security beliefs and actions for them to be naturally adapted to employees' daily tasks. (Karjalainen, 2011)

Karjalainen also acknowledges that social aspect of learning and communal change need to be emphasized in IS security trainings as organization's security culture is developed socially. It is argued, that this can be done with social constructivism as the theoretical basis for IS security training. This theoretical standpoint also guides the first pedagogical requirement introduced by Karjalainen, which states that the training approaches in teaching and learning need to be based on group-oriented theoretical approaches. (Karjalainen, 2011)

As transformation-oriented training is focused on learners' experiences and communal involvement, it is perceived as learner-centered. The content of the learning is not separable from the teaching methods and is formulated during the educational practice. This guides the second pedagogical requirement identified by Karjalainen, which states that collective experience and meaning perspectives of the learners are the basis of IS security trainings. The used methods should enable students to critical reflection of information with real world problems. Third pedagogical requirement specifies that the used teaching methods enhance collaborative learning, so that learners can reveal and produce collective knowledge. Fourth requirement focuses on the evaluation of learning. The requirement is that the methods used for evaluation need to focus on experiential and communication-based methods. What this means is that students have an active role and responsibility in the evaluation process, and that learning community is the viewpoint in the evaluation. (Karjalainen, 2011)

Karjalainen also introduces a new training approach that takes into account all the four requirements, as has been noted that none of the previously formed approaches were lacking in those. She chose experiential learning as their learning approach, as it is a constructivist instructional design approach, it suits adult education and used in organizational context. Kolb's learning cycle is used as a theoretical basis for understanding learning process. It consists of four stages: accumulation, interaction, examination and accommodation. Each of the stages have certain processes which need to be fulfilled in order to create change. Karjalainen applies this four staged experiential learning to be as an example of the intuitive thinking level in her meta-theory of designing security training approaches. (Karjalainen, 2011)

The learning cycle begins with concrete experiences (1), which in the case of IS security training, are former experiences that the learner has in relation to the existentialistic features of IS security training. Reflective observation (2) is the second phase of the cycle, and it takes place with retrieving, exchanging and structuring groups' shared experiences. In IS security training context, this can be done with learners working in small groups to form meanings and implications of the existentialistic features of IS security training in their own organization. Third phase is the formation of abstract concepts and generalization, which are the processes of negotiation, interpretation and evaluation. Now the meanings formed in the previous phase are reflected on organizational viewpoints. Active experimentation (4) is the last phase of the cycle, and this is where the analyzed experiences of employees' are used to develop new organizational practices. Essential is that the learners receive the trainings concrete outcome in written form. The learners also need the chance to test their new understanding in practice. (Karjalainen, 2011)

What these theories, presented here, indicate is that trainings and their effectiveness can be perceived with many different approaches. Now, as the framework of cyber security training has been established, it is time to move on to adult education.

3 ADULT EDUCATION

Adult education was chosen as the pedagogical framework for this research as the cyber security trainings targeted for organizations teach adults. By reflecting the approaches received from empirical data to adult education framework, the question of whether the approaches are suitable for adults to learn in organizational context is answered. This chapter's intention is first to explain what adult education is and why adults are perceived to learn differently compared to other groups. Then it will proceed to introducing two adult learning theories. As was with cyber security training, in adult pedagogical field, there is no unanimity on how adults learn best. For that reason, the most noted theories regarding adults and their learning will be showcased.

3.1 Adults as Learners

Defining adults is one of the key questions of adult education framework. One way to define them is by chronological aspects such as age. This is a popular and a common way, but there are also some fundamental problems with it. One problem that should be addressed with this definition is that age is very cultural concepts, which means that different cultures interpret age and years differently. For this reason, in the academic world, adults are usually defined through the development of adult thinking.

Adult thinking development is part of the developmental psychology field, and its theories try to explain how and why adult thinking differs from children. The field is very fragmented, but one of the first and most noted is Piaget and his theory of cognitive stages. The main ideas of this theory are the development process of causality thinking, the construction of new knowledge on top of old knowledge, and the construction of mental schemes based on action. The capability to formal thinking is the highest developmental stage, where abstract thinking is done. This theory has led to multiple countertheories, where adult thinking levels have been explained with things varying from behavioral complexity (Dynamic Skill Theory) to mathematical models (Model of Hierarchical Complexity). (Kallio,2016) Because of this complexity, this research will not use any specific definition on adults, as it is outside of the research scope. Thus, it will only acknowledge that adults differ from children due to thinking development.

3.1.1 Andragogy

Malcolm Knowles can be seen to be the first to distinguish adults as learners. He introduced the concept of andragogy, which explained adult learning with situation-motivation and experience centrism. It is based on humanistic psychology as it perceives that humans are good and able to control what and when they learn. Its philosophical roots can also seen to be in pragmatism, existentialism and behaviorism. (Malinen, 2000)

Knowles distinguished six assumptions, called *System of Concepts*, for adult learners:

1) With ageing, people shift from being dependent to being self-directive.
2) Adults have gained life experiences that should be used for learning.
3) Adults learn better when the learning task is related to their social position.
4) Adults are more problem centered than subject centered learners as they wish to apply the learned immediately instead of learning for the future.
5) For adults, internal motivators are stronger than outside motivators.
6) Adults need to know the reason why they are learning.

The first fours assumptions can be distinguished to describe the adult learner, where the last two are more about the learning conditions. These assumptions have been seen as the foundation for adult education. (Malinen, 2000)

The difference between pedagogical model and andragogical model is in that in pedagogical model the focus is on the content of the learning rather as in andragogical model the focus is on the learning process. In andragogy, the facilitator’s role is to set the climate for the learning, and involve the learners in the planning, delivery and evaluation of their own learning. Andragogy also perceives that if pedagogical principals are used in adult learning situations, resistance and resentment towards the content appears, as the learning is seen to be imposed on the learners rather than the learners choosing to learn for themselves. This is due to the fact that adults see themselves as independent and self-directive. Andragogy also distinguishes that adult learners may have negative past experiences on learning, or they may be close-minded on learning something new as they perceive their old information to be still relevant. These are aspects that pedagogy focusing on children does not really have to notify. (Merriam & Bierema, 2013)

Knowles never explicitly stated what knowledge is expect that education's purpose is to transmit knowledge and in order for people to become competent, they need to acquire the knowledge in the context of its application. As experience is the richest resource for adults' learning, the analysis of experience is the core methodology in adult education. The design and conducting of learning experiences happen through interactions as adult educators together with adult learners define the learning experience. (Malinen, 2000)

Andragogy has been questioned for representing learning in a too simplified matter, as it does not take social context into consideration and sees that adults are capable of controlling their own learning totally. (Merriam & Bierema, 2013) Andragogy is also seen by many scholars as being a set of assumptions regarding adults as learners rather than being theory of adult learning. (Merriam & Baumgartner, 2020)

3.1.2 Self-Directive Learning

Another approach to adults as learners is represented with the theory of self-directive learning. Malcolm Knowles can also be seen as one of the founders in this approach, as self-directiveness has a crucial role in his andragogical approach. Still, it is good to examine this theory separately, as it has been widely studied and used outside the framework of andragogy. (Merriam & Baumgartner, 2020)

The goals of self-directive learning can be divided into three categories: (1) to enhance the ability of the adult learners to be self-directive in their learning, (2) to foster transformational as central to self-directive learning, and (3) to promote emancipatory learning and social action as an integral part of self-directive learning. Thus in adult education, the target has been to train adults to be self-directive. It has also been noted that the first goal is not only merely meant for adults as self-directiveness should be targeted at every developmental phase. (Merriam & Baumgartner, 2020)

Self-directive learning can be either seen as an attribute of an individual, as a goal itself or as a skill to be developed. If self-directive learning is seen as an attribute, it is stated to be the individual's skill level, personality, ability and motivation. (Lemmetty, 2020) When applied to a learning process, it means individual's initiative in their own learning process, with or without the help of others. The learning process can be seen to start from the assessment of one's learning needs moving to formulating learning goals, followed by identifying human and material needs, and implementing learning. In the end, evaluation of the learning takes place. Whether an adult showcases self-directiveness in learning has been identified to be affected by four different aspects. These aspects are: (1) the technical skills related to the learning process, (2) familiarity of the learned subject, (3) one's sense of personal competence as a learner, and (4) the commitment to learn at that time. (Merriam & Baumgartner, 2020)

The criticism of self-directive learning has focused on the problem of individuals being represented as too autonomous, and the learning to being seen as detached from the outside world. (Lemmetty, 2020) Still, self-directive learning and self-directiveness have been applied especially in the field of employee competence building. (Merriam & Baumgartner, 2020)

Now that the distinction on who adult learners are, the focus will shift to the learning process itself.

3.2 Adult Learning Theories

Learning processes can be interpreted with learning theories. (Merriam & Bierema, 2013) First it has to be noted that there are contradictory uses of the term theory in the adult education field. There are many principals and frameworks, but which do not have the core content as in theory. Also, the field is very fragmented in that small theories which occur in certain situations have been formed and used, instead of forming universalistic theories that can be evaluated with empirical evidence. (Malinen, 2000) Thus, it is very similar to cyber security framework. The two theories presented here are ones which have been widely acknowledged and used by scholars to study learning of adults in different contexts.

3.2.1 Transformative Learning Theory

Transformative learning theory perceives learning as a process where new knowledge transforms the learner based on their past experiences. The learner finds new ways to think of situations that their past experiences are not able to deal with sensibly. (Merriam & Bierema, 2013) Jack Mezirow is the founder of transformative learning theory of adult learning, with his book, which was published in 1991. His transformative theory can be seen to fit the philosophical context of Habermas' critical theory. (Malinen, 2000)

Knowledge is one of the key concepts in transformative learning theory, and Mezirow distinguishes three qualities of knowledge. These qualities are: (1) recipe knowledge, (2) meaning perspective and meaning schemes, and (3) emancipatory knowledge. Knowledge is also seen to be located in the knowing subject. What this means is that knowledge is seen to come from the learner's ability to construe and reconstrue the meanings of an experience in regards to their own terms. (Mezirow, 2008) This can also lead to the possibility of inappropriate knowledge structures. These inappropriate structures can be seen as cultural constructions as they usually form in relation to people being on different stages on intellectual development. It is acknowledged that some form of objective knowledge exists, but main perception is that knowledge does not derive from books or educators. Thus, transformative learning can be seen as the process by which adults learn how to think critically for themselves rather than taking information as given. (Mezirow, 2008) This Mezirow's perception on knowledge can be defined to be overly contextual, as one can only know in terms of one's own perspective. (Malinen, 2000)

Knowing is happening, in Mezirow's perception, in the meaning perspectives. These meaning perspectives constitute interpretive frameworks for living, knowing and learning. Meaning perspective refers to the structure of assumptions in which one's experience assimilates and transforms new experiences. Understanding is often derived from finding the right metaphor to fit the experience analogically into one's meaning schemes. These constructed meanings then guide people in their mental and behavioral activity. They also reject ideas that do not fit the preconceptions made. (Mezirow, 2008) Thus, meaning perspective is also a personal paradigm, which tells how people perceive themselves and their relationships. These personal meanings are gained and validated through experiences from human interaction and communication. (Malinen, 2000)

Mezirow perceives discussion or dialogue as the most important aspect to guide adult learners. Social interaction is the only way which perspective transformation is affected as it allows to see alternative ways of seeing through the perspective of others. Reflective dialogue also gives meaning to experience and justification to assumptions. Perspective transformation is also never complete without action, and this action needs to be based on the transformative insights. Thus, all transformative learning involves action taking to implement insights derived from the critical reflection. (Mezirow, 2008)

Ten phases have been seen to constitute transformative learning (Malinen, 2000):

1) Experiencing an event in society that disorients one's sense of self within a familiar role.
2) Engaging in reflection and self-reflection.
3) Critically assessing the personal assumptions and feelings that have alienated self from traditional role expectations.
4) Relating discontent to similar experiences of others; recognizing the shared problems.
5) Identifying new ways of acting within the role.
6) Building personal confidence and competence.
7) Planning a new course of action.
8) Acquiring the knowledge and skills necessary to implement this new course of action.
9) Trying out the planned action and assessing the results.
10) Reintegrating into society with the new role behaviors and with new assumptions and perspectives.

