Security training gap analysis in Company X

Annette Forsell

2018 Laurea

Laurea University of Applied Sciences

Security training gap analysis in Company X

Annette Forsell
Security Management
Bachelor's Thesis
November 2018

Laurea University of Applied Sciences **Abstract**
Security Management

Annette Forsell

Security training gap analysis in Company X

2018 2018 Pages 59

This bachelor's thesis is conducted as a case study and is commissioned by a company that is called in this research as Company X. The objectives of this study are to determine gaps between of the case company's security training system's current and desired states by using gap analysis methodology. The identified gaps are improvement opportunities for the case company to ensure that their security training system is compliant with different requirements in the future.

The current state of the case company's security training system is researched to understand how security training is organized in the case company now. The current state analysis is conducted by running a quantitative questionnaire to the company's employees, interviewing four managers and analysing the company's current training materials. The desired state of the security training system is determined by using content analysis to study relevant acts, security standards and guidelines. The theoretical framework includes the desired state and functions of corporate security, successful security training systems and some pedagogics.

The current state analysis indicate that the company's employees are interested on their own and their employer's safety and security. The case company educates employees in security, but the held training sessions are mainly focused on new employees and on current employees' voluntary participation. Mandatory annual security trainings are carried by asking employees to read the case company's Security & Safety guidebook and then sign a form that they have done this.

Based on the conducted gap analysis there were identified gaps which are improvement opportunities. The case company is recommended to provide their employees with more regular security training and steadier updates on current security related topics. During the gap analysis there were identified some required subjects that are missing from the case company's current security training program. These topics include remote working policy, mobile device policy, crypto graphic's policy and threats of malwares. These topics are recommended to be added to the case company's security training system in the future to ensure compliance with legislation and different security standards.

Keywords: security, training, gap, analysis, compliance, improvement, opportunity

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma

Annette Forsell

Security training gap analysis in Company X

2018 2018 Pages 59

Tämä opinnäytetyö on toteutettu tapaustutkimuksena ja työn toimeksiantajana toimivaa yritystä kutsutaan tutkimuksessa nimellä Yritys X. Tämän tutkimuksen tavoitteena on määrittää mahdolliset kuilut toimeksiantajayrityksen turvallisuuskoulutusjärjestelmän nyky- ja tavoitetilan välillä käyttäen kuiluanalyysin metodologiaa. Kuilut nähdään kehitysmahdollisuuksina, jotka täyttämällä yritys voi jatkossa varmistua siitä, että heidän turvallisuuskoulutuksensa on vaatimustenmukainen.

Yrityksen turvallisuuskoulutuksen nykytilatutkimuksen tavoitteena on selvittää, miten kattava nykyinen koulutusjärjestelmä on. Nykytilatutkimukseen on käytetty yrityksen työntekijöille suunnattua määrällistä verkkokyselyä, haastattelemalla neljää esimiestä ja analysoimalla yrityksen nykyisiä koulutusmateriaaleja. Turvallisuuskoulutuksen tavoitetila on määritelty käyttämällä sisällönanalyysia tutkittaessa valikoituja lakeja, turvallisuusstandardeja ja -ohjeita. Tutkimuksen teoreettisen viitekehyksen muodostavat tavoitetilatutkimuksessa käytetyt lähteet sekä yritysturvallisuuden aspektit, menestykselliseksi todetut turvallisuuskoulutusjärjestelmät ja pedagogiikan perusteet.

Nykytilatutkimus osoittaa, että yrityksen työntekijät ovat kiinnostuneita omasta ja työnantajansa turvallisuudesta. Toimeksiantajayritys kouluttaa työntekijöilleen turvallisuusasioita, mutta koulutus keskittyy uusiin työntekijöihin ja nykyisten työntekijöiden vapaaehtoiseen osallistumiseen. Yrityksen vuosittainen turvallisuuskoulutus järjestetään tällä hetkellä siten, että työntekijöitä pyydetään lukemaan yrityksen Turvakansio ja kuittaamaan nimensä lomakkeeseen, että ovat lukeneet ja ymmärtäneet kansion sisällön.

Kuiluanalyysin avulla pystyttiin löytämään kehitysmahdollisuuksia yrityksen turvallisuuskoulutusjärjestelmästä. Yritykselle suositellaan, että se tarjoaa jatkossa työntekijöilleen säännöllisempää turvallisuuskoulutusta ja ajankohtaisia päivityksiä liittyen turvallisuuteen. Kuiluanalyysilla pystyttiin myös identifioimaan vaadittuja aiheita, jotka eivät kuulu nykyiseen koulutusjärjestelmään. Aiheet ovat etätyöpolitiikka, mobiililaitepolitiikka, kryptografiapolitiikka ja uhka haittaohjelmista. Edellä mainitut aiheet suositellaan lisättäväksi osaksi yrityksen turvallisuuskoulutusjärjestelmää, jotta se on jatkossa vaatimustenmukainen.

Keywords: security, training, gap, analysis, compliance, improvement, opportunity

Table of Contents

1 Introduction

Any company that operates in a high security level environment must comply with several internal and external requirements. The requirements can be based on legislation, standards or the company's own security policies. To be compliant with all these requirements the company's management needs to make sure all employees are aware of the company's security procedures and guidelines to comply with the requirements. The company's security personnel, physical and technical solutions alone are not able to protect the company's assets and ensure safe and continuous operation in all situations. Security aspects should be included in all operations instead of being a separate process that is only performed by the company's security professionals. Security training needs to be a part of the company's security management system and employees should be trained to follow and adhere to the company's security policies and procedures and understand how security is tied to their everyday work. (Hight 2005)

It is important that all employees understand what is behind of the policies that they need to be compliant with. Security training should not be just a part of new employees' induction, because security requirements do change, and people naturally forget things. Security training should cover every employees' whole employment life cycle from contract signing to termination and consider on the needs of different positions inside of the company. (Hight 2005)

The objective of this bachelor's thesis is to research the case company's security training system's current and desired states by using gap analysis technique. Based on the conducted gap analysis the company is provided with a set of opportunities to close identified gaps between of the training systems desired and current states. To follow Yochum's (2018) article's guidelines about how to conduct gap analysis, the first research is run to examine the case company's security training system's current state. For the current state research there are used an online questionnaire and four unstructured interviews. The second research is performed to describe the desired state of the case company's security training system. The desired state is a situation when the company's security training system is compliant with local legislation, specified standards and with the company's own security policies. The desired state research is conducted by using qualitative data analysis to examine written documentation. The desired state also forms a part of the theoretical framework of the aimed security training system. The desired state and theoretical framework are formed by researching what functions are included in corporate security, examine internal and external requirements and some pedagogics. In the theoretical framework is also heeded how an efficient employee training could be held.

Based on the gap analysis technique, it is important to understand why there is a difference, the gap, between of the current and desired states of the subject. After current and desired

states are examined, is the final phase of the gap analysis to define how the desired state can be reached. This description is provided to the case company to show what improvement opportunities there are found based on the conducted gap analysis.

The first step in any research should be formulating a research problem. The destination of the research is identified by the research problem and the research problem should also tell the researcher, research supervisor and readers what the researcher intends to research. The clearer and more specific the research problem is, the better it is as everything that follows in the research process is influenced by the research problem. (Kumar 2014)

The research problem of this bachelor's thesis is the case company's demand to understand the current state of their security training system and to identify improvement opportunities to ensure that the training system is compliant with specified requirements in the future. The research questions were formulated to answer the research problem. For successfully conduct this research, the research questions are:

- What improvement opportunities can be identified in the case company's security training system by using gap analysis?
    - What is the current state of the case company's s security training?
    - What is the desired state of the case company security training system that is compliant with set requirements?

The research methodology and literature should be chosen to be appropriate to answer the research questions (Kumar 2014). In this bachelor's thesis are performed two separate researches and both qualitative and quantitative research and data collecting methods are used to be able to answer the research questions and solve the research problem.

The case company has defined that they aim to comply with the local legislation, specified standards and KATAKRI's guidelines. Those sources form the theoretical framework and the desired state for the security training system, together with aspects of corporate security functions and pedagogics.

Despite of the case company's security policies and guidelines being confidential, are readers provided with an extensive understanding of the company's security training system's current and desires states and improvement opportunities based on the research results. The readers will be able to understand what is advised to be done in the case company to close the gaps between the security training system's current and desired states.

During this bachelor's thesis, it is not aimed to generate any general theory of security training systems and the results are not generalizable outside of the case company. Companies operating in the same industry might be able to benefit from the results of this study while identifying their requirements for security training and its improvement. It is the case company's decision, which parts of the provided improvement opportunities they decide to implement to their security training system. This bachelor's thesis is conducted to research the case company's security training system's current and desired states and to provide the company with improvement opportunities to close the gaps between of the states. This bachelor's thesis does not include implementation actions.

2 Methodology

"Methodology is the philosophical framework within which the research is conducted or the foundation upon which the research is based" (Brown 2006). It is important to use appropriate research methods. Research methods' main function is to decide and explain how the researcher is planning to find answers to the research questions. (Kumar 2014)

This bachelor's thesis is conducted as a case study to research the case company's security training system's current and desired states using gap analysis' methodology. During the gap analysis there are conducted two separate researches, one for the current state and for the desired state. Based on the conducted gap analysis the company is provided with a set of improvement opportunities to close the gaps between of the current and desired states. To answer the research questions and reach the objectives of this mixed methods research, there are used both qualitative and quantitative research and data collecting methods as part of the gap analysis.