Transformative learning theory can be seen as adults learning from aha-moments, whereas the next introduced experiential learning theory is based on learning happening with experience.

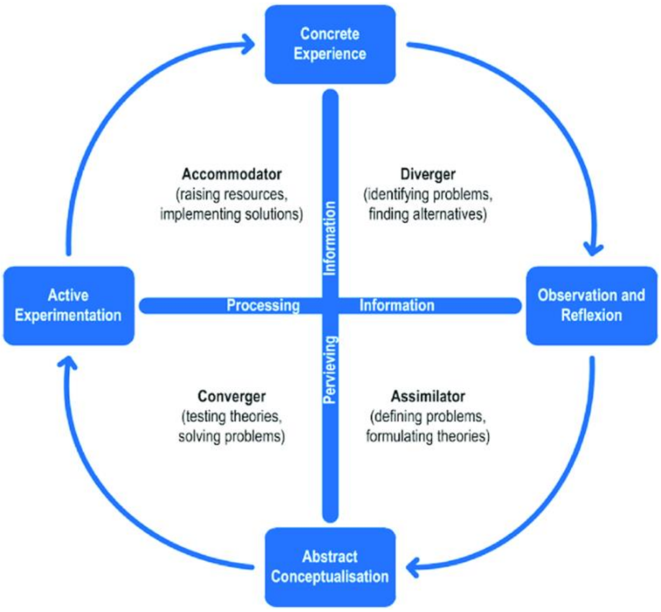
3.2.2 Experiential Learning Theory

Experimental learning theory has been widely used in adult education and different divers contexts. It has been understood and used as a paradigm, a framework or even as a method to teach adults. David Kolb can be seen as the main theorist behind experiential learning theory, with his book *"Experiential Learning, Experiences as the Source of Learning and Development"* published in 1984. Especially professional development research has used Kolb's theory. (Malinen, 2000)

Kolb identifies six principals for experiential learning (Kolb, 1984):

1) Learning is Best Conceived as a Process, Not in Terms of Outcomes
2) Learning Is a Continuous Process Grounded in Experience
3) The Process of Learning Requires the Resolution of Conflicts Between Dialectically Opposed Modes of Adaptation to the World
4) Learning Is a Holistic Process of Adaptation to the World
5) Learning Involves Transaction Between the Person and the Environment
6) Learning is the Process of Creating Knowledge

So, in this theory knowledge is derived from experience and is also tested out in the experiences of the learner. Still, simple perception of an experience is not seen as sufficient enough for learning and knowledge building. Something most also be done with the experience. Knowledge is seen to be obtained in the sensation that follows after being affected by an object. Thus, knowledge is then the internal representation of external matters and rests upon sensations. (Malinen, 2000) This knowledge building and learning is represented in figure 5 below.



Concrete Experience
Accommodator
(raising resources, implementing solutions)
Diverger
(identifying problems, finding alternatives)
Information
Active Experimentation
Processing
Information
Observation and Reflexion
Pervieving
Converger
(testing theories, solving problems)
Assimilator
(defining problems, formulating theories)
Abstract Conceptualisation

Figure 5 Kolb's Process of Experiential Learning and Basic Knowledge Forms (Kolb 1984,p.42)

Kolb divides elementary knowledge into four forms as represented in figure 5. These forms are formed due to the two dialectically opposed forms of prehension and two opposite ways of transforming that prehension. The four forms are divergent knowledge, assimilative knowledge, convergent knowledge and accommodative knowledge. (Kolb, 1984, p.42)

Kolb perceives that in regards to learning, everyone has more or less formed ideas about the topic at hand. For that reason, perception is the basis for knowing and knowledge. Also, learning requires the resolution of conflicts between dialectically opposed modes of adaptation to the world, and it is an emergent, continuous, cyclical, holistic and adaptive process. (Malinen, 2000)

Important factor to also notify is that experiential learning is retrospective, as the experience under modification has been passed or lived through. This retrospective is necessary as the learner has to live through the experiences before being able to modify them. The modified past experience does not disappear as it can be reflected upon in the future. (Malinen, 2000)

3.3 Learning at Workplace

Adult education as a field is usually divided into two or three sections, depending on where the learning takes place. Workplace is seen as a crucial part, and it is regarded as one section in the tripartite division. (Vanhalakka-Ruoho, 2014) There are also many different types of learning, but this study will focus on nonformal learning, as it is stated to be the learning opportunity, which is provided by an institute or an organization, but where the main focus is not on education such as a degree. Descriptive to non-formal teaching is short-term and voluntary. It usually also follows a certain curriculum and a facilitator. (Merriam & Bierema, 2013)

In the workplace there can be many types of learning processes going on, but the reason why employee training and competence building is facilitated is seen to be driven by either management or social change. What this means is that learning at workplace can either be seen to be action that is managed from above for the employees to meet the organizational demands, or on the other hand it can be employee's own competence building regarding their own personal goals. (Poikela & Poikela, 2014)

The challenges that adult learning can face are manyfold. For example, adults usually have different responsibilities overlapping with learning, such as family and work matters. These matters can affect negatively on the motivation or concentration, which will then affect negatively on the learning process. (Merriam & Bierema, 2013) Also, the facilitator of the learning process may not be aware of the special pedagogical features of adult learning, which means that they are not capable to guide the adults properly in the learning process. This is visible in that in adult education, the word teacher is not commonly used anymore to make the distinction that adults cannot be "taught" in the same way as children. The facilitator should be more as a guider to the knowledge. Also, the greatest difference, regarding teacher's role in the teaching between children and adults, has been stated to be that children cannot learn without teachers but adults can. The challenge then is for the facilitator to form such an environment, where the adults are responsible for their own learning without neglecting their needs to guidance. (Poikela & Poikela, 2014) This study will further on use facilitator as the term for teachers but will still use teaching when referring to adult learning process.

The challenge with facilitators is also their lacking in pedagogical education. It has been studied that especially in the field of technology, the facilitators teaching adults do not have pedagogical background. (Heikkinen, 2014) This means that usually the facilitators are people with competence on the taught area. Teaching based on practical knowledge can be perceived to be personal combination of certain forms of knowledge. (Jarvis, 2004) So, in conclusion, facilitators, who do not have any pedagogical background, and only may have practical knowledge on the taught matter, are only teaching subjective form of the matter.

4 Methodology

This chapter will now focus on the empirical part of the research. First, the used methodology and data collection are presented. Then the chapter will proceed to the results of the analyzed data.

4.1 Data Collection

As has been brought up, the concept of cyber security trainings is manyfold. For this reason, the study also has different features from different fields. With the focus on the pedagogical perspective of the trainings, the study will be placed in the pedagogical and educational research category. Pedagogical research can be defined to be focused on how the pedagogy is formed and how effective it is, whereas educational research's main focus is on providing principal bases for knowing and policies. Educational research can also be divided into four different groups based on how they study the phenomenon of education: (1) descriptive, (2) exploratory, (3) explanatory, and (4) evaluation. This research will fall into the exploratory research category as the goal is to identify what the phenomenon is about without explicit expectations. The methods used in these types of research are usually ones, which are able to grasp large amount of unstructured data. Also, many different types of methods maybe used due to the complexity of the phenomenon. (Check & Schutt, 2012)

To ensure the full comprehension of the training phenomenon in question, qualitatively driven mixed method research was chosen as the methodological standpoint. This type of research, where both qualitative and quantitative methods are used, should be used for five different reasons: (1) triangulation, (2) complementarity, (3) development, (4) initiation, or (5) expansion. Triangulation can be defined as the convergence of the data collected, which can be seen as enriching and fortifying the conclusions. Complementarity as a reason gives the researcher the possibility to fully understand the research problem, as the data collected with different methods give answers to different aspects. Developmental reason is used when data collected via one method is then used to collect more data with another method. Initiation and expansion are reasons regarding future research. (Hesse-Biber, 2010)

Another approach is set by Bryman (2006) on why mixed-methods research should be used. He forms six classifications for using mixed methods: (a) credibility, (b) context, (c) illustration, (d) utility, (e) confirm and discover, and (f) diversity of views. In regards to both of these approaches, this research will use mixed methods for triangulation and complementarity to achieve credibility and contextualization. (Bryman, 2006)

The data collection and analysis is done concurrently, even though the methodology is qualitatively driven. This is achieved with a questionnaire, where both open and close-ended questions are present. Their findings will be also analyzed at the same time, but as the main research questions were qualitative in nature, qualitative analyses will have more emphasized primacy. Thus, the design of the empirical study is inductive-sequential (Schoonenboom & Johnson, 2017):

QUAL + quan

The integration of the data is something that also needs to be thought of for the study to fully fulfill mixed method research qualification. There are different perceptions on how this can be done, but this study will focus on the classification of Teddlie and Tashakkori (2009), who have distinguished four data connection points. These points of integration are:

1) Merging the two data sets
2) Connecting from the analysis of one set of data to the collection of a second set of data
3) Embedding of one form of data within a larger design or a procedure
4) Using a framework to bind together the data sets (Teddlie & Tashakkori, 2009)

This study will be situated in category one, as the two data sets will be formed with the same method.

The method used to collect data for this empirical part was by a structured online questionnaire. As the questionnaire had both open-ended and close-ended questions, intramethod mixing was used. Intramethod mixing can be defined as the use of a single method that includes both qualitative and quantitative components. By using both components in a single method, it gives the change to broaden the understanding of the phenomenon in comparison to if only one component was used. (Tashakkori & Teddlie, 2010)

The questionnaire had 20 different questions (appendix 1), where were used to identify which company had answered the questionnaire. This identification was only made to make sure that only one answer from each company was qualified. All the other questions were formed around three themes recognized from the frameworks of cyber security training and adult education regarding cyber security learning and teaching:

1) Principle for training
2) Learning situation
3) After learning

This type of question formation is suitable in cases where the research question reflects to previous research. Regarding the questions on training, seven were quantitative with possibility for open answer and 11 were completely open-ended. The quantitative data was collected as a cross-sectional study. This type of method is used when the researcher, for example, wants to know how common something is. These types of questions do not tell causation. (Valli & Aarnos, 2018).

With the use of questionnaires, there are both strengths and weaknesses. The strengths are aspects such as good for measuring attitudes, perceived anonymity, possible ease in data-analysis and quick administration to groups. The weaknesses are aspects such as the possibility for missing data, vague answers, different capabilities in verbal ability, low response rate. (Tashakkori & Teddlie, 2010)

All the questions regarding the training itself were mandatory. The questionnaire could be saved and continued later on, so it was not compulsory to answer all questions at once. The questions were both in Finnish and English to make sure that possible language barrier would not stop from answering. To tackle to problems linked to questionnaires, special attentions should be given to aspects such as the language used to form the questions, in the selection of answerers, and the possibility of too difficult questions. Especially with open-ended questions, the possibility of not receiving the information in the answers also needs to be taken into account. In regards to validity of a questionnaire, there are four measures, which are content validity, face validity, criterion validity, and construct validity. Content validity measures whether the domain has been properly covered, face validity regards the appearance of the questionnaire, criterion validity measures the effectiveness of the questionnaire, and lastly construct validity is about how well the questions form a relationship with each other. (Bourke, Kirby & Doran, 2016). All of these notions regarding questionnaires, were tried to be taken into account in this study.

In this research, the questionnaire was sent to 22 different companies, who advertised cyber security related trainings in Finland on their webpages. The companies were not pre-selected in any way, and thus varied in size and resources. This was deemed to give versatile data, which would then hopefully add to the validity of the research. For this reason, the companies were also not only ones listed on the National Cyber Security Center's partner list, as it could have given distorted data, as it could be that not all companies wish to be on the list due to different reasons. The first official question regarded what services the company offered to make sure the validity of the answers. All the companies answered to providing separate training, and four also stated to having separate simulations and combined simulation trainings.

The questionnaire was done by using an online service Webpropol. It is an acknowledged service used to form and distribute questionnaires. In Webpropol, the answerer can reflect the questions to each other as the answerer is able to see the more than one question at a time. This feature can have an effect on how questions are answered, as the answers can be more consistent with each other as the answerer is able to see the whole picture with where the questions are heading. On the other hand, if the questions are similar in structure, the answerer might not be as thorough in answering all of them. These aspects need to be taken into consideration, as the success rate of the questionnaire is crucial in the overall success of the research. (Valli& Aarnos, 2018)

A link to the questionnaire was sent by email in mid-December 2020, and it was open until mid-January 2021. A reminder email was sent at the beginning of January 2021. In the email, it was explained what the research was about and why the company was contacted. It also tried to clarify what type of training was in question, and that answers regarding exercises and simulations should be left out. It was also brought up that if the person receiving the email was not the correct person to answer such a questionnaire, that they would then send it forward to someone who was valid to answer.

In the end, five different companies answered the questionnaire and it was deemed to be sufficient as the answer rate was then approximately 20%. Saturation could have also been one indicator of sufficient data amount, but as there is no exact knowledge on the phenomenon, there is no possibility of knowing when saturation is reached (Tuomi & Sarajärvi, 2018). For this reason, the answer rate can only be judged to be either sufficient or not. With this answer rate, the answers were seen to give a general picture on what is being done in the private sector, which was one of the goals of the research. Thus, the answer rate was deemed sufficient.

4.2 Data Analysis

As the research is qualitatively driven mixed method research, qualitative data is in the focus. Thus, qualitative content analysis method was then chosen to be used to distinguish the different pedagogical aspects in the questionnaire. This type of method is applicable to any message medium, and it does not only focus on the words but also on the concepts and ideas that are being communicated. This differs from quantitative content analysis in that in this the coding structure is created based on the researcher's interpretation and identification of the meaning. In addition, quantitative content analysis is also focused on the frequency of occurrence of content, which is not intentionally done in qualitative content analysis. (Newby, 2014)

In content analysis, the main idea is to classify the words of a text into much fewer content categories. These categories can consist of many different words or just one. The categories are based on the assumption of the similarity in meaning. The similarity can be based on aspects such as connotations or precise meaning. This classification process is very crucial as it should be consistent throughout the data. Also, it should be documented in a way that other researchers conducting the study are able to come to the same conclusions. There are three reliability types relevant to content analysis, which need to be taken into account in the coding process. These are stability, reproducibility and accuracy. (Weber, 1990)

This study follows theory-guided approach in content analysis, as it gives the possibility to choose the coding based on the text. Still, it distinguishes that theory cannot be left out completely in regards to influencing the researcher in some way. In this research, the theory-guidance is visible in forming the three themes, which were then used to form the questions. However, this is not same as theory-based approach where theory is used to form the actual codes or to test the data based on a theory. (Tuomi & Sarajärvi, 2018)

The content analysis will follow this process formed by Weber (1990):

1) Defining the record units by themes.
2) Defining the categories to be non-exclusive (word can belong to multiple categories).
3) Test coding on a sample of text.
4) Revise the coding rules if necessary.
5) Code all the text.
6) Assess achieved reliability or accuracy.

The codes are then be interpreted, which is the process of translating linguistically expressed elements into another. This transformation is done to map the content of the text to fit theoretical structures. As the amount of text formed in empirical part is not massive, the analyzing is done by hand rather than using a computer tool. (Weber, 1990)

The metric for quantitative data was chosen to be YES and NO, with the possibility to elaborate on YES answer. This metric can be useful in cases where the questions are straight forward, but it also possesses the possibility of lacking in regards to reliability. This is because it cannot be tested with these metrics alone. (Valli& Aarnos, 2018) The quantitative questions in this research were deemed to be such that they could use YES and NO metrics, and as there is also qualitative data analyzed, reliability should not be an issue. Also, any possible unintentional leading of the answerers was the goal, as if the metrics had been, for example, descriptive, it could have given the answerers the perception that the used metrics were a necessity in a good training.

The quantitative data is first quantified and then the trends are evaluated. As the role of the quantitative data is not leading, aspects such as correlation or regression are not searched for. Together with content analysis, this type of quantitative data analysis gives a good understanding of cyber security trainings as a phenomenon.

5 Empirical Results

Now the results of the empirical data analysis will be represented in subchapters based on the three themes that were identified from the two theoretical frameworks. Then these answers will be elaborated more in the next chapter.

5.1 Principle for Training

At the start, none of the companies proclaimed to have used any pedagogical theory as a basis for the training, but two companies stated to have used other types of theories. Of these two, one claimed to follow *"A design theory for information security awareness"* formed by Petri Puhakainen, and the other company stated to use multiple different researches from the fields of criminology and social psychology.

The companies were asked what they perceived to be the main principles for their cyber security training. They were also asked whether they tailor their trainings based on customer, and if yes, then what aspects are taken into consideration. 80% of the answered companies stated to tailor their training based on the customer, and based on the open-ended answers, three categorized approaches could be made on how companies formed training. These are summarized in the table 1 below, where the contents, which justify these categories, are mentioned below the approach.

Table 1 The principles used to form training.

Customer-Oriented Principle	**Student-Oriented Principle**	**Content-Oriented Principle**
Answering to need	One aspect at a time	Awareness building
Building the training based on customer's wishes	Learning goal is achieved	A lot to be taught

Extending cyber security culture to personnel	People are in a rush	Extending cyber security culture to personnel
Customer's field	Subject is not interesting	Subject is not interesting
	Target group's know-how	Learn how and why
	Participants' background	One aspect at a time
	Students' wishes	Information security policy

Customer oriented principle is brought forward in statements, where customer needs regarding the training are mentioned. These are aspects such as answering to customer needs and planning the training with the goal of teaching specifically personnel. Only one company proclaimed fully to follow only the wishes of the customer as the baseline for their training. Other companies also brought this customer-oriented principle forward, but had also either student-oriented approach or content-oriented approach distinguished in the answers as well.

In student-oriented principle, the learner was seen as the focus when thinking of training. This came up in statements where aspects such as the learning process and what can affect the process were brought up. The third identified category was content-oriented principle, where the content was seen as the main principal in training baseline. This came up in answerers where taught subject was seen as the most crucial aspect in forming the training. Some of the statements are the same in student-centered and content-centered approaches as they could be seen to be linked to either one of the categories depending on the interpretation. As it was not clear in short answers, they were categorized in both groups.

5.2 Learning Situation

In regards to teaching cyber security, two different categories could be formed on how the companies approached the teaching situation. These were Student-Centered Approach and Content-Centered Approach, as summarized in table 2.

Table 2 Approaches to Teaching.

Student-Centered Approach	**Content-Centered Approach**
Learner's role	Is equivalent to real situation
Learner's abilities	Increasing general knowledge to understand risks
Content linked to work tasks	Practical training
Content linked to free time	
Learner's work role	

Relevance to work role and domain	
Practical training	

These two approaches were identified to guide the companies on what was the most important aspects to be taken into consideration when teaching cyber security. The facilitators were categorized to be either information security and cyber security professionals or professionals from other fields. The professionals from other fields consisted of people with varying backgrounds. Only one company brought up to have people with academic pedagogical background teach in the training with other professionals.

Two companies distinguished what general training usually consisted of content wise. The other companies stated that the content could not be generalized, as it was so dependent on the customer. The companies that could distinguish the content stated that the content usually evolved around the topics of cyber threats and their impacts, and information security.

The methods used in the trainings could be divided into two groups of hands-on methods and other types of methods. These are summarized in table 3.

Table 3 Methods used in the trainings

Hands-on Methods	**Other Types of Methods**
Gamification	Lectures
Exercises	Public discussion
Demos	Question answering
Minimal theory	Watching recorded material
Practical training	Going through case examples
Group work	Groupwork

The hands-on methods included methods such as gamification, exercises and demos. It was also brought up that minimal use of theory was the goal. Other types of methods were also brought up such as regular lectures, question answering and going through example cases. Group work was a method that has been included in both categories, as it can be used in either of the groups. Only one company did not bring up the use of hands-on methods in their training.

The training would usually take place either in person either at the customers facilities or at the training companies' own premises. The trainings could also be done virtually via some VoIP service. Some also had the option to watch recorded trainings later on. In addition to the recordings, other materials that could be distributed to the trainees were identified to be things such as posters and other written materials. Two companies answered to providing some material in advance. These could be either some exercises and readings, or the agenda of the training and how to prepare for the training.

In regards how long the training took place, the answers varied immensely. Some companies stated to have trainings lasting from one hour, where other stated trainings to last for days. One company also stated to have continuous training, where short sessions were done few times a year. Group sizes were also something that divided the companies. Others seemed to prefer small groups of 20-50 people, where other companies trained as much of personnel as they could at a time. This could mean over 150 people at a time. There were no typical student bodies that the companies recognized, but mostly their trainees were either personnel working with information technology, such as software and application developers, or people in management positions.

5.3 After Learning

To get a better understanding on the impact of the training, the companies were asked how they measured and followed the successfulness and effectiveness of the trainings. Successfulness was something that almost all companies stated to measure, and it was done mostly by customer feedback. One company stated that they did not measure it any way as that would be the customer's task, and other company answered to measure it with a test on how much the participants had gained knowledge.

Customer feedback was also one way the companies measured effectiveness. Some companies also stated to do some sort of tests either in between the training or afterwards. Only one company answered to not measuring the effectiveness at all. The companies were also questioned on have they done any evaluation of long-term effect on the learning results, and one company answered yes. However, the company stated that the training is so new that they have not had the time to implement the evaluation of long-term effect yet but would do so in the future.

All the companies stated that their trainings could be seen as beneficial in the trainees' personal life as well. The reasons were manyfold, but mostly the answers revolved around the topic of how learning about information and cyber security is useful generally in everyday life. One company also brought up that their training relies on improving the employees' overall skills in cyber security as that way the organization's security is automatically improved.

5.4 Conclusion

So as a conclusion to this part, the companies did not specify to use any pedagogical theories as the basis for the trainings, but few companies did identify to use other types of theories from different fields. Also, the companies could be seen to base trainings from the perspectives of the costumer, the learner or the content. Usually, they had more than one principle.