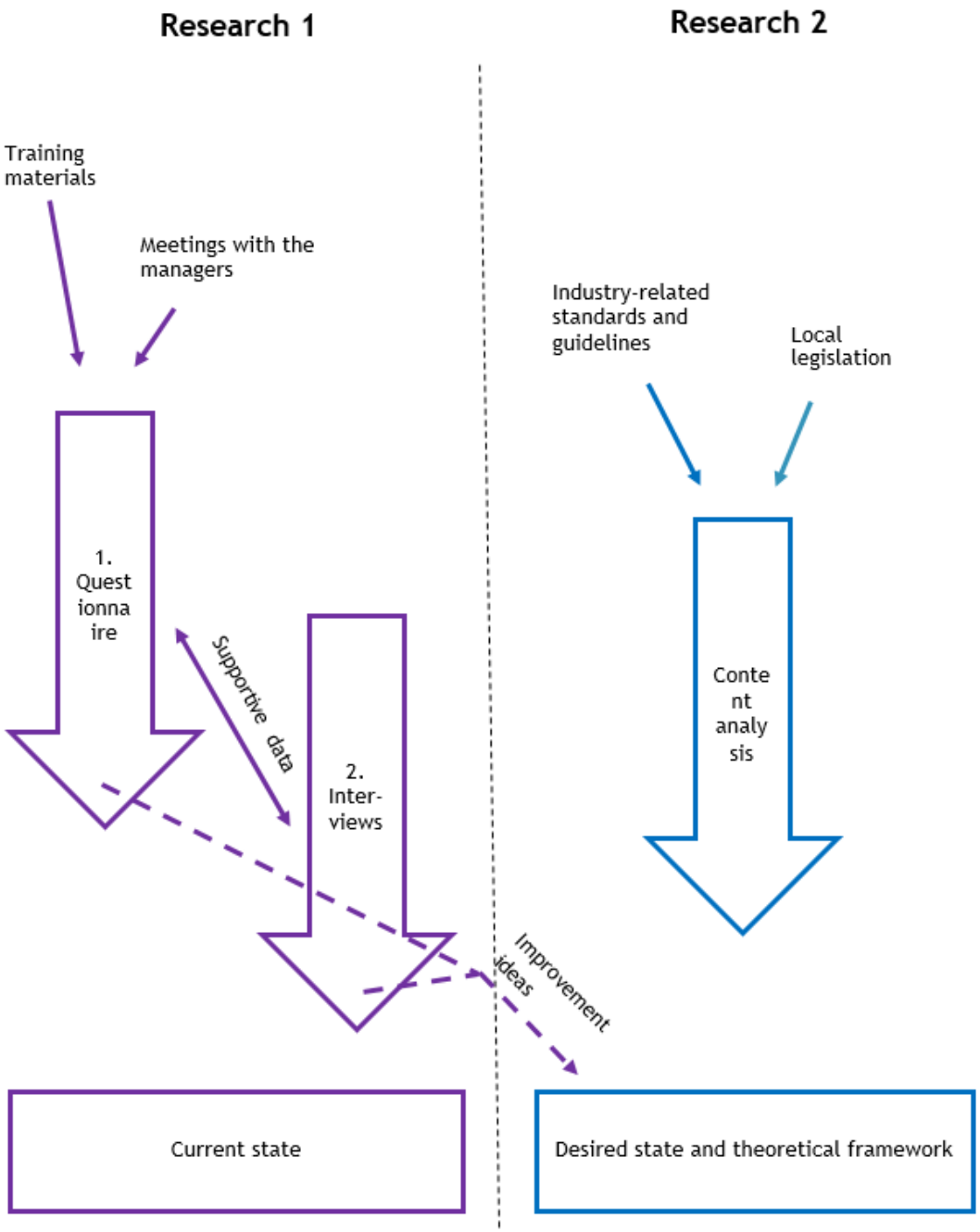


Figure 1. Data collecting methods in the researches

2.1 Mixed methods study

Creswell and Plano Clark describe (2011) mixed methods research to be a study where researcher collects and analyses convincingly and accurately both quantitative and qualitative data, uses both research methods in one study and mixes or links the two varieties of data simultaneously by merging them. Research problems that are suited for mixed methods study are problems in which one data source might be inadequate, results need to be explicated, a

second research method is needed for to supplement the primary method and an overall research goal can be best covered with several phases.

In this bachelor's thesis are used both qualitative and quantitative research methods, making this study a mixed method research. From qualitative data collecting methods are chosen unstructured interviews and content analysis and from quantitative methods is used a questionnaire to collect and analyse needed data to reach the objectives of this study. By mixing both qualitative and quantitative research and data collecting methods can researcher gain deeper understanding on research problem than using just either quantitative or qualitative methods (Creswell & Blanko 2011).

Mixed methods study is suited when researcher wants to corroborate or verify the results obtained from other research methods (FoodRisc Resource Centre 2018). For the current state research there is used a quantitative questionnaire to ask the case company's employees what security training they have received from their current employer. In the questionnaire it is also surveyed some supporting topics, for example if the employees work remotely. The employees are asked their favoured training methods for future security trainings and they are given a possibility to share their own security training development ideas. To verify and support the results of the questionnaire, are four managers interviewed in qualitative unstructured interviews.

The theoretical framework of the security training system is constituted by using qualitative content analysis. The case company has defined which industry-specified security standards and guidelines they aim to comply with and those official documents form the desired state of the security training system and the desired state is a part of the theoretical framework. In the theoretical framework it is also defined what is included in general corporate security, pedagogics and aspects of successful security training programs.

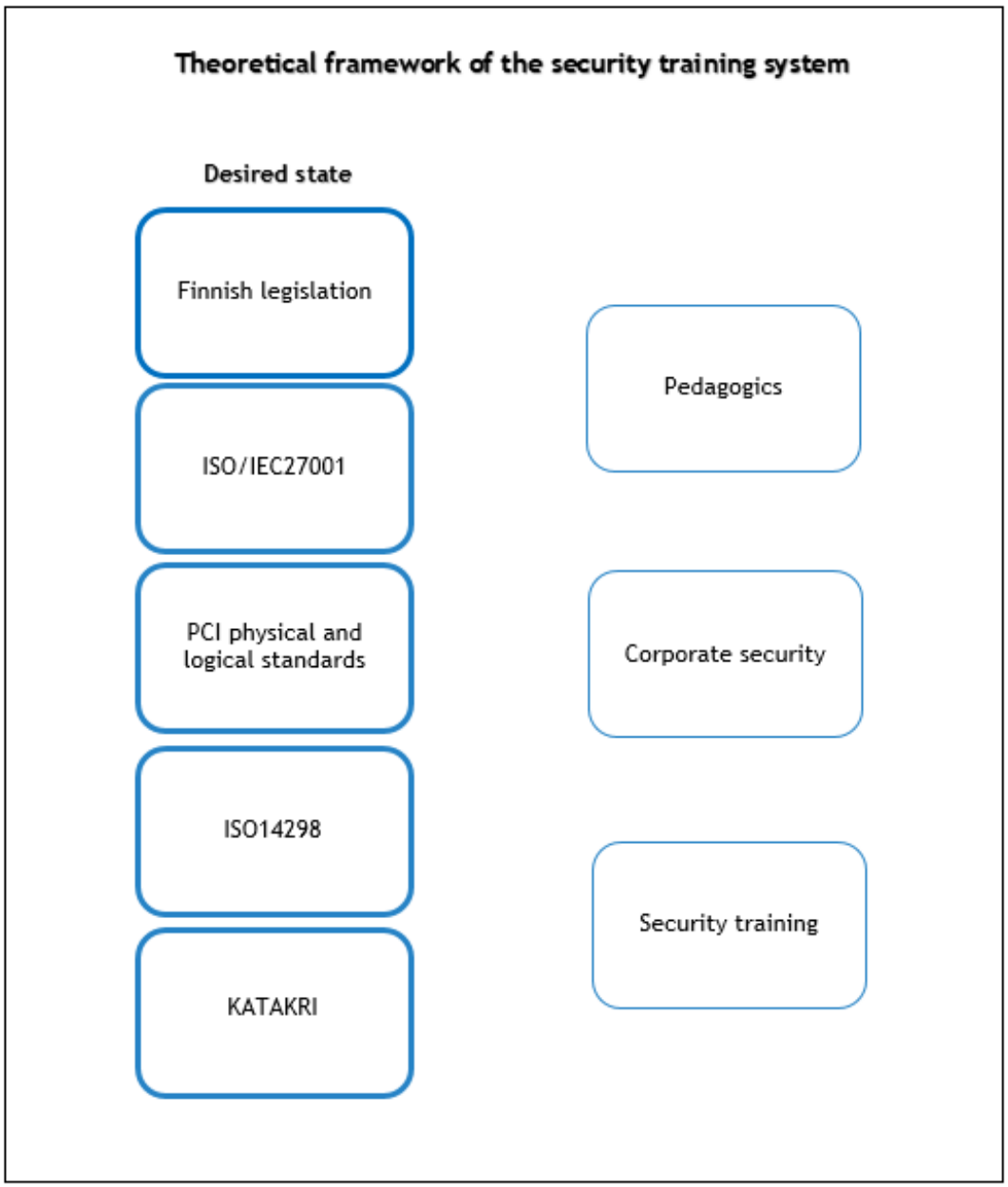


Figure 2. Theoretical framework of the security training

2.2 Case study

The term case study indicates to a method of analysis and a research design for indicating a problem. A case could be a group, an event, a town, a specific process or an individual. To call a study as case study, it is important that researcher treats the total study population as one entity. In a case study, the selected case becomes the basis of exhaustive and holistic investigation of the aspect that researcher wants to find out more. In a case study one or a few aspects are studied intensively. Case study can be a very useful design when researcher is investigating an area where they want to gain a comprehensive understanding of a phenomenon, a situation or other specific subject. (Kumar 2014)

Case study should concentrate on a single case with objective to get intensive and detailed information of the selected case. Case study should also aim to gain understanding of processes and structures in a manner that the results of a case study should be valid in broader social-culture context as well. (Koppa 2 2010)

The case of this bachelor's thesis is the case company's security training system. The objectives of this study are to provide the case company with improvement opportunities that are based on the conducted gap analysis. The improvement opportunities identify how the case company could close the gaps between of their security training system's current and desired states to ensure compliance with internal and external requirements in the future.