The teaching itself was either done as student-centered or as content-centered, and the facilitators were most likely professionals from the field of information and cyber security. The content of the training was tailored by all the answerers', so the specific content of the trainings could only be stated by few. The methods consisted of either hands-on methods or other types methods, such as lectures and answering questions. The trainings were stated to be held either in person or online. Some also provided recorded materials to the trainees. The group sizes varied immensely from small groups of 20 trainees to over 150 trainees at once.

The effects and success of the trainings were measured usually with customer feedback. All the companies did perceive that their trainings could have an effect on the trainees' personal lives as well, but only one answerer admitted to have plans to do long-term study on the effects of the training.

Next these results are reflected on the frameworks cyber security training and adult pedagogy that were distinguished in the previous chapters.

6 REFLECTION

In this chapter, the results received from the empirical data are reflected on the frameworks of cyber security learning and adult pedagogy. This will give an understanding on how well the approaches are suited for the fields, and also if there are aspects that should be taken into consideration in the fields in the future. The topics will be covered with the same themes as they were showcased in the previous chapter.

6.1 Principle for Training

This sub-chapter is divided into three parts based on the questions presented for the companies. First the theoretical basis used for trainings are discussed, then the tailoring of the training is reflected on the frameworks and lastly the principles used as the basis for training are evaluated.

6.1.1 Theoretical Basis of the Training

Both the theories of Puhakainen and Karjalainen, from the cyber security framework, proclaim that the use of theories as a basis for the training is a necessity to understand why the training is in fact efficient (Puhakainen, 2006; Karjalainen, 2011). The lacking in theoretical explanation in academic research has been noted by both. This lacking could be seen to be the practice of the companies as well as most of the companies answered to not use any theory as a basis for their training. Two companies did identify to use other than pedagogical theories. One specified using Puhakainen's design theory. The other company stated to have used a wide range of theories from psychology to criminology.

The use of theories from other disciplines in information security research is noticed by Karjalainen (2011). She divides previous research to into seven different approaches based on the underlying theories. By identifying the underlying theories, gives in Karjalainen's perception the understanding on how information security, and matters relating to it, are perceived. In regards to pedagogical theories, Karjalainen argues that they should be identified as that way they can be enhanced to be more effective in regards to learning. Also, she notifies that with identifying the pedagogical theories, the practitioners identify the limitations that are inevitable in every learning situation. (Karjalainen, 2011)

The lacking in use of theories as a base for training is stated by Puhakainen (2006) to be because of the lacking in the research. He states that the theoretical basis should be identified in each study focusing on information security awareness training, as it would help the practitioners also to see what theories are applicable in different situations. Puhakainen also states in his work that information security training approaches should be based on appropriate (kernel) theories and identifies that as learning is such a complex matter, one theory alone cannot fully scope the whole phenomenon. For that reason, more than one theory should be used in the planning of the training. (Puhakainen, 2006)

Karjalainen (2011) addresses that the lack of proper theoretical research on effective information security training has also lead to the problem of not using proper pedagogical theories. Karjalainen sees that without proper meta-level understanding on information security training, no proper pedagogical theories can be selected. For this reason, she identifies the special features of information security training. (Karjalainen, 2011)

Adult education framework also emphasizes using theories. For example, Kolb states that for one to understand learning completely, they must understand the nature and form of human knowledge, and process where this knowledge is formed and processed. Experiential learning theory offers education and learning the process of lifelong learning that is based on social psychology, philosophy, and cognitive psychology. It is not only educational methods, but also the way adults learn. It sees that ideas are not fixed, and thus are in constant change due to experiences. (Kolb, 1984, 26) Thus, the theories are perceived to be a necessity to understand how knowledge is built. Without this, the trainings cannot be seen to be effective in teaching.

So, the lacking in the use of theoretical basis in practice can be noticed to be in relation with the lacking of proper academic research. The use of theories from other disciplines can be seen as justified, but one must understand that they alone do not give the full understanding on the phenomenon on information security training. To select the proper pedagogical theories for the training, one must also understand the special qualities of information security training.

6.1.2 Tailoring and Principles used as the Basis for Training

All of the companies answered to tailor their trainings based on the customer. Many of the companies stated to take into account aspects such as the target organizations' information security policies, used technologies, and the needs and wishes of the organization. This would seem to fit in with both frameworks, but how the tailoring, and especially what the company receiving the information security training, should take into consideration is perceived inside the cyber security framework a bit differently.

Puhakainen (2006) identifies that the role of information security should be addressed in the organization to understand what the employees' attitudes are towards it. This way the proper methods can be found to address the learning needs. The approaches towards information security can be either technical, social-technical or social. In technical approach, the priority is given to technical matters and users can be forced to do certain technical procedures to keep security level high with the threat of punishment. Social approach is on the other end of the spectrum, with user-centric view. In this approach the users' perception on the compliance and motivation are key factors in keeping IS security. Autonomy of the users is respected. Social-technical approach the IS security is based on two unique sub-systems (social and technical), and both of the systems are equally important. In this approach both technical and social aspects are perceived as important in keeping IS security. (Puhakainen, 2006)

Karjalainen (2011) proclaims in her work that three existentialist features are characteristic of IS security training, which need to be addressed in order for the training to be proper for the target organization. These features are: (1) the existence of security-sensitive organizational asset, (2) threats towards them, and (3) different mechanisms for protecting the assets. In regards to the first feature, the employees should be aware of and understand the assets that need protection. Without this understanding the training is lacking in substance. For the second feature, the threats need to addressed in the training in a proper pedagogical way to ensure that employees are able to understand them. The third feature means that there already are protection mechanism in place in regards to the assets, so that training is meant only to reach the objective of securing the asset.(Karjalainen, 2011) Thus, without recognizing these special features in the training, the training is not proper IS security training.

The guidelines perceive tailoring of the training from another perspective as they see the training to be something that is done inside the organization and not by a third party. The NIST SP 800-50 (2003) guideline sees that information security training should be focused for the whole organization. The main focus of the training should be in delivering information to employees that they can use in their daily work. The program also needs to communicate the rules and guidelines set in the organization regarding information security. The main target is to change the behavior of the employees to fit with the policies and guidelines. Also, the punishment of disobeying the rules should be discussed. (NIST SP 800-50, 2003)

The NIST SP 800-50 (2003) guideline perceives that organizations have three different ways to implement the training. The first way is to centralize policy, strategy and implementation. The second is to centralize strategy and policy but distribute implementation. The third is to centralize policy and to distribute strategy and implementation. The approach that is chosen to implement the training is seen to be dependent on the size and geographic dispersion of the company, defined organizational roles and responsibilities, and budget allocation and authority. (NIST SP 800-50, 2003)

The NIST SP 800-50 (2003) guideline also brings up that there are different metrics that can be used to determine the needs of the organization in regards to training. The metrics can be also used to determine whether the training reached the goals set. It sees that the most important action for the organization to do before the training is a needs assessment. This allows to set the right strategy from the beginning. It also reflects on the possible continuation of the training. Targeting the right aspects in the training is crucial especially when planning for the training material, as the needs skills building and knowledge gaining is set through them. (NIST SP 800-50, 2003)

The NIST SP 800-50 (2003) guideline does identify that organizations can buy trainings from an outside source, but they should be careful in that they communicate their needs clearly. They should also make sure that the company is capable of meeting those needs to receive relevant training. The organization should not use any off-the-shelves types of trainings, even if they are offered, as those might not be what the organization needs. Also, even thought the organization has decided to buy the service from outside, they still need to do a needs assessment to see what their needs are in regards to training. The guideline also suggests that organizations should co-operate with trainings instead of buying from an outside source. (NIST SP 800-50, 2003)

In addition to being asked about the tailoring, the companies offering training were asked what they perceived to be the basis for their training. These principles could be identified to be customer-centered, student-centered and content-centered. Most of the companies had more than one principle, and that is also something that the cyber security framework also proclaims in regards to effective training.

Karjalainen (2011) perceives that in order for information security training to be effectual, both the persuasive and non-cognitive nature and the existentialistic features of the training need to be taken into account. What this means is that communal transformation meta-orientation is the best option to use as the basis. Transformation-oriented training focuses on transforming predominant beliefs and actions. This means that it pursues to develop students by integration of affective and cognitive domains. The learned issue is connected to learner's previous experience. In information security, this can mean to connect the security procedures to employees' own work tasks and experiences. This connection is important as new knowledge is constructed through previous experience. This method allows the employees to reflect for themselves what the threats for the assets are and how the assets can be protected. (Karjalainen, 2011)

Karjalainen (2011) also addresses the social side of the training. She proclaims that communal training design should be used, as the information security trainings is primarily focused on creating a communal change rather than only an individual change. This means that the personal development is not the only goal of the training but rather the development of organization's security culture. The communal aspect is also important to recognize as the organization can have unwritten behavioral rules on what is acceptable and what is not. To modify and change those rules, the training approach needs to be group-oriented as then the employees are more acceptive of the changes in the behavior as well as obtain richer knowledge from the group. (Karjalainen, 2011)

Thus, Karjalainen's perception can be seen to have all three approaches, as the students' learning process needs to be taken into account, which is student-centered, as well as the existentialistic features of the IS security training, which can be seen to fit in with the customer-centered approach. Content-centered approach is the basis of the training in Karjalainen's theory as the content gives the uniqueness to the training (both the unique nature and the existentialistic features need to be taken into account).

Puhakainen (2009) also forms four meta-requirements that the information security training should meet.

1) Training should take the learner's previous knowledge into account.
2) Training should take possibilities and constrains caused by the instructional task, the learning environment, and the organizational setting into account.
3) Training should enable systematic cognitive processing of information.
4) Training should motivate for systematic cognitive processing of information.

Thus, the trainings should take both the learner's context and the actual learning process into account to be successful. These requirements are also derived from the uniqueness of IS security training, so the content-centered principle is visible. The customer-centered principle is not as straight forward in these as in Karjalainen's theory, but it is there with the perception that learner's context need to be taken into account.

Adult education framework can be perceived to be about student-centered principle. The andragogical model, for example, was formed to focus on the learning process and not on the content. In this model, it is the facilitator's task to set the atmosphere of the training to be such that adults are able to learn. Thus, the content of the training session is not emphasized in the delivery. (Merriam & Bierema, 2013)

"Climate setting" is also an important notion in the andragogical model, and it is used to explain what kind of environment adults need in order to learn. The first notion in this is the physical environment, which needs to be comfortable and adult-oriented. The second aspect is the psychological atmosphere, which should be trusting, respectful and collaborative. This ultimately means that adults should be able to contribute to the planning of the content of the training, as that will enhance their self-directiveness. (Merriam & Bierema, 2013)

The adult education framework recognizes that in order for adult to learn, self-directive learning needs to be enhanced. This can be done in four different ways. The first is to aspire to gain knowledge or new skills. The second is to aspire more of the hope of becoming more self-directive learner, and third is to aspire for transformational learning. Fourth relates to emancipatory. (Merriam & Bierema, 2013)

The student-centered principle can also be found in cyber security framework. The NIST SP 800-16 (1998) guideline bases its perception on learner in andragogy theory. This is brought up in the notion that training planners should be aware that adults have a special way in learning, and their beliefs, values and opinions should be taken into consideration when planning teaching. Every adult also has a preferred learning style, and everyone has their past education, experience and previously learned information that needs to be addressed in the teaching. (NIST SP 800-16, 1998)

The NIST SP 800-16 (1998) guideline also follows result-based learning, so its basis is in the job functions, unique backgrounds and different levels of understanding. The guideline proclaims that discussion of learning theory is beyond its scope. Still, it recognizes that it is important that the facilitators of the training are specialist on this area. This is to make sure that they are able to understand that the learners do not learn at the same pace and style. The guideline even states that this is as important as the content of the training itself (NIST SP 800-16, 1998)

The learning theories in adult education can also be seen as student-centered. For example, transformative learning theory begins with the individual. The learning process is seen to start with the individual questioning and altering the way they see the world. The goal is to make the adults be aware of their own capabilities in making liberate choices by becoming more critically reflective in thinking. (Merriam & Bierema, 2013)

Kolb also identifies in experiential learning that everyone come to the learning situation with some sort of idea or perception on the matter that the facilitator has to take into account. (Kolb, 1984, 28) Karjalainen (2011) uses Kolb's experiential learning theory to explain the learning process in information security training. There the perception is both on the individual but also on the customer and the content. (Karjalainen, 2011)

The first stage in this model is the creation of experience, as experience can be seen as the foundation for learning. Karjalainen (2011) explains that in the context of information security this means the learners' previous experiences with the existentialistic features of the information security training. The second stage is reflective observation. In the context of information security, the observation is done in groups and it happens via retrieving, exchanging and structuring group's shared ideas. The focus is again on the existentialistic features of the training to define their meaning and implications for the organization. (Karjalainen, 2011)

The third stage is the formation of abstract concepts and generalizations. It involves the process of negotiation, interpretation, and evaluation. The groups viewpoints are reflected to those of the organization, which are presented in the information security guidelines. The reflection, again, has to be done in groups to form communal experience. The last stage is about active experimentation. In information security, this means that the employees' experiences that have been formed in the previous stages, need to be used in forming new information security policies to the organization. This also requires that the employees need to follow the guidelines formed by their experiences. (Karjalainen, 2011) Thus, even if adult education theories emphasize the individual, the theories can also be used to understand other principles as well.

Customer-oriented principle can also be seen to have role in adult education framework in the concept of lifelong learning. In this, the workplace is seen as the enabler for lifelong learning. This is because, for some adults, learning combining work and study can be more productive in comparison to when just one of the aspects is used. (Kolb, 1984, 6) Also, the models of andragogy and self-directive learning notice that the teaching content has to be relevant to the learners. Thus, the customer needs and employee roles have to be taken into consideration when planning for the content.

As a conclusion, the principles that the companies have in forming their trainings can be seen to be relevant in the light of the frameworks of both cyber security and adult education. Next, the learning situation will be reflected upon.

6.2 Learning Situation

This section will now focus on the actual learning and teaching situation. This was approached in the empirical data from multiple different perspectives to get a good understanding of the practices used. The student body was distinguished by the companies to be very heterogeneous groups, which were usually identified by work tasks such as management or software developers.

6.2.1 Approaches used for Training

From the empirical data, two groups could be identified regarding the approaches used in the trainings. These approaches were student-centered approach and content-centered approach. In student-centered approach, aspects such as the learners' work tasks and abilities were mentioned. In content-centered approach, aspects such as relevance to real-life risks and building general knowledge were central. These two approaches can also be visible in both cyber security training and adult education frameworks.

In the empirical data, student-centered approach in teaching was brought up in the importance of the learner's role, abilities, and relevance to free time. In cyber security training framework, Karjalainen (2011) perceives that students should be seen as the vital part of the training as their previous experiences guide their learning. As a basis for her pedagogical requirements regarding effective information security she uses transformation-orientation. In addition to seeing learning to be constructed on previous experiences, Karjalainen also sees that the learning should be communal. What this means in regards to teaching approaches, is that the students as a group form new knowledge. Thus, the approach should be student-centered and the content should be formed around the learners experiences. (Karjalainen, 2011)

In addition to these pedagogical requirements, Karjalainen brought up the key entities of information security training. The entities included an explicit asset, which means that the content of the training should be seen as crucial as the learner to reach full efficiency. If the training is not relevant in the protection of the asset, then the training is not efficient and thus is unnecessary. (Karjalainen, 2011)

In her research, Karjalainen (2011) also recognizes that the objective of the training is goal-oriented, and it is noncognitive and persuasive. Based on Siponen et al. (2006), she argues that IS security training needs more normative training approaches, as the security procedures can be assimilated to norms rather than facts. Persuasiveness is needed in IS security training as the commitment to change is low. Non-cognitivism is based on the fact that the IS security procedures are not necessarily based on any science or facts but on organizational context. Lastly Karjalainen notices that IS security trainings usually are focusing on employees' routine work instead of the focus being on exceptional cases or situations. (Karjalainen, 2011) This then indicates that Karjalainen also sees the content of the training to be as relevant as the learner's previous experiences and the communal construction of knowledge. In other words, both student-centered approach and content-centered approaches are used equally in Karjalainen's theory.

On the same lines is also Puhakainen (2009). As seen in previous sub-chapter, Puhakainen also has formed requirements that the training should meet in order to effective. These requirements are formed around the perception that students' previous experiences should be taken into account.(Puhakainen, 2009) This can be interpreted that Puhakainen sees student-centered approach as vital for the training.

Also in Puhakainen's design theory, the learning is happening in the third phase, which is called instructional design. Before this phase, the instructional task has been chosen and the needed skills and knowledge to reach the task level have been identified. The instructional design phase in Puhakainen's design theory is divided into two sections. The first section is for the employee to learn about the organization's principles on information classification. Also, it should emphasize the importance of the classification. It is also addressed that the learner's previous knowledge should be activated before the learning situation. The second section is about the specific risks related to the topic at hand. This should be done as instructor supervised collaborative work. (Puhakainen, 2009) In other words, the content of the training sets the goals for the training, but the skill levels of the learners in the beginning is also important to analyze, so that the training can target right aspects to reach the goals set in the beginning. Thus, Puhakainen also uses both student-centered and content-centered approaches in his design theory.

In the cyber security framework, also guidelines can be seen to approach teaching situation from both perspectives. The NIST SP 800-16 (1998) introduces a matrix, which can be used in helping to form right instructional material for the training, which are specifically targeted to the participants. The goal of the matrix is to help in developing and designing proper and targeted training for different job tasks. The matrix is built with the training content forming three categories, which are divided into sub-categories. The main content categories are:

1) Laws and Regulations
2) Security Program
3) System Life Cycle Security

The roles of the learners are divided into six categories. The categories are:

1) Manage,
2) Acquire,
3) Design and Develop,
4) Operate,
5) Review and Evaluate
6) Use. (NIST SP 800-16, 1998)

Thus, the job role of the learner is perceived to be important as well as the content. However, the guideline does not take into account the learners' roles outside of the work. The guideline is from time, when digitalization was not as central as it is nowadays, so that could be the reason for this lacking.

In adult education, the emphasis on the teaching approach is seen focused on the learner. Thus, the learner is central in the teaching regardless of the content. The framework also gives explicit claims on how the learner should be perceived in order the teaching to be effective.

In andragogy, six assumption regarding adults as learners are presented, which can be seen as guidelines for teaching as well. The first assumption is the self-concept of the learner. This means that adults should be perceived as self-directive and thus responsible for their own learning. The second and third assumption are about adults using accumulated experience as the main source for learning and that adults also have readiness to learn. The latter means that different life related aspects, such as work tasks, need to be take into consideration to ensure that adults are capable to focus on learning. The fourth assumption is about adults' orientation to learn and motivation to learn is the fifth assumption about adult learners. The last assumption is about learner's need to know. Thus, adults need to understand why they need to learn something. (Merriam & Baumgartner 2020)

Transformative learning theory also focuses on how transformative learning can be achieved from the perspective of the learner. Three fundamental aspects have been recognized in regards to transformative learning, which are seen teach for transformation. These aspects are: empowering learners, fostering critical reflection and self-knowledge, and supporting learner. With empowering learners, three aspects should be taken into consideration: (1) exercising power responsibly, (2) encouraging discourse, and (3) involving learners in decision making. (Carton, 2011, 57)

In adult education, the communal aspect of the learning is perceived in the organizational learning theory. The underlying assumption in this theory is that the organization itself is evolving through employees' learning processes. The learning can happen either intentionally or unintentionally, and the learning is communal as the overall learning is perceived to be greater than individual learning. The organizational learning is also important from the perspective of the organization as it enhances the relevance of the organization in the markets. (Merriam & Baumgartner, 2020)

Thus, as a conclusion both of the approach groups identified from the empirical data can be seen as relevant from the point of view of the frameworks. Cyber security framework had both approaches used in an equal matter, and the importance of the learner's context and the content was seen relevant. This fits with the empirical data in that in addition to dividing the approaches to content-centered and student-centered, most the companies also distinguished the student bodies regarding their work roles. This could be an indicator that they also use those roles to contextualize the learners.

In adult education framework, the focus is on the learner and thus the student-centered approach is emphasized. The adult learner can be perceived to have multiple different special qualities that should be taken into consideration in the teaching. Also, to achieve transformative learning special aspects have to be taken into consideration. This can then be seen an enhancing the justification for the companies to use student-centered approach as one way to approach the learning and teaching situation. In the next sub-chapter the pedagogical methods used will be reflected.

6.2.2 Pedagogical Methods

In the empirical data, the teaching methods used by the companies could be divided into either hands-on methods or other types of methods. Hands-on methods included methods such as gamification, practical trainings and exercises. The other types of methods were things such as lectures, discussions and going through case examples.

In cyber security training framework, Karjalainen's (2011) distinguishes effective teaching methods for information security training in one of her pedagogical requirements. She distinguishes the experiential learning is the most suitable for information security training. Thus, the teaching methods should also be such that make connections between the real world and the learner. This means that the learning should happen through critical reflection of information either by authentic problem solving or communication. With using critical reflection, the goal is to have the learner reflect their actions, beliefs, thoughts and feelings to change their meaning perspectives. She states that the teaching methods should also focus on collaborative learning. This will then allow the production of collective knowledge. In addition, to create communal perception change, teaching methods that apply communal experience through discussions concerning experiences, attitudes and behaviors towards information security issues need to be used. (Karjalainen, 2011) Thus, the methods used in the training should be ones where knowledge is built in groups via critical reflection.

Puhakainen (2009) likewise addresses the communal aspect of information security training with stating that when specific risks related to the topic are discussed, the teaching should be done as instructor supervised collaborative work. In addition to identifying the communal aspect, Puhakainen also identifies in his research that the training should enable and motive for the students to have cognitive learning moments. (Puhakainen, 2009)

The communal aspect, such as using group work, was distinguished specifically by only one company in the empirical part, but all of companies stated to train groups. Thus, some sort of communal knowledge building can have been tried. Critical reflection or cognitive thinking was not specifically identified by any of the companies in the context of methods used, but one company identified that the goal of the training should be for the learners' to understand real life risks. This learning could be perceived to happen through critical reflection. Also regarding Puhakainen's perception that the learner's previous knowledge should be activated, only 40% of the companies in empirical data addressed to give any material in advance of the training.