2.3 Gap analysis

Gap analysis can be conducted when for example a company wants to improve performance of their systems or processes. There are four main steps in the gap analysis. The first step is to identify the current state of the subject. The second step is to identify the desired state. The third step is to recognize the gaps by comparing the results of the current and desired states and understand why there is the gap. The fourth and final step is to figure out how to improve the performance to close the gap. (Yochum 2018)

Understanding of the current state is one of the most important steps to take in any project. Skipping current state analysis can lead to a situation where the project is not solving the core problem. It is hard to know, how to improve or solve anything, if you don't know where you are starting from. One mistake that is often taken in current state analysis, is that researcher studies only documentation of showing how things should be done. Many times, things are documented this way, but done that way. Therefore, it is recommended to use several methods, like document analysis, interviews, observation and questionnaires to study the current state of any subject or development target. (Crosby 2017)

The desired state can also be called as future goal or future target. The desired state is the state where the company wants to be with their performance. (Yochum 2018) The desired state in this study is a security training system that is compliant with requirements set on Finnish legislation, specified standards and guidelines, which the case company aims to comply with.

In this bachelor's thesis it is seen suitable by the author to use the gap analysis methodology to answer the research questions and solve the research problem. The gap analysis methodology was chosen, because during this bachelor's thesis the case company's security training system's current and desired states are examined. Based on the current and desired state researches the case company is provided with a set of improvement opportunities to close the gaps between of the examined states.

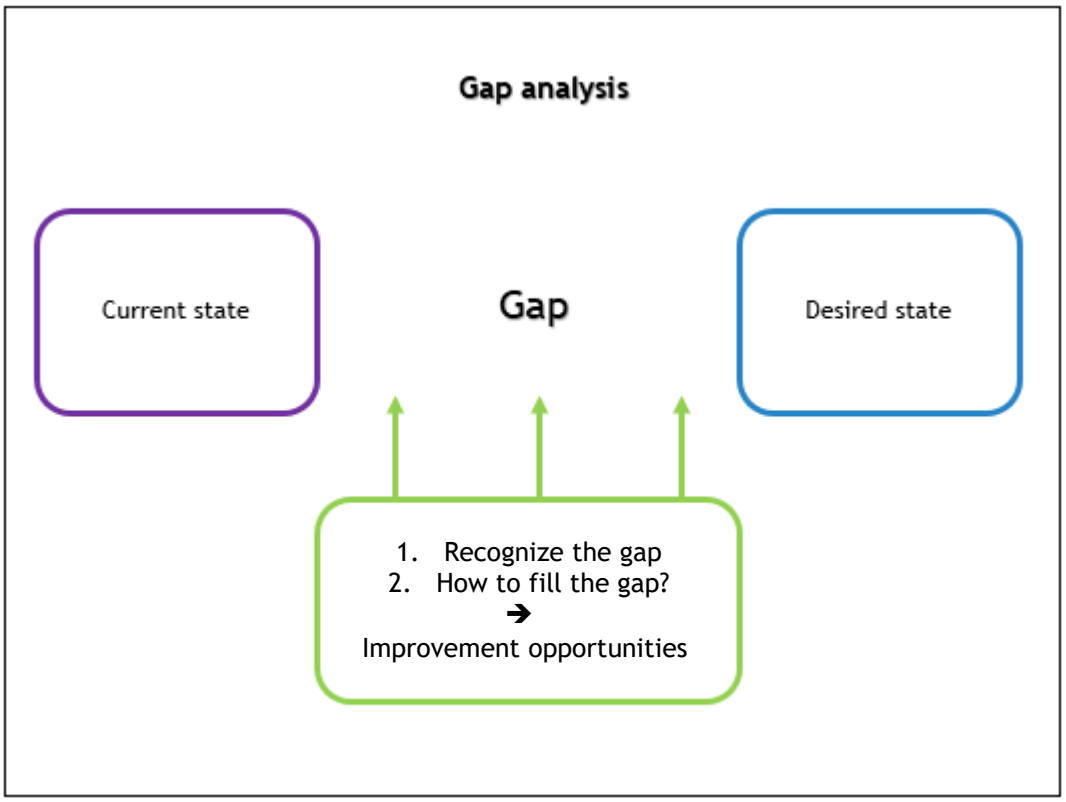


Figure 3. Gap analysis.

2.4 Qualitative research

The term 'qualitative research' is a broad term that includes a wide range of techniques and philosophies. In general, qualitative research is an approach that lets researcher to examine people's experiences by using qualitative data collecting methods for example depth interviews, content analysis, observation and biographies or life histories. Qualitative research's objectives can be to get detailed understanding of reasons, processes or meanings. Purpose of the qualitative research can be to be able to describe why? How? What is the process? Qualitative research's outcome is to develop an initial understanding of the subject or to be able to explain behaviours and appearances. (Hennink, Hutter & Bailey 2011)

In this bachelor's thesis qualitative data collecting methods are used on side with quantitative data collecting methods. Together with quantitative questionnaire there is used qualitative unstructured interviews to learn what the current state of the case company's security training system is. The theoretical framework of the security training is constituted by using qualitative content analysis to study Finnish legislation, KATAKRI's guidelines, PCI's physical and logical security requirements, ISO standards' requirements together with some pedagogics and aspects of successful security training systems.

2.4.1 Content analysis

Content analysis is both a qualitative and a quantitative data collecting method to systematically analyse data. Content analysis can be used to methodically study news articles, essays, books and other documents in written format. (Hall 2018) In this research content analysis is used to qualitatively analyse written documentation.

Researcher using qualitative content analysis has to choose whether the analysis is manifest or latent analysis. In manifest analysis researcher describes what informants really say and describes the obvious and visible in the text. In latent analysis researcher tries to understand underlying meanings of texts and to be able to tell what the text is deeply talking about. (Bengtsson 2016)

In the content analysis there are recognized four main stages of data analysing process. The four stages are decontextualization, recontextualization, categorisation, and compilation. Decontextualization is a stage where researcher reads through analysed text to get an overall understanding of 'what is going on' before breaking the text into meaning units. A meaning unit is the smallest unit that comprises some of the insights that researcher needs. Identified meaning units are labelled with codes, which should be understood in proportion to the context. This process is called as an 'open coding processes. (Bengtsson 2016)

The second stage is recontextualization, the stage after meaning units have been labelled. The researcher has to check if all aspects of the content have been covered in relation to the objectives. Third stage is categorisation where researcher aims to identify categories and themes and try to fit labelled data inside of those. Each meaning unit should fit in just one category. Once the researcher has created categories, can analysis and writing processes begin. This stage is called the compilation stage.

When researcher is using content analysis, should the data collected to be considered from a neutral perspective and consider the objectivity of the data. As a final check, researcher should consider how the new findings harmonize to the literature and if the results are logical and apprehensible. (Bengtsson 2016)

In this study research qualitative data analysis are used to analyse different written documents including standards, acts, articles, books and guidelines. Content analysis are used to define the theoretical framework of the ideal security training system that is also compliant with several requirements.