The NIST SP 800-16 (1998) guideline bases its perception on proper methods in that knowledge and skills building are the main goal in information security training. To achieve this, it introduces practical instructions such as lectures and demos, case studies and hands-on practice to be used. The suggested methods differ from methods used in awareness and education in that awareness should be reached with methods like media usage. Education, on the other hand, could be taught with theoretical instructions such as seminars and discussions, reading and studying, and research. This is because awareness is about identifying learning and education is about interpreting learning. Training, in the middle, is then about applying the learning is practice. (NIST SP 800-16, 1998)

The NIST SP 800-50 (2003) guideline goes one step further from NIST SP 800-16 in that it gives actual practical advice for the trainings. It, for example, states that effective training material uses technology that is easy to use, scalable, accountable and has a broad base in industrial use. The guideline also addresses some training delivery methods and suggests that multiple different methods should be used to keep the audience active. The first delivery methods is interactive video training. The method is perceived to be better than non-interactive methods, but it stated to sometimes be too expensive. The second delivery method presented is web-based training, which is also stated to be the most popular at the time of the forming of the guideline and there are no negative sides for this type of delivery Third method is non-web computer-based training, but the lack of interaction is seen as a problem. The fourth training delivery method is onsite instruction led training. This is also addressed to be one of the most popular training methods, but the problem is with large organizations, as no large number of employees can attend at the same time. Still, this is addressed to be one of the favorite training delivery methods stated by the learners. (NIST SP 800-50, 2003)

All of the companies in the empirical data stated to have at least the option to have the training online. Many had different varieties of online teaching methods from live webinars to recorded playbacks. Many companies also indicated that they would use different approaches during the training, as was suggested in the guidelines in cyber security framework. What is noteworthy is that many proclaimed to use different seminar or lecture types of methods, which might not be the best possible option if NIST SP 800-16 guideline is followed. On the other hand, as has been stated, the companies used multiple different methods so the lectures or seminars were usually paired with more hands-on methods such as practical training or exercises.

From the perspective of adult education, the methods used by the companies could be seen also somewhat relevant. Andragogy has six assumptions on the adult learner, and it also has six guidelines on how to take these assumptions into account in the learning situation. First, the teaching climate needs to be adult-friendly and learners need to be provided with the experiences of planning, self-diagnosis and self-evaluation. Second, the emphasis in the teaching should be on experiential techniques and practical application. In addition, the learners need to learn how to learn from experience. Thirdly, proper timing and grouping of the training needs to be addressed. Fourthly the context of the practical concerns of the learners in the training should be used. Fifth, the facilitator should recognize why the learner is participating in the teaching event. Lastly, the facilitator needs to provide a rationale to the learners on the course-objectives and activities. (Merriam & Baumgartner 2020)

From this list, the companies in the empirical part can be perceived to apply at least two. These are number two and four, where the emphasis is in experiential techniques such as practical training or exercises and the learner's context is taken into account. The companies can also apply other guidelines as well, but they do not come up in the answers explicitly, such as making sure the timing is correct. The timing of the training can be seen as important also in the context of cyber security framework, as Puhakainen (2009) in his meta-requirements states that the constrains caused by the learning tasks and the environment should be taken into account in the training (Puhakainen, 2009). The companies in the empirical data could meet this requirement with the possibility of watching a recorded training session when it suits the learner.

To achieve transformative learning experience, experiential learning methods can be used. Methods such as field trips, job shadowing, service learning and other real-life case work have been seen to be efficient in creating transformation with adults. However, case works have to be able to give new perspectives to adults in order for them to be have the critical reflection moment. This critical reflection is necessary in transformative learning for learning to be truly transformative. The facilitator can help this by having discussions before and after the case work, and beforehand encourage in writing journals and do critical questioning. The facilitator needs to make sure that the guidelines for the journal are clear so that the students know what needs to be focused on. Also, the danger is that the journal will turn out to be just a simple log of what happened. (Carton, 2011, 57)

As was brought up in Karjalainen's perception on methods for information security, experiential learning theory bases its perception that experience is the source for adults to learn. The learner also needs to have a conflict in the perception on how they perceive something in order to be able to have the perception change. The perception is also that learning should be conceived as a process instead of just the outcomes. (Kolb, 1984, 34)

The answers from the empirical data, for the most part, did not distinguish that critical reflection would necessarily be happening in their trainings. Still, some of them did identify to use methods that could enhance this reflection such as using real-life case examples. With the question whether critical reflection or transformative learning has happened during the training, the role of the time cannot be overlooked. Many of the companies stated that their trainings lasted for about an hour. Whether a training session was done more than once with the same group was not distinguished. In the answers, it was also stated that trainings where a certain skill was being taught, such as how to react to something, were usually longer lasting than knowledge building trainings.

In the next sub-chapter, the role of the facilitator will be reflected. This is something that is lacking in the framework of cyber security, but as it has great emphasis in the adult education framework especially regarding learning, it was decided to be perceived a bit more closely.

6.2.3 Facilitator

Most of the answers in the empirical data stated that the trainers were subject-experts. Few stated that there were also some trainers with pedagogical background, but the majority had no pedagogical training. Also, it was instigated that no pedagogical requirements were set for the trainers from the companies' side. In adult education framework, the role of the facilitator is perceived to be crucial especially in the learning theories. Without proper facilitator, the perception is that the learning process cannot reach its full efficiency.

As Karjalainen (2011) brings up that the communal aspect of the information security training is important, the role of discourse can be seen to have a crucial role when targeting transformative learning. Thus, it is especially important for the facilitator to recognize the role of discourse in the empowerment process as the participation in the dialog may not be equal or occur naturally. Thus, the facilitator's task is to find different ways to stimulate to discussion, without regulating it or dismissing learner's contribution. In addition to making sure that the discourse and dialog is respected, the facilitator should also involve the learners in the planning phase of the training. This could mean choosing all or few of the topics taught. Also, the methods used in the teaching event could be chosen by the learners and keep decision-making open and explicit. (Carton, 2011, 57)

The facilitator should also make sure, especially in transformative learning, that learners have the chance for critical reflection and critical self-reflection. One way a facilitator can help with this is by asking questions. Facilitators can ask the learners what assumptions they are making about a process and then challenge those assumptions underlying the process. The questions can vary from what the learners' beliefs are regarding a certain matter, how they came about with these beliefs and why they regard that these beliefs are of value. (Carton, 2011, 57)

In transformative learning, special attention by the facilitator needs to be given to the fact that the learners might have held on for some of the transformed assumptions for a very long time. For that reason, the facilitator should be one who is encouraging in the process and not judgmental. The facilitator should know the learners and be aware of what is happening in their lives at the moment for the learning to be truly transformative. The other learners can be given the responsibility in keeping the atmosphere such that everyone is able to freely and without prejudice do critical self-reflection. The learners are also able to receive support from the network for the process as well as form lasting networks to reflect upon in the future. (Carton, 2011, 57)

In comparison to transformative learning, experiential learning sees that excellent facilitators understand one's unique way of learning from experience. They are also perceived to need to have the ability to intentionally direct and control one's learning. In experiential learning theory, it is seen that the ability to deliberately learn from experience is the most powerful source in adult learning. Deliberate experiential learning draws from three areas: (1) mindfulness, (2) metacognition, and (3) deliberate practice. The main focus is that individual is able the control their learning process by conscious metacognitive control. Thus, metacognition allows them to monitor and select learning approaches that are suited for them depending on the situation. (Kolb & Kolb, 2017, 114) Thus, the facilitator's task is to guide in this process.

Experiential learning theory also recognizes the importance of subject-matter experts as facilitators. Still, it does so with some precautions. Experiential learning theory perceives that extensive knowledge in itself does not meet the criterion of a true expert experiential educator. This is because facilitator should also encompass the knowledge and understanding of how students create meaning of their experience. The underlying problem is seen to be that experts are usually unable to connect to the experiences of the learners, as they are only able to rely on their current experiences. Less experienced subject educators have been seen to be able to connect with the learners better as they can relate to the experiences the learners have. (Kolb & Kolb, 2017, 386)

Subject-matter expert as a facilitator should use different approaches to connect with the learners if experiential learning is the aim. First, the facilitator should try to connect the subject matter to learners' interests. This means that the facilitator has to recognize what interests them personally and try to understand what might interests the learners. This might not be something that the facilitator is interested about, but still has to be introduced so that the learners' interest is awaken. The second guideline is that the facilitator should organize the subject matter around concepts central to the discipline. With this, the facilitator gives the keys to the learners to understand the subject in the future as well in a higher level of complexity. (Kolb & Kolb, 2017, 388)

The third guideline for facilitators is that they should try to image the learners' minds. This will allow the facilitator to grasp where the learners' might stumble to understand. Fourth guideline is that less is more. Covering a lot of content does not mean that the learners' are able think in depth. It takes time for experiential learning to go through the full cycle. Fifth guideline states that the facilitator should draw out mistakes. This sets excellent facilitators apart from good ones as the excellent facilitators see learners' mistakes as a chance to get to understand how they learn. (Kolb & Kolb, 2017, 389)

The last two guidelines are on the punctuation of the experience and the need to study learning. This means that the facilitator should encourage revision at the end of the training as that way the learners' are able to then reflect on what they have learned. This also gives the facilitator a chance to see what the learners have perceived to be important enough to have learned it. The facilitator should also study learning as excellent facilitators see teaching as a scientific process, which should be studied. (Kolb & Kolb, 2017, 390)

In regards to the facilitators, experiential learning also distinguishes that those who might not be experts in the subject, should take few extra aspects into account. First, they should establish a climate of trust and safety. They should also elicit and support a meaningful purpose of learning. In addition, they should promote inside-out learning and encourage expressions of thoughts, feelings, and emotions. Lastly, they should also make themselves available as learners and accept their limitations. (Kolb & Kolb, 2017, 394)

As seen, the role of the facilitator is seen as crucial for the learning to be successful. Still, even though the trainers in the trainings might not have pedagogical background, they can be good facilitators from the perspective of experiential learning. Many of the trainers might already practice some of the methods that have been mentioned in this sub-chapter, but which did not come up in the empirical part. Also, some of the aspects are such that only the learner could be seen as relevant to say whether it had been done, such as creating atmosphere.

Next, the aspects that are implemented after the training will be deliberated.

6.3 After Learning

In the empirical data, what happened after the training varied between the companies. How the effectiveness and successfulness of the training was evaluated differed between the companies. Many of the companies stated that these evaluations were left for the employees of the learners, and the training companies were not involved in this part anymore. Also, only two companies stated to do long-term monitoring on the study results.

In cyber security framework, the question on who should do the evaluation is not the key issue but more the fact that learning evaluation should be done after the training. For example, Puhakainen (2009) in his design theory has included in the last phase the "Diagnosis of Success". In this phase, the training should be evaluated in the terms of whether the goals set in the first phases have been met. This can be done in different ways, but Puhakainen suggests methods such as surveys and interviews. The questions can be directed to either the participants, their co-workers or their employers to see how the learners' behaviors have possibly changed. (Puhakainen, 2009)

Karjalainen also sees this evaluation step vital, and her fourth pedagogical requirement is on the evaluation of the learning. In her theory, the evaluation should focus on experiential and communication-based methods, and the viewpoint should be on the learning community. The learners should also be seen as active participants in this process, with having the responsibility to do self-evaluation and reflection. This evaluation should be continuous throughout the training. The learners should also be able to give feedback to their peer-students to enhance the communal learning. Thus, the evaluation phase is not only to reflect what has been learned but also gives the possibility for new learning experiences. (Karjalainen, 2011)

NIST SP 800-50 (2003) guideline has a special section where post-implementation is discussed. Its main perception is that continuous improvement should be the goal of the training as it is an area where one can never do enough. Methods to do this post-implementation are presented to be manyfold. For example, monitoring compliance by different actors such as CIOS and IT security program managers are explained. In addition, evaluation and feedback are stated to be critical components in to ensure continuous improvement for the training. Different methods to do evaluation and receive feedback are presented in figure 6.