2.4.2 Unstructured interview

Interview is a qualitative data collecting method that involves social interaction. Interview requires at least two people, an interviewer and a respondent. Interviews are based on what

respondents tell the interviewer and are more personal than questionnaires. Qualitative interviews can be divided into structured, semi-structured and unstructured interviews. (Dapzuri & Pallavi 2018)

Unstructured interview can be used when the researcher wants to gain deeper understanding on subject. Unstructured interview is sometimes called ‘discovery interview’ or ‘guided conversation’. It doesn’t have any set format, but interviewer can have key questions or topics formed in advance that need to be covered during the interview. All questions in this interview method are open-ended. Unstructured interview is more flexible than a structured interview because there is no need to follow strict interview schedule and it allows freedom for both interviewer and individual participant, interviewer can ask follow-up questions and inquire further information from the participant. Unstructured interview involves one-on-one engagement with participants and usually takes place face-to-face or on phone and can be time consuming. (McLeod 2014)

For successful results of the unstructured interview, the interviewer should have clear plan in the mind about goals and focus of the unstructured interview. Discussion should be guided by this plan. It is recommended to use this interview method when the researcher has gained enough knowledge on the subject and is able to have a clear agenda for the discussion. Unstructured interview can be very useful method for developing better understanding of ‘as-of-yet’ not fully understood setting. Unstructured interview allows the researcher to test their preliminary understanding on the setting but allows still ample understanding of the subject. (Robert Wood Johnson Foundation 2008)

Unstructured interviews are used as a part of the current state analysis of this bachelor’s thesis to ensure that the author has as extensive understanding of the current state of the security training in the case company as possible. Four managers in different positions are interviewed to know how they see the current state of the security training being. Interviews are carried to get supportive data to confirm results of the earlier conducted security training questionnaire and to get comprehensive understanding of case company’s security training system’s current state. The managers who are interviewed are responsible of different phases of training employees in security related matters.

2.4.3 Managers’ interviews

The case company’s four managers in different positions were interviewed separately in unstructured interviews. The interviews were hold after the security training questionnaire’s results were analysed. Objectives of the interviews were to get data to support the questionnaire results, deepen the understanding of the case company’s security training’s current state and get possible improvement ideas from the managers. Interviews were not recorded but the interviewees were provided with a summary of their own interviews to make sure that

the interviewer, the author of this study, had understood them correctly. Interviewees had a chance to make corrections to the summaries before the interviews were used as sources of this bachelor's thesis. The interview summaries will not be published as part of this study.

The first interviewee was the case company's security manager. The security manager was interviewed first to get an overall understanding of the division of the responsibilities and related to the security training in the case company. The security manager and the case company's security team have the responsibility of providing of security training to the employees (The security manager 2018).

The second interviewee was the case company's QHSE-manager. The QHSE manager was interviewed to learn how employees are trained in occupational and environmental safety issues and asked their opinion of the functionality of the current security training system.

The third person interviewed was one of the company's production managers. Objectives of the production manager's interview were to understand more deeply how production workers are trained to be compliant with different security requirements in their work and how carefully employees follow and understand the rules concerned to occupational safety and security in the production. The production manager does not directly provide security training to the employees but has the responsibility to supervise and control that employees follow the given rules.

The case company's human resources (HR) manager was interviewed as the last interviewee. The HR assistant manager is responsible of educating new employees on security issues during the first day of the new employees' carriage in the case company. The HR assistant manager also has a significant role of organizing 'Welcome to the Company X' training sessions.

2.5 Quantitative research

Qualitative research's methodological pair is quantitative research. Quantitative research is based on describing and interpreting the subject through statistics and numbers when qualitative research seeks to comprehend the quality, characteristics and meanings of the object comprehensively. Quantitative research aims to describe phenomena through numeric variables and uses several statistical methods of analysis. (Koppa 2010)

Quantitative research is used to generate numerical data and data that can be transformed into usable statistics. Quantitative research quantifies opinions, attitudes and other variables and generalizes results from big sample populations. Quantitative data collection methods are more structured than qualitative data collection methods. There are several quantitative data collecting methods that can be used to collect data, for example online surveys and questionnaires, face to face interviews and systematic observations. (DeFranzo 2011)

A quantitative questionnaire is used in this bachelor's thesis to collect data about the case company's security training system's current state. The quantitative security training questionnaire is executed to find what are the strengths and improvement opportunities of the case company's security training system.

2.5.1 Questionnaire

Questionnaire is a quantitative data collecting method. Questionnaire is written list of questions for gathering information from respondents. Respondents read the questions and write down or choose from given options the best suitable responses. In the questionnaire can be open and closed questions to collect both quantitative and qualitative data. Closed questions limit the responses to given answer options. Closed questions can provide ordinal data and data collected in closed questions can be easily converted into quantitative results. One limitation of closed questions is that they might be suffering from lack of detail as the respondents have to choose their responses from the given options and there is less scope for them to reflect their true opinions or feeling on the topic.

Open questions allow the respondents to answer and express their opinions and feeling in their own words. Open questions work better when the researcher wants to get more in-depth information from the respondents. Analysing answers of open-ended questions is more time consuming than analysing responses from closed questions. If using open questions, researcher needs to read all qualitative answers and put them into categories by coding. (McLeod 2018)

There are numbers of ways how the questionnaire can be administrated. The method of administration depends on the ease in determining respondent population and on expectation how respondents would prefer to participate the questionnaire. A mailed questionnaire used to be the most common approach to collecting information. With a progress of communication technology, online questionnaire, which is used in this research, has become very popular method of administrate a questionnaire. (Kumar 2014)

From the internet can be found online programs to develop questionnaires. The advantage of online questionnaires is the possibility to send a link to the questionnaire to all potential respondents via email. The respondents answer questions on the same way as in a traditional mail questionnaire. Answers of the respondents are automatically saved in an appropriate program. Many questionnaire programs automatically arrange answers in statistic form, making it simple for researcher to read the collected data. (Kumar 2014)

According to Kumar (2014) with a questionnaire should be sent a covering letter that should briefly:

- introduce the researcher and the institution they front

- describe in a few sentences the aims of the study
- give any general instructions
- insure respondents of the anonymity of the answers provided by them
- provide contact details (email address or phone number) in a case they have any questions
- thank them for the participation in the questionnaire

Questionnaires can suffer from low response rates and therefore it is necessary that the questionnaire is well-designed to get as many people as possible to complete it. It is important that all questions are easy to understand as there is nobody to explain the meaning of questions to respondents and all questions should be asked to address the aims of the research. There should not be any unnecessary or too complicated questions as the longer the questionnaire is, the less people will complete it. (McLeod 2018)

It is recommended to run a small pilot questionnaire before launching the final questionnaire to ensure all questions are understandable. Pilot respondents can be asked to give their honest feedback on the questionnaire design and layout. The layout of the questionnaire should be professional looking and pleasant to respondents' eyes. In the questionnaire should be clear instructions as there is nobody respondents could ask from if there is anything, they don't understand in the questionnaire process. (Kumar 2014)

The researcher must consider on ethical issues when using questionnaire as data collecting method. The researcher needs to ensure that respondents' responses are handled confidentially and let respondents know that they will not be identified from their answers. Respondents should also know that answering a questionnaire should be done in voluntary basis. (McLeod 2018)

2.5.2 Security training questionnaire

As a part of the current state research of the case company's security training, there is conducted a security training questionnaire. The sample of the questionnaire are all employees working for the case company at the time when the questionnaire was open for respondents.

The objectives of the questionnaire are to get understanding of the extent of the case company's security training, to learn how company's employees would like to be trained on security topics in the future and to get updated statistics of how many employees work remotely or have completed training modules in the organization's eLearning portal.

The results of the security training questionnaire are used align with manager interviews to understand what the case company's security training system's current state is.

2.5.3 Security training questionnaire process

The questionnaire designing was started by identifying relevant functions of corporate security that should be covered in the case company's security training system. There were separate meetings held with the company's security manager, information security manager and QHSE manager to discuss about topics that should be covered in the questionnaire. Those three managers were chosen because they have the best visibility on the topics that should be trained to the case company's employees.

After the meetings was the first pilot version of the questionnaire designed. In the first version respondents were asked to evaluate in scale 0-1-2-3 how comprehensive security training they have received on different security functions. This triggered the pilot respondents to evaluate their own knowledge and not to answer the questions if their current employer has trained them or not.

After the first pilot, core questions were modified to be "Have you been trained for…" and response scale was No training – Initial training – Comprehensive training. This question model started to give pursued responses. The aim was not to ask the employees to evaluate their own knowledge in safety and security because they might have gained their knowledge in school, from previous employers or by self-studying subjects. The aim was to know, how well their current employer has trained them in security and learn to know how encompassing the current training system is. There are security subjects that employer must train to their employees to be lawful and complaint with regulatory requirements.

Following the second pilot was a meeting held with the security manager to make final modifications and corrections to the questionnaire. At this point was an English version of the questionnaire made to be launched together with the Finnish version. In the company there are employees from different nationalities and both Finnish and English languages are used.

The security manager shared the questionnaire to employees who have company email address. Notification of the questionnaire was also launched on the case company's intranet. In the company there are production workers who don't have their own email addresses. In cowork with the IT department it was possible to organize a work station to the production area. Production managers were asked to share information with their employees about the security training questionnaire and about the possibility to all employees to participate it on the additional work station. A week after the questionnaire launch there was a reminder sent to the employees' email addresses about the ongoing questionnaire.