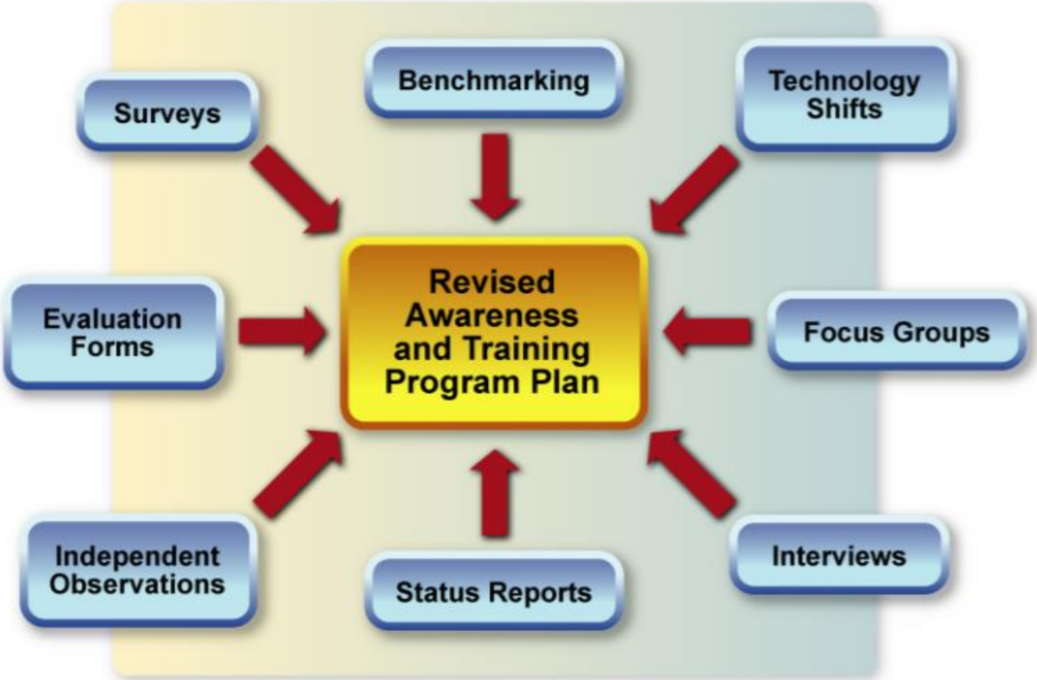


Figure 6 Evaluation and Feedback Techniques (NIST SP 800-50, 2003, p.37)

A feedback strategy is also introduced, which should have account quality, scope, deployment method, level of difficulty, ease of use, duration of session, relevancy, currency and suggested modifications. (NIST SP 800-50, 2003) It of course has to be taken into account that the guideline has been formed regarding mostly in-house trainings, where the post-implementation is done by the employers such as was also mentioned in the empirical data.

The most used method in evaluating the effectiveness of the training was stated by the companies to be customer feedback. Only few of the companies evaluating the effectiveness stated to use also other methods such as exams or quizzes. None of them brought the communal aspect forward, which was identified by Karjalainen (2011).

How to evaluate learning effectively has been raised in the adult education framework. The most noted aspect is that the methods chosen for the evaluation should fit with what is being evaluated. Thus, different methods should be used when evaluating instrumental knowledge or transformative knowledge. (Harva, 1971, 134) With transformative learning the debate has been how to evaluate transformative learning in instructional setting. Most of the methods are based on the learner to explain their learning process. This can be done either by either interviews, writing journals, doing videos or case studies. The underlying problem in evaluating transformative learning is perceived to be the fact that transformative learning is emancipatory in nature rather than instrumental. Thus, the facilitators can create an atmosphere which should enhance transformation, but they cannot force it to happen. Also, a competent facilitator is capable to recognize this transformation in the learners. (Merriam & Bierema, 2013)

The success of the training was also mostly evaluated by costumer feedback. One company identified that they measured it with questions to see how understanding of the taught matters had changed. This can be seen to mean that only one company perceived that the training was successful if some sort of knowledge building could be evaluated. The other based the success rate on how the learners evaluated the training. Customer feedback can also include elements of critical reflection, so they can also measure transformative learning.

In adult education also the aspect is brought up of who does the evaluation and why. It is stated that if increasing the efficiency of the training is a target, the evaluation of the learner is not sufficient if the teacher does not get the results. Also, there is the need to understand fully where the good and bad learning results are deriving from. (Harva, 1971, 137) This could be seen as contradictory with the findings from the empirical data.

In the end, all the companies also perceived that their trainings could be deemed as sufficient in the learners' personal lives as well. This was due to the fact that the trainings build basic awareness, and the learned skills could be used in real-life. This perception fits in with the perception of lifelong learning in adult education framework. In lifelong learning, the main conception is that adults learn throughout their lives either intentionally or unintentionally skills and knowledge that they can use in their lives either professionally or in their personal lives. With adults learning different skills or knowledge, it cannot be astricted to be applied to only one are of their lives. Also, as has been stated, in order for adults to learn properly, the learning cases should be derived from the adult learners' lives. This also cannot be restricted to only be focused on one part of the adults lives. (Merriam & Baumgartner, 2020)

As most of the companies in the empirical part did not monitor the effectiveness of the training, NIST SP 800-50 (2003) guideline brings up the notion, why the evaluation should be relevant to all trainers. The guideline states that to be able to manage change, trainers should recognize when new skills or new designs should be implemented in the training sessions. (NIST SP 800-50, 2003). Thus, for the training companies to keep their trainings relevant, they should monitor the effectiveness.

7 Discussion

The aim of this study was to understand the phenomenon of private companies' cyber security trainings from pedagogical perspective. To achieve this goal, two research questions were formed. The first question was to find what pedagogical aspect could be distinguished from the companies, and the second question was how the gathered questions were in relation to cyber security and adult education frameworks.

22 companies were approached with an online questionnaire, which five answered. The companies varied in size and in the type of training, but all of them had business operations in Finland. The questionnaire had 20 questions regarding different pedagogical aspects. The questions were both quantitative and qualitative in nature, thus the methodology was mixed-method. Even though the answers were analyzed at the same time, more emphasize was given to qualitative answers. Those were analyzed with content analysis.

The answers of the companies were grouped in to three categories, which were derived from the frameworks of cyber security and adult education. These categories were learning principle, learning situation, and after learning. It was distinguished that the companies used three different principles in forming their trainings, which were student-centered, content-centered and customer-centered. This meant that many perceived that students' learning capabilities should be the main focus as others saw in content-centerism that the content itself should be the main focus. Some also saw that what the customer wanted was to be perceived as the most important principle regardless of the content or the student learning capabilities. Many of the companies were using more than one principle. Only few recognized to using any special theories as the basis.

In regards to learning process itself, the learning situation was approached either with student- or content-orientation. These fit with both of the reflected frameworks. Both of the main theories used in cyber security framework distinguished that students' previous knowledge should be something to address in the training, but that should not overlook the importance of the content, which should be derived from the workplace. With reflection to adult education framework, it was distinguished that many of the requirements for adults to learn were taken into consideration, such as using experiential methods. Also teaching methods and tools such as gamification, online classes and practical case works were once noted in the cyber security guidelines. What could be seen as lacking in the companies' answers was the communal aspect raised in cyber security framework and the role of the facilitator emphasized in adult education framework.

In the after learning section, it was noteworthy that many of the companies did not do any long-term studies on the effectiveness on the trainings. In adult education framework, it was especially distinguished that in order for the training to evolve, this should be something done. Some of the companies did evaluate the effectiveness and successfulness of the trainings, but the method which was used for it was based on customer satisfaction. From the adult education framework, it was seen that to evaluate transformative or experiential learning is complicated. It was also perceived that the evaluation itself could be seen as learning situation. From cyber security guidelines, it was also distinguished that there are multiple different methods of evaluating the learning.

7.1 Reliability and Validity

The empirical part of this study was formed with an online questionnaire that had both open- and close-ended questions. The questionnaire was formed at the same time as the reflected frameworks, but it was decided that no special theory will guide the question formation. This was done as the goal was to understand the phenomenon of the trainings without any preconceptions.

The questionnaire was distributed by email to different companies that had business operations in Finland regarding cyber security trainings. The emails were sent to contacts found on the companies' webpages. In the email it was stated that if the person receiving the email was not in charge of the trainings, they should forward it to someone who is. This way it was made sure that all the answerers had sufficient knowledge regarding their trainings. The questionnaire was open for five weeks, and it was such that the answerers could save the answers and continue later on.

In the end five different companies answered the questionnaire. It was deemed to be sufficient, as the goal of the research was to identify different pedagogical aspects of the companies. As the phenomenon has not been studied before, there was no way of knowing what the saturation point would be so the decision on sufficiency was based on the quality and depth of the answers. Based on those, the answers from five companies was enough.

To make sure that only one answer from each company was analyzed, the answerer had to identify the company they worked in and what their status in the company was. There were no duplicate answers that should have been disqualified. During the analyzing phase, the companies could not be identified from the answers. This was done to be sure that no prejudice about the company could affect the analysis of their answers. Both open- and close-ended questions were analyzed at the same time, to also make sure that no biases could be formed from there. Still, the emphasize was on the open-ended-questions as they were in the beginning perceived to give more thorough answers compared to close-ended question.

This study did not answer the question on whether the trainings are in fact efficient or not, as that would need a wider understanding of the phenomenon. Instead, the focus was on the phenomenon from the perspective of pedagogical aspects, as it was deemed that it would only need the answers of the companies and not anyone else's. Thus, the gathered data answers the questions set for this research.

7.2 Implications for Further Research

This research will give the understanding of the phenomenon of private companies providing cyber security trainings from the pedagogical sense. In the future this research can help in forming official requirements and standards regarding private companies' trainings as there is knowledge on what different aspects are found in the trainings.

This study can be used in the future to help in planning a study regarding the effectiveness of the trainings. This study gives the understanding of what methods have been used, and thus in the future those methods can be specifically targeted in the research regarding effectiveness.

In addition, aspects to be looked in the future could be the perspectives of the students as well as the companies buying the trainings. With those perspectives, the question on whether the trainings are in fact efficient in teaching cyber security could be answered. At least, without the perception of the students, this question cannot be properly answered.

The providing companies are also able to gain from this research as they are able to see how their methods, perceptions and approaches fit with the frameworks of adult education and cyber security. They can also see what their trainings could lack and what practices are in use in other companies. This study also gives the academic world the understanding of what is done in the field of cyber security. Most of the companies answered to not using any specific theories as the basis for their trainings. This should be something that the academic world should address. Theories formed in the academic world should be ones that are also used in practice as without the usage they do not serve any purpose.

In addition to studying the trainings and their effectiveness, the trainings should also be studied from the perspective of society. This means that the trainings should be perceived as the main teachers for working adult population, and thus are very crucial in the building of national resilience regarding cyber security. As the field is growing and more companies are entering the business, the society should address this issue of adults learning at workplace the needed cyber security skills that they also might apply at home.

8 SOURCES

Aaltola, K. & Taitto, P. (2019) Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training. *Information & Security: An International Journal* 43, no. 2 (2019): 123-133. Retrieved https://www.theseus.fi/bitstream/handle/10024/264740/Aaltola_Taitto.pdf?sequence=1&isAllowed=y

Amankwa, E. Loock, M. & Kritzinger, E. (2014). "A conceptual analysis of information security education, information security training and information security awareness definitions," *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014),* London, pp. 248-252. Retrieved https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/7038814

Bourke, J., Kirby, A. & Doran, J. (2016). *Survey & questionnaire design: Collecting primary data to answer research questions*. Ireland: NuBooks, an imprint of Oak Tree Press.

Bryman A.(2006). Integrating quantitative and qualitative research: how is it done? *Qualitative Research.* 2006;6:97–113.

C, Ruth. (2020, December 16). 1 in 5 employees fall for phishing emails even after a security training. (Retrieved 7.4.2020). https://atlasvpn.com/blog/1-in-5-employees-fall-for-phishing-emails-even-after-a-security-training

Carton, P. (2011). Adult Learning and Instruction: Transformative-Learning Perspectives. In Rubenson (ed.) *Adult Learning and Education.* Elsevier: Academic Press.

Check, J. & Schutt, R. (2012). Science, schooling and educational research. In *Research methods in education* (pp. 2-20). SAGE Publications, Inc., https://www-doi-org.ezproxy.jyu.fi/10.4135/9781544307725

ENISA. (2010). *The new users' guide: How to raise information security awareness.*

ENISA. (2015). *Stocktaking on Exercises: The 2015 Report on National and International Cyber Security Exercises Survey, Analysis and Recommendations.*

Harva, U. (1971). *Aikuisten opettaminen.* Kustannusosakeyhtiö Tammi : Helsinki.

Hautamäki, J., Karjalainen, M., Hämäläinen, T., & Häkkinen, P. (2019). Cyber security exercise : Literature review to pedagogical methodology. In L. G. Chova, A. L. Martínez, & I. C. Torres (Eds.), *INTED 2019 : 13th annual International Technology, Education and Development Conference,* pp. 3893-3898. Valencia: IATED Academy. Retrieved https://library.iated.org/view/HAUTAMAKI2019CYB

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., et al. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences.* 10, 5702.

Heikkinen, A. (2014). *Päteviä vai Sopivia aikuiskasvatustieteen ammattilaisia?* In A. Heikkinen & E. Kallio (ed.) Aikuisten kasvu ja aktivointi. Tampere: University Press. Retrieved https://www.ellibslibrary.com/book/978-951-44-9686-8
Hendrix, M., Al-Sharbaz, A. & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cybersecurity training? *International Journal of Serious Games,* Volume 3 (1).

Hesse-Biber, S.N.(2010). *Mixed Methods Research : Merging Theory with Practice.* Guilford Publications, ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=471119.

International Organization for Standardization. (2013). *Societal security – Guidelines for exercises* (ISO 22391:2013). Retrieved https://www.iso.org/obp/ui/#iso:std:iso:22398:ed-1:v1:en

Jarvis, P. (2004). *Adult Education and Lifelong Learning: Theory and Practice.* Taylor & Francis e-Library. https://www.ellibslibrary.com/book/0-203-34476-6

Kallio, E. (2016). Aikuisuuden ajattelun kehityksen laaja kenttä – perusteita ja avoimia kysymysyksiä. In E. Kallio (ed.), *Ajattelun kehitys aikuisuudessa – Kohti moninäkökulmaisuutta (15-56).* Jyväskylä: Yliopistopaino.

Karjalainen, M. (2011). *Improving Employees' Information Systems (IS) Security Behavior Toward A Meta-Theory of IS Security Training And A New Framework For Understanding Emploees' Is Security Behavior.* (Thesis). University of Oulu. Retrieved http://jultika.oulu.fi/files/isbn9789514295676.pdf

Karjalainen, M. & Kokkonen, T. (2020). Review of Pedagogical Principles of Cyber Security Exercises. *Advances in Science, Technology and Engineering Systems Journal* Vol. 5, No. 5, 592-600.

Kolb, D.A. (1984). *Experiential Learning: Experience as The Source of Learning and Development.* US : Prentice Hall, Inc.

Kolb, A. Y. k. & Kolb, D. A. (2017). *The experiential educator: Principles and practices of experiential learning*. EBLS Press.

Lemmetty, S. (2020). *"Self-Learning is Present Every Day – in fact, it's my job" – Self-Directed Workplace Learning in Technology-Based Work.* (Thesis). University of Jyväskylä. Retrieved https://jyx.jyu.fi/bitstream/handle/123456789/71221/978-951-39-8196-9_vaitos04092020.pdf?sequence=1&isAllowed=y

Malinen, A. (2000). *Towards the Essence of Adult Experiential Learning – A reading of the theories of Knowles, Kolb, Mezirow, Revans, and Schön.* (Thesis). University of Jyväskylä:SoPhi.

Merriam, S.B. & Bierema, L.L. (2013). *Adult Learning: Linking Theory and Practice.* US:John Wiley & Sons, Incorporated. Retrieved https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/reader.action?docID=1376941

Merriam, S.B. & Baumgartner, L.M. (2020). *Learning in Adulthood: A Comprehensive Guide.* US:John Wiley & Sons, Incorporated. Retrieved https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/reader.action?docID=6007459

Mezirow, J. (2008). *Contemporary Theories of Learning : Learning Theorists ... in Their Own Words.* By Knud Illeris (ed.), Routledge, 2008. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=425525.

National Institute of Standards and Technology. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (NIST SP 800-16). Retrieved https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151633

National Institute of Standards and Technology. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST SP 800-50). Retrieved https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Newby, P. (2014). *Research methods for education* (Second edition.). London: Routledge, Taylor and Francis.

Nykänen, K. (2011). *Evaluation of the effectiveness of information security training on the information security behavior of individuals and organizations.* (Thesis). University of Oulu. Retrieved http://jultika.oulu.fi/files/isbn9789514295713.pdf

Poikela, E. & Poikela, S. (2014). *Ongelmaperustainen aikuisopiskelu – tarinankerronta osana oppivaa matkailua.* In A. Heikkinen & E. Kallio (ed.) Aikuisten kasvu ja aktivointi. Tampere: University Press. Retrieved https://www.ellibslibrary.com/book/978-951-44-9686-8

Puhakainen, P. (2006). *A Design Theory For Information Security Awareness.* (Thesis). University of Oulu. Retrieved http://jultika.oulu.fi/files/isbn9514281144.pdf

Puhakainen, P & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*. 34. 757-778.

Reid, R. & Van Niekerk, J. (2014). "From information security to cyber security cultures". *Information Security for South Africa, Johannesburg,* pp. 1-7. Retrieved https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/6950492

Rosaline, B. (2008). *The scope and contribution of qualitative research.* In Introducing qualitative research (pp. 9-34). SAGE Publications, Ltd, https://www-doi-org.ezproxy.jyu.fi/10.4135/9780857029034

Schoonenboom, J., & Johnson, R. B. (2017). *How to Construct a Mixed Methods Research Design.* Kolner Zeitschrift fur Soziologie und Sozialpsychologie, 69(Suppl 2), 107–131. https://doi.org/10.1007/s11577-017-0454-1

Stake, R. E. (2010). *Qualitative research: Studying how things work.* New York: Guilford Press.

Siponen, Mikko. (2001). Five dimensions of information security awareness. *Computers and Society*. 31.

Siponen M, Pahnila S & Mahmood A (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance. *Innovations in Information Technology:* 1–5.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research,* Volume 104, Pages 333-339. Retrieved https://www.sciencedirect.com/science/article/pii/S0148296319304564

Tashakkori, A., & Teddlie, C. (2010). *SAGE handbook of mixed methods in social & behavioral research* (2nd ed.). SAGE Publications, Inc. https://www.doi.org/10.4135/9781506335193

Teddlie CB & Tashakkori A.(2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences.* Los Angeles: Sage.

Traficom. (2019). *Kyberharjoitusohje : Käsikirja harjoituksen järjestäjälle.* 2019(26).

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos.). Helsinki: Kustannusosakeyhtiö Tammi.

Valli, R. & Aarnos, E. (2018). *Ikkunoita tutkimusmetodeihin: 1, Metodin valinta ja aineistonkeruu : virikkeitä aloittelevalle tutkijalle* (5., uudistettu painos.). Jyväskylä: PS-Kustannus.

Vanhalakka-Ruoho, M. (2014). *Aikuisten opiskelu, työ ja elämässä suunnanotto ohjauksen ja neuvonnan mahdollisuutena.* In A. Heikkinen & E. Kallio (ed.) Aikuisten kasvu ja aktivointi. Tampere: University Press. Retrieved https://www.ellibslibrary.com/book/978-951-44-9686-8

Weber, R. (1990). *Content classification and interpretation.* In Basic content analysis (pp. 16-40). SAGE Publications, Inc., https://www-doi-org.ezproxy.jyu.fi/10.4135/9781412983488

APPENDIX 1 QUESTIONNAIRE

1) Yritys, jonka koulutusta vastaukset käsittelevät.
   Company that is represented in the answers.

2) Vastaajan ammattinimike yrityksessä.
   Answerer's job title in the company.

3) Yrityksenne tarjoaa:
   Your company provides:
   - Koulutusta / *Training*
   - Simulaatioita/Harjoituksia - *Simulations / Exercises*
   - Yhdistettyjä koulutus-simulaatioita/harjoitteita - *Combined training with simulations/exercises*

4) Oletteko tietoisesti hyödyntäneet jotain pedagogista teoriaa koulutuksienne suunnittelussa? *Have you intentionally used any pedagogical theory as a base when planning trainings?*
   - Kyllä, mitä? *Yes, what?*
   - Ei / *No*

5) Oletteko tietoisesti hyödyntäneet jotain tieteellistä tutkimusta koulutuksia suunniteltaessa? *Have you intentionally used any scientific research as a base when planning trainings?*
   - Kyllä, mitä? *Yes, what?*
   - Ei / *No*

6) Minkä koette olevan ensisijainen lähtökohta koulutuksissanne?
   What would be the primary basis in your trainings?

7) Mitkä koette olevan tärkeimpiä asioita, mitä tulee ottaa huomioon kyberturvallistuutta opettaessa? *What do you think are the most important things to be taken into consideration when teaching cyber security?*

8) Kuvaile koulutuksenne sisältö lyhyesti. *Shortly desrcibe the content of the training.*

9) Kuinka toteutatte koulutuksen? *How do you implement trainings?*

10) Kuinka kauan koulutuksenne kestää? *How long does the training last?*

11) Saavatko osallistujat ennakkomateriaaleja ennen varsinaista koulutusta? *Do the participants get any material in advance before the training?*

    - Kyllä, mitä? *Yes, what?*
    - Ei / *No*

12) Ketkä toimivat koulutuksen vetäjinä? (esim. taustakoulutus) *Who implement the training? (ie educational background)*

13) Kuinka mittaatte koulutuksen tehokuutta? *How do you measure the effectiveness of a training?*

14) Kuinka mittaatte koulutuksen onnistumista? *How do you measure the success of a training?*

15) Teettekö / oletteko tehneet pitkäaikaisseurantaa koulutuksen vaikuttavuudesta? *Have you done any long term monitoring on the effects of the training?*

    - Kyllä, Kuinka? *Yes, how?*
    - Ei / *No*

16) Räätälöidäänkö koulutuksenne asiakaskohtaisesti? *Are trainings tailored according to costumer?*
    - Kyllä, mitä asioita otetaan huomioon? *Yes, what are taken into consideration?*
    - Ei / *No*

17) Koetteko, että koulutuksestanne on hyötyä myös osallistujien siviilielämässä? *Do you think that your training is also useful to trainees regarding their private life?*
    - Kyllä, miksi? *Yes, why?*
    - Ei / *No*

18) Minkä kokoisia ryhmiä koulutatte kerralla? *What size groups are trained at a time?*

19) Missä koulutus pidetään? *Where does the training take place?*

20) Kuvaile tyypillinen opiskelijaryhmänne. *Describe your typical student body.*

In the end, the participants could leave their contact information to hear about the results.