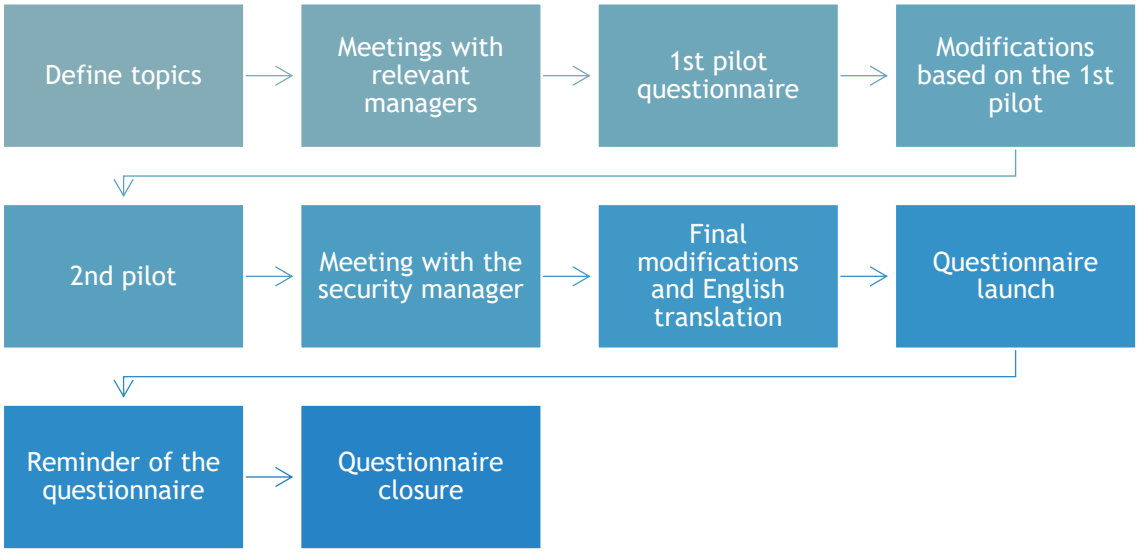


Figure 4. The security training questionnaire process, the time frame is ~six weeks.

The results of the questionnaire's open and close-ended questions are analysed using quantitative data analysis. Respondents' answers to open-ended questions will not be published but information from the answers may be used.

In total 117 employees completed the security training questionnaire. The questionnaire was sent to around 230 employees by the case company's security manager. The aim was to gather responses from all work departments and offer every single employee with an opportunity to participate the questionnaire. The challenge was to reach production operators who don't have personal company email addresses. Participant percentage of employees who have company email addresses is 51. When all case company's employees are counted to sampling, is the participant percentage 29.

The security training questionnaire reached principally officials of the company. 29% of respondents work in production and 71% in other departments. 61% of respondents have been working for the case company eleven years or longer, 79% six years or longer. The questionnaire does not give a truthful view of the whole company's employee turnover. In the production there, work plenty of young operators and in the production the employee turnover rate is significantly higher than along the office workers. Production employees are aimed to get engaged better to the company by amending fixed term contracts to permanent (The production manager 2018).

Questions marked in the security training questionnaire results (Appendix 1) with * were mandatory for everyone. The questions marked with 'multiple choices possible' could respondents

select more than one response options. The core questions in Section 2 are reviewing if employees have been trained on different security guidelines and practices, evaluation is done by using a three-step scale. Given answer options were No training (1) – Initial training (2) – Comprehensive training (3). In the results are presented averages of core questions, 1 being the lowest and 3 the highest possible average. Other results are given in percentages or in total count of responses.

3 Literature

In this chapter is defined the literature that forms the theoretical framework of the case company's security training system in this study research. In the theoretical framework is described some basics of learning by using the VARK approach, defined functions of corporate security in general and described aspects of educating company employees in security.

The case company operates in digital security business and there are industry-specified standards, for example ISO/IEC27001 and ISO14298 which the company aims to comply with. Those standards together with Payment Card Industry's physical and logical security requirement standards, Finnish legislation and KATAKRI's guidelines form the desired state of the case company's security training system. The conducted gap analysis is performed in the scope of these official documents. In the chapter 5 is also considered what previous studies justify about successful security training systems and pedagogics, which the case company can benefit from while improving their own security training system in the future.

3.1 Learning

Learning can be described being a process where an individual gets more knowledge, memorises or reproduces applying facts or procedures to understand something in a new way. People learn by adding new information on top of what they already know. By adding variations to existing knowledge, people's understanding of things become more complex and intricate. (Carnell 2000)

People are individuals, and everyone has their own way to receive and process information. There are several learning style theories and models. One of the theories is Neil Fleming's VARK model that divides people to four groups depending on their dominant learning style. The acronym VARK stands for Visual, Auditory, Read/write and Kinesthetics sensory modalities and express those four modalities to learn information.

Visual preference includes description of information in maps, charts, diagrams and flow charts. This preference does not include still pictures of reality, movies, videos or PowerPoint shows. It includes shapes and designs that are used to highlight and convey information. Vis-

ual learners can benefit when a whiteboard is used to present relationships between of different things in diagrams. Visual mode could also be called Graphic, because that describes the mode better.

Aural describes modality when information is heard and spoken. Learners who have aural as their preference learning modality learn best from lectures, group discussions, radio and talking things through. Aural learners like to sort things out by speaking out loud and they might repeat things that has already just been said.

Read/write is preference for information being in written words. Read/write learners prefers text-based in-and out-puts. They like to write and read essays, reports, assignments and manuals. People who prefer this modality, many times enjoy having lists and diaries and like to spend time in Internet reading Wikipedia and searching new information from Google.

Kinesthetic modality refers to preference when kinesthetic learners prefer learning information from videos, movies and demonstrations connected to ‘real life’. They like to learn from doing something and they value their own experiences. Kinesthetic learners prefer case studies, applications and practices. They like to hold, taste and feel things. It is possible to write or speak kinesthetically if the topic is based strongly in real life. (VARK Learn 2018)

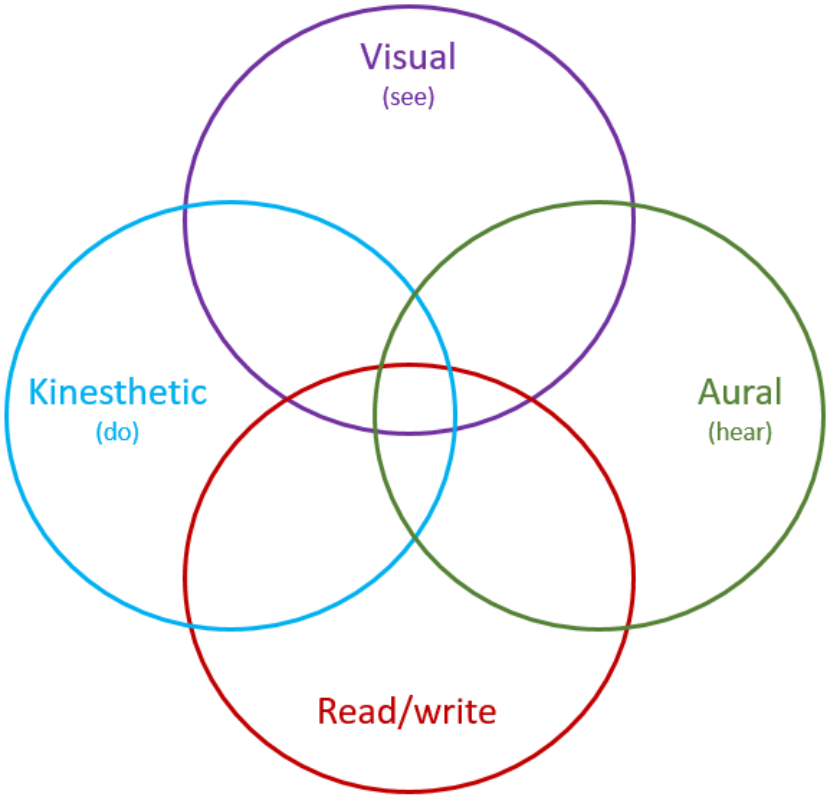


Figure 5. VARK learning model.

The VARK learning model and other learning theories have also been criticized. There has been discussion if knowing learning style will benefit learners or even worsen their study results. Life is multimodal, and many people can recognize that they have several learning style preferences. Teachers and other trainers can anyway benefit from the VARK model by designing their lectures and training sessions covering even all four modalities. Not everybody learns by reading written instructions without further explanation and for some learners it is easier to adopt information when it is spoken and visual at the same time. (Cherry 2018)

It is important to bear on mind that adults learn new information on different way than children do. Adults have already a very strong idea of 'self' and they have experiences, memories and prejudices. Adults need to be willing to learn new things, motivation is essential, and learning process should be designed to relate to their current knowledge base and they should be able to relate to what they are being taught. (McIlwraith 2007)

3.2 Security training

There are several security compliance standards that require companies to implement security training as part of the company's security management programs (Mortman 2009). To be

compliant with standards and to operate as a responsible employer, should security training be a part of the company's security management system (SMS). It is necessary for the company's security personnel to understand that it is not enough that security policies just exist in an SMS document. Policies must be explained throughout the company, to all its employees, provide personnel with security training. Employees need to understand what there is behind of the security policies that they are asked to conform with. Without a comprehensive explanation of the policies, can employees ignore them and use it as an excuse of not complying. Security policies can only be effective if employees, know, understand and accept the necessary procedures. (Hight 2005) Briefly can be said that security training is a continuous process where employees are educated to comply with company's security policies and procedures. Security policies set frames for security training and different standards, guidelines and procedures that company aims to conform with, set more exact aspects for the security training program.

According to Mortman (2009) security training can be divided into two main categories: general security training and group specific training. General security training is appropriate for all company's employees in all different positions. General security training can include topics of company's security policies and procedures, information of whom to contact if an employee believes they have identified a security incident or risk and company's rules for handling confidential information. General security training should be regular as it is a cornerstone for a strong security posture. Group specific security training is given to employees depending on the needs of their job tasks. The training should be handled as any other subject-specific training and it aims to be more in-depth than general security training. Group specific training can include educating finance team in fraud-detection or IT-operations staff in recovery planning.

Widely used term 'security awareness training' means educating employees about information technology (IT) security. Security awareness training educates employees about company's policies and procedures for working in IT environments. (Rouse 2011). Commonly seen acronym 'SETA' related to IT security, stands for Security, Education, Training and Awareness. SETA program can be defined as a training program that is designed to reduce security breaches that occur due the lack of employees' security awareness. The program is meant to make employees understand what security expectations employer has to them. SETA program aims to explain security policies and the existence of the policies to make it easier for the employees to understand why they should comply with the company's security policies. The program aims to generally put security in forefront in employees' minds in daily basis and to show where employees can play an important role to protect company's information. (Hight 2005)

Information security defines to processes and procedures that actively maintain confidentiality, integrity and availability of company's information assets that can be in various forms. Confidentiality, integrity and availability are also referred to as the CIA triad of information security. Information security includes different processes and tools to protect sensitive business information from modification, interference, desolation and purposeless screening. Information security and cybersecurity are often confused, but information security refers solely to data security while cybersecurity is a more overall term. Information security is included in cybersecurity. (Cisco 2018)

The case company operates in digital security business and therefore the company's security training system includes training in security awareness, comprising training to company's information security policy and practices too. In this study it has not seen necessary to differ security training and security awareness training as they are tightly tied together in the case company's security training objectives.

There are many reasons why companies should invest resources in employee security training. Good security training improves security of all business practices because training deducts errors and mistakes, when people know what they are expected to do. If company has uneducated employees, it is taking a prominent risk in putting the entire company in hands of company's security department that cannot by themselves secure employees' safety and security, security of information or other assets and continuous business operations with only help of technology and protective physical solutions. (McIlwraith 2007)

When planning any employee training, it is important to follow a logical order. Trainings should be started from baseline and objectives should be built on previous knowledge. Training needs assessment is a process that aims to indicate what training each employee needs. Employees should be trained for what their positions require. It is also important to train employees for scenarios and situations they might really experience in their job.

Communication and marketing are key to engage and change employees' behaviours. It should be ensured that there is at least one person in security team who has those soft skills or is partnering with someone that has. (SANS, 2018) It might also be needed to send company's in-house trainers to their own trainings to be able to run better security training sessions in the future. (Rouse 2011)

3.3 Corporate security

Security and risk management are not merely business support and core activities, they are also management practices that must be considered in decision making in all company's activities. Security and risk management are part of the decision-making process, no matter where

decisions are made. Security and risk management are part of the overall management of company's operations. (Leppänen, 2006)

Corporate security in general, is security of all company's activities. Corporate security protects company's important values like personnel, information, reputation, assets and environment. The focus of the corporate security is to advance the company's competitiveness and improve productivity. Corporate security does not target to be disconnected security activity inside the company. It aims to ensure the corporation's continuity, workers' safety, security and compliance in all situations.

Confederation of Finnish Industries has developed a corporate security model to describe different sectors that are included in corporate security. Sectors can be one on the other and company's industry and business describe the importance of each sector. In some businesses some sectors are more important than in others. It is essential for every company to choose vocabulary sectors and measures and fit the needed sectors of the model in their own business

Corporate security model's nine security functions are

1. Physical security
2. Malpractice and incident management
3. Anticipation and crisis management
4. Fire safety and rescue
5. Personal security
6. Environment security
7. Occupational safety
8. Production and operation security
9. Information security.
(Elinkeinoelämän keskusliitto 2018)

Corporate security functions are also inseparable at many points. For example, access control isn't just a physical security control, but it also protects company's valuable information from unauthorized access and is part of information security function too. (Leppänen 2006)

3.4 Occupational Safety and Health Act

Occupational Safety and Health Act (2002/738) aims to improve working environment and working conditions. It also aims to ensure and maintain workers' ability to work and to prevent occupational accidents and diseases. The act obliges both employers and employees.

Requirements identified in Occupational Safety and Healthy Act (738/2002)	
	know what hazards and risks are in their work
	work, work environment, work and safe production practices, tools
	be familiar with safe work practices especially before starting in new job/position or when employee's position changes
	know how to reduce risks and hazards in their work
	know how to avoid harms and hazards
	know how to practice during maintenance, repair or cleaning processes
	know how to operate in a case of a security incident
	improve work safety in co-operation with employer
	follow employer's instructions and to take care of own and other employees' safety and health
	correctly use personal protective equipment (when needed)
	handle hazard substances correctly
	know how to act in a case of workplace accident or sickness

Table 1. Requirements identified in Occupational Safety and Health Act (2002/738)

3.5 Rescue Act

Finnish Rescue Act indicates duties of individuals', companies' and legal people to prevent and prepare for accidents. It also lays down processes when there is a threat of an accident, when an accident happens and limit the consequences of happened accidents. (379/2011) In Rescue Act there are duties and responsibilities that should be trained to company's employees.

Requirements identified in Rescue Act (379/2011)	
	General duty to Act. Employees shall be trained to know how to act if they observe or receive information about a fire or other accident
	Duty of care. Employees shall be trained to be careful to avoid the risk of a fire or other accident and the damage it causes
	Emergency plan. Instructions should be given for building residents and other persons on how to prevent accidents and what action to take in accidents and dangerous situations

Table 2. Requirements identified in Rescue Act (379/2011)

3.6 ISO/IEC 27001:2017 Information Technology: Security techniques. Information security management systems. Requirements

ISO/IEC 27001 (2017) is a part of ISO/IEC 27000 family of standards and it provides requirements for constituting, maintaining and continually developing information security management system (ISMS). The constituting and implementation of company's ISMS is affected by company's needs and objectives, company's security policies and requirements and company's processes. It is rather a management standard than technical standard and it does not describe technical requirements of information management systems. ISO 27001 focuses on finding, managing and reducing risks related to information. The purpose of the standard is to provide requirements for companies how to protect confidentiality, integrity and availability of information and to give confidence to external parties that information security risks are properly managed. If a company claims conformity of ISO/IEC 270001:2017 any of the requirements on clauses 4-10 cannot be excluded from their information security management system.

In ISO/IEC 27001 there are several requirements and objectives (clauses 4-10 and Annex A) that should be guided to company's employees if the company is conforming of the standard.

Requirements identified in ISO/IEC27001:2017	
	Compliance with security policies and standards
	Teleworking policy. Employees who work outside of company's premises (business trips, working remotely) shall be trained to comply with company's teleworking policy to protect information accessed, processed and stored while outside of office
	Mobile device policy. Employees shall be trained in company's mobile device policy to manage risks regarding use of different kind of mobile devices
	Unattended user equipment. Employees shall be trained to ensure that unattended equipment (laptops, mobile devices etc.) has appropriate protection
	Clear desk and screen policy. Employees should be trained to follow clear desk and screen policy
	Use of cryptographic controls policy. Employees shall be trained in company's policy of cryptographic controls to understand when confidential data need to be protected with cryptographic controls
	Project management. Employees need to know that information security must be addressed in project management, in all projects
	Classification of information policy. Employees shall to be trained to know company's classification of information policy to understand that information need to be classified in terms of legal requirements, value, criticality and sensitivity to protect it from unauthorised disclosure or modification

	Data labelling policy. Employees shall be trained in company's data labelling policy
	Awareness. Employees need to be aware of company's information security policy. Employees need to understand their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance.
	Information security training. All employees and contractors shall receive information security education and training, regular updates in company's security policies and procedures relevant for their work tasks
	Disciplinary process. Employees shall be told about disciplinary process if they have committed an information security breach
	Termination or change of employment responsibilities. Information security responsibilities and duties that remain valid after termination of employment or when employee's responsibilities change shall be communicated to the employees

Table 3. Requirements identified in ISO/IEC27001:2017 standard

3.7 Katakri

Katakri is a public audit tool that can be used to evaluate company's ability to protect authorities' confidential information. Katakri is compiled by minimum standards based on national regulations and international obligations. Katakri itself does not set absolute requirements for information security. The requirements set in Katakri are based on existing legislation and international obligations. Katakri can be used as an audit tool for assessing company's security arrangements in Facility Security Clearance (FSC). It can also be used to help organizations to develop their other security practices. Use of Katakri targets to ensure that company has adequate security arrangements for unauthorized disclosure of authorities' confidential information in all environments where data is stored and processed. (Puolustusministeriö, 3)

Katakri is used to assess company's general ability to protect authorities' confidential information. Facility Security Clearance carried by following Katakri's requirements can be used in

both Finnish/domestic and international projects. (Puolustusministeriö, 4) Katakri sets requirements also for company's security training. In Katakri are indicated following guidelines that companies can implement to be part of their security training system.

Requirements identified in KATAKRI (2015)	
	Security training. Security training and guidance is carried out considering the needs of employees' work tasks.
	Security procedures/guidelines. Security guidelines are trained and available for all employees.
	Managing security incidents. Managing security incidents is trained and instructed to employees, documented and practised
	Confidential information. Employees are given instructions and training on the proper processing and handling of confidential information. This includes where the information can be stored. Training is regular and employees who have participated trainings are documented.
	Visitors. Employees are trained in visitor procedures
	Malwares. Users are guided by threats of malwares.
	Information security policies. Users are guided to follow company's information security policies

Table 4. Requirements identified in KATAKRI 2015

3.8 ISO14298:2013 Graphic technology: Management of security printing process

The standard specifies requirements for security printers for their security printing management system. In ISO 14298 there are specified requirements for employees' security training. According to the standard employees should be trained on the following topics

Requirements identified in ISO14298:2013	
	Compliance. Employees shall be trained to know how to be compliant with company's security policies.

	Work influence. Employees shall be trained to be familiar with company's security objectives and to understand how their work contributes to meeting security objectives and requirements
	Security rules. Employees shall be trained to know rules and procedures in the company concerning security

Table 5. Requirements identified in ISO14298:2013 standard

3.9 Payment Card Industry

Payment Card Industry's (PCI) the PCI Card Production and Provisioning – Physical security requirements manual (2016) is an extensive information source for companies involved in card production and provisioning. Card production and provisioning might include card manufacturers, personalizers, pre-personalizers, data-preparation and fulfilment and chip embedders. The manual specifies the physical security requirements that companies operating in card production and provisioning must follow during all phases of card production processes.

The PCI Card Production and Provisioning – Logical Security requirements manual (2016) specifies requirements for all systems and business processes associated with the logical security activities in card production and provisioning. Card provisioning and production include data preparation, card personalization, pre-personalization, PIN mailers, card distribution and card carriers. The manual specifies requirements that entities perform in

- cloud-based or secure element provisioning services;
- managing over-the-air personalization, life-cycle management and preparation of personalization data or
- managing cryptographic keys.

The PCI Card Production and Provisioning both physical and logical security requirements set also requirements for card production or provisioning entities' employee security training.

According to the PCI Card Production and Provisioning physical and security requirements employees need to be trained on the following topics.

Requirements identified in PCI CP physical and logical requirement manuals (2016)	

	Company's security manual. Employees shall be familiar with company's internal security manual and to know where they can find the document
	Reporting of breaches. Employees shall be trained to report any observed breaches of established security policy. Employees need to know what possible breaches there are
	Reporting of abnormalities. Employees shall know to whom they can report any unexpected or unusual activity relating to production operations and equipment
	Password policy. Employees shall be trained to be familiar with company's password policies when they have access cardholder information, or any other system used as part of personalization processes
	Visitor procedure. Employees shall be trained to be familiar with company's visitor procedure.
	Mobile device policy. Employees shall be compliant with company's mobile device policy. The policy should include all mobile devices and removable storage devices

Table 6. Requirements identified in PCI CP logical and physical requirements (2016) manuals

Employees working in the payment card processes shall also participate annual mandatory security trainings that the employer organizes. Annual training sessions shall educate employees in the company's security policies and in employees' responsibilities. Employees shall also affirm that they adhere to company's security policies. Guards working in company's property shall be trained of all assigned tasks defined within the company's internal security manual at least annually or prior new responsibilities. Personnel having responsibilities in key management, shall be trained annually. (PCI 2016)

4 Case: Company X

The beneficiary and the case company of this bachelor's thesis is called as Company X. The case company is a high security level manufacturing site of an international digital security organization. This study focuses on researching the case company's security training system's current and desired states. Organization level security policies are implemented on the manufacturing site to be in line with Finnish legislation and other local requirements and this study

submits security training requirements for the case company that operates in a high security level environment in Finland.

The case company's premises are composed of production facilities, research and development department, offices, visitors' meeting rooms, employee restaurant and other company facilities. The case company operates manufacturing, developing and selling high security level products and many of their processes are confidential. Due the sensitive nature of the case company's business, they are called as Company X and their real name or exact location will not be published in this study.

The organization itself employs around 14.000 people all over the world and its revenue was 3 billion euros in total in 2017. In the case company there are around 400 employees working in several business departments at the manufacturing site. The company's revenue was ~90 million euros in 2017.

The case company has a comprehensive security management system. The security management system is based on both corporation and local security policies, local legislation and other external requirements as International Organization for Standardization's (ISO)-standards. Security policies, procedures and guidelines are deployed to employees via security training. The security training is a part of the company's complete security management system.

Continuous training is needed in the changing world of security requirements. One example of a major change of regulations is The European General Data Protection Regulation (GDPR) that was applicable from 25th of May 2018. All companies handling personal data of European Union's citizens need to be compliant with the data privacy regulation from May 25th onwards. (European Commission, 2018) If company is not compliant with the regulation can it face fines up to 20 million euros or 4% of its annual turnover (GDPR Associates, 2018). Therefore, employees in all companies handling EU customers' personal information like names, email addresses or any other identification data, needed to be trained to understand effects of the new regulation on their own work.

2018 SANS Security Awareness Report (2018) analyses data collected from 1,718 security awareness specialist to recognize and benchmark how organizations from around the world manage their human cyber security risks. The security awareness professionals often report time to be the greatest challenge of educating employees in security awareness. Time is the major challenge that the security manager (2018) sees for the reason why security training is not on desirable level in the case company.

The objective of this bachelor's thesis is to indicate possible gaps between of the case company's security training system's current and desired states by using gap analysis methodology. The identified gaps are improvement opportunities for the case company. The aim of this research study is to provide the case company with opportunities to implement to their security training system to ensure the training system's compliance with different requirements in the future.

4.1 Current state

In this chapter is defined the current state of the case company's security training system. The understanding of the current state of the training system is based on the research results of the conducted security training questionnaire and managers' interviews and the company's security training material that was analysed using content analysis.

Security training questionnaire's responses (Appendix 1) were analysed by using quantitative and qualitative content analysis. The responses' averages were analysed in a three-step scale (1-2-3). If the response average is <2,0 can be seen that function is on insufficient level. If the response average is ≥2,0 can the function be seen in satisfaction level. It should be noted that, the functions on satisfaction level should not be excluded from the future training system as continuous training is needed.

The case company's business environment is specific and requires extra-attention on security. New employee orientation is an important process to get new comers to comply with different requirements, understand the company's security culture and mode of operations and provide them with a safe and convenient work environment. The orientation includes 1st day introduction given by HR, manager's or supervisor's training new employees to safe and correct work habits, including evacuation practices and information security and confidentiality. Welcome to Company X sessions are part of the new employee orientation.

The case company's HR assistant manager welcomes new employees to the company. New employees sign a non-disclosure agreement with the company and gets a general introduction of their new employer. The general introduction includes also some of the most important security rules and procedures that the employees must follow straight from the beginning. (Production manager, 2018) The new employees are trained by HR during their first day in physical security including how to get around in the building, most important aspects of information security including examples of confidential information. The new employees are also given instructions of what they can share on social media about the company. Social media guidelines would be good to be added to 'Welcome to company X' sessions' material. (The HR assistant manager 2018)

New production employees are given security training by department supervisors. The supervisors' responsibility is to train employees in information security, fire and evacuation practices and in occupational and environmental safety issues related to the employees' own work. New employees are trained for safe and correct machinery use by experienced operators of each workstation. At the moment there isn't any named instructors in the production and therefore new employees' training can be fragmented because new employees might have several different people instructing them in the use of machines and devices. New employees training for right and safe work habits could be better guaranteed by having specified instructors who would know exactly how and what to educate for new operators. (The production manager 2018)

From time to time new operators work orientation at workstations is affected negatively by missing resources. Sometimes new employees' training might be even be rushed through. There are also challenges in the production to know which operator is trained for which machine use. Sometimes it is expected that 'old' employees are trained for everything but really their training might be incomplete. There are some operators who have worked in the company for several years and those are prone to consciously bypass some of the security features of machines. Always when this behaviour is noted it is intervened by supervisors or production managers. (The production manager 2018)

In the new employee orientation there is used a template to make sure all mandatory security topics are explained and trained to all new employees during their probationary period. The case company's HR team manages the orientation templates (The security manager 2018). About 70% of the orientation templates return to the HR automatically. The existing 30% are returned after the HR team has requested them. (The HR assistant manager 2018)

In the questionnaire results (Appendix 1) can be seen that occupational and environmental safety questions' averages are all below 2,0. These results were also analysed using only responses from the production workers because occupational and environmental safety matters are there more visible in the production than in the office environment. The result averages increased by ~0,1. The case company has organized Safety Day security training sessions for its employees during the past couple of years. Department managers are informed in advance about the coming trainings and they have been able to decide if their team members should participate it. (The security manager 2018) Safety Day training is focused on physical security and fire and evacuation practices and occupational safety and environmental matters are also presented during the training. Employees are provided with chances to receive training in occupational and environmental safety, but for most employees, it has been their own choice to participate or not. (The QHSE manager 2018)

When analysing of the security training questionnaire results (Appendix 1) can be noted that many employees feel that they have been trained comprehensively in physical security, fire and evacuation matters. In the Gap analysis chart can be seen that Rescue Act's requirements are covered in the new employee orientation, in the company's Security and Safety guidebook and in Safety day training.

Team managers and production supervisors are responsible of educating employees in confidentiality and other information security requirements. Information security training is based on the company's information security policy, but some departments have also special requirements for information security training. (Security manager 2018) Security training questionnaire results show that employees' training in information security is on good level, averages being between of 2.1 and 2.4.

In the Gap analysis chart can be seen that the requirements based on ISO/IEC27001 are partially covered in company's current different training methods. For example, the case company's classification of information security policy is trained to the employees partially during the new employee introduction and is partially covered in Safety & Security guidebook. The local current training does not include rules for transmission or storage of the information. The most comprehensive coverage in the ISO/IEC27001 requirements is in the corporate level's eLearning portal. 68% of the respondents had completed security training modules in the organization's eLearning portal and information security has been one of the major subjects in the portal. Anyway, when employees were asked on what topics they would like to have further training of, information security was the second wanted topic.

The case company is a part of an international digital security organization and many employees travel in business purposes. According to the questionnaire results, respondents are lacking training in remote working and business travel guidelines. 74% of the questionnaire respondents have been on a business trip. The employees were asked if they had received training for safe business traveling and the average result was 1.7. Some employees also have a possibility to work remotely. 42% of the questionnaire respondents say that they do work remotely. Results to questions if employees were trained on safe use of Wi-Fi networks and remote working guidelines, were 1.7 and 1.6. 36% of employees who work remotely have answered that they have not got security training in remote working practices at all.

The Gap analysis chart shows that the case company's current local training does not cover the requirements of ISO/IEC27001 comprehensively. The conducted current state research indicates that the case company does not have guidelines for remote working and business traveling. In the corporate's eLearning portal, the required topics are covered better and there are given instructions regarding remote work.

The case company's mandatory annual training is carried by asking employees to read the company's Safety and Security guidebook and sign a template that they understand and adhere to the company's security policies and requirements of the guidebook. (The security manager 2018) According to the questionnaire results many employees are missing continuous training in security matters. The employees were asked to evaluate reasons for their possible security training insufficiency and the preponderant reason was that there has not been training available in the questioned topics. The company aims to educate 100% of new employees and 80% of the current employees in security annually (The security manager 2018). According to the questionnaire results this is not fulfilled for the company's current employees. The managers' interviews support the factor that the security training is focused on new employees and can be insufficient for new comers as well, due the lack of 'Welcome to Company X' sessions where employees should be provided with general level security training and knowledge. In 'Welcome to Company X' employees are provided training for example on company's security policies that should build a knowledge base for the employees' security education.

The case company does not have local eLearning system and the current security training sessions are mostly held traditionally in a class room environment. The case company's security training is strongly focused on new employees and employees' voluntary participation. The PCI Card Production and Provisioning both physical and logical security requirements set a requirement for the company to provide employees (who are part of the payment cards' processes) annual security training that is mandatory. In the case company, the annual mandatory training is carried by collecting employees' signatures to confirm that they have read and understood the content of the company's Safety and Security guidebook. The company does not run annual exams to test employees' knowledge on security (The security manager 2018).

The case company aims to follow ISO/IEC27001's requirements and one of the requirements is to provide the employees with training on information security and give them regular updates on information security topics. According to the security training questionnaire's open-ended questions' answers, respondents would like to receive regular updates on current security topics. Manager interviews reflect that new employees are given important training on security, safety and environmental topics on 'Welcome to Company X' sessions. In the company there isn't any substitute training option to cover possible information gaps due the not held part of the orientation. Having 'Welcome to Company X' training sessions in video format should be considered but it would be important to give new employees an opportunity to ask questions as it has now been possible in the welcome sessions (The QHSE manager 2018).

In the case company there work employees in the production who don't have company's email addresses or company's laptops. This sets challenges for the intercompany communication because everybody can't be reach by email. All employees have a possibility to access

the company's intranet from workstations but in the production, there is used paper notes to communicate with operators. (The QHSE manager 2018) This challenge was faced with the security training questionnaire that didn't reach production operators.

The case company operates in an environment that requires high security awareness from employees. Even there are ~250 employees working in the production using different machinery and devices, there does not happen many workplace accidents annually (The QHSE manager 2018). The case company's security manager (2018) does not remember any security incident that's root cause had been employee's unawareness. When workplace accidents occur are the mostly due employees' thoughtlessness or them consciously behaving against rules, for example lifting heavy objectives alone even they have been instructed to always have two people to do the task (The production manager 2018).

Providing the employees with security training and content of security trainings are responsibilities of the case company's security manager and the security team. The responsibility is kept within the security team due regulation reasons and it is reasonable that the security training is provided by security professionals. (The security manager 2018) The case company has a comprehensive security management system and security training is part of it. According to the questionnaire's results employees would like to participate more regularly security training sessions or receive current updates. Only three respondents of the questionnaire answered that they have decided by themselves not to participate to security training sessions.

In the security training questionnaire respondents were asked to tell how they would like to be trained in security matters in the future. eLearning, classroom training and workshops were the most preferred training forms among respondents. Respondents were given chance to tell what security functions they would like to receive further training in the future. Two of the most popular future training topics were security incidents and information security, environmental issues coming as the third wanted.

4.2 Desired state

The desired state of the case company's security training system is a situation when the system fills both internal and external requirements. The desired state of the security training system is also a significant part of the theoretical framework of this study. The desired state of the security training was distinguished by conducting qualitative content analysis. Content analysis were used to research written documentation to find what requirements there are in Occupational health and safety Act, Rescue Act, ISO/IEC27001, ISO14298, KATAKRI and PCI's standards. In Gap analysis chart (Appendix 2) are listed the requirements that were found from each of the document.

The case company desires to provide its employees with regular security training on different subjects. The case company's security manager (2018) defines that the aim is to train 100% of new employees and 80% of current employees annually on security. Otherwise the desired state of the security training system is based on the conducted content analysis to analyse external legal and regulatory requirements. In the chapter 5 Conclusions and recommendations for improvement are also defined how efficient security training could be conducted based on the knowledge gained by analysing relevant articles and of successful security training system. The desired state is based on the company's own requirements and requirements identified from regulatory and legal documentation.

4.3 The gap

In the gap analysis the gap means the distance between of the current and desired state of the subject. Based on the gap analysis technique, after the current and desired states have been defined, it is necessary to analyse the gaps between of the states and why those exist.

Gap analysis chart (Appendix 2) defines how regulatorily required security topics are trained to the employees currently. Gap analysis chart is a table, and, in the table, there are listed the requirements that were identified during desired state research. The listed requirements form the desired state based on the regulatory requirements, those topics should be included in the security training system to ensure its compliance with external requirements.

In the table there are used three marks that are X, / and -. X (green) means that the required topic is included in the specific training, / (yellow) means that the required topic is partly covered in the training and – (light red) indicates that the topic is not included in the current content of the specified training.

	Current					
Requirements	1st day introduction by HR	Supervisor/ manager training at the workplace	Welcome to Company X session	Turvakansio/Safety &Security guidebook	Corporate's eLearning	Safety day (voluntary participation)
ISO14298:2013						
security policies	X	/	X	X	X	X
employee's work's influence to company's security objectives	X	X	X	X	-	X

Figure 6. Example of Gap analysis chart (Appendix 2) use.

The requirements of the desired state can be seen on the desired level if the requirements are comprehensively covered in the current training system. In the Gap analysis chart (Appendix 2) can be seen that requirements of Rescue Act are included in many phases of employees training and therefore the training can be seen on sufficient level. Also, the security training questionnaire supports this. An example of insufficient training coverage is remote working policy that can't be seen fully covered in any of the current trainings.

In the security training questionnaire employees were also asked to evaluate reasons for their possible security training insufficiency and the most popular response was that there has not been security training available in the questioned topics. As a part of the new employee orientation the company aims to organize 'Welcome to Company X' sessions. In the sessions there are presented comprehensively general security, quality, human resources and occupational and environmental safety topics by professionals of each theme. During the research there were noted some gaps in the company's ability to organize 'Welcome to Company X' sessions. The company has not set any time limit for organizing these sessions for new employees and there has been challenges to get sessions' leaders schedules to match together. In general, it has not been possible to plan security training sessions far in the future because there are plenty of changing factors and limited resources. In the case company there is not working anybody in a specific training coordinator's position. (The security manager 2018)

In the Gap analysis chart can be seen that Occupational Safety and Health Act's requirements are trained to new employees during the orientation but most of the required topics are not covered in the company's Safety & Security guidebook. At the moment the case company's annual security training is run by directing employees to read the guidebook and sign a form that they have read and understood the content of the guidebook. Some occupational safety and health topics are covered in Safety Day training sessions, but the participation to the training is based on the employees' voluntary. Occupational safety and health topics have more significant role in the production than in the office environment. In the production there are supervisors monitoring the employees work and they are expected to guide employees to safe working habits continually. In the case company there are general and specified security trainings provided. For example, only employees handling chemicals are provided with training for safe use of different chemicals. Despite of the work department, every new employees' orientation should include identifying risks and hazards in own work and right action in a case of work place or commute accidents. (The QHSE manager 2018)

Results of security incident training coverage show that many of the respondents don't feel that they are trained comprehensively in security incident practices or being able to satisfactorily describe what security incidents are. Occupational Safety and Health Act, KATAKRI and PCI's standards require that all employees are trained to identify security incidents or abnormalities and to know how to act if they recognize one of them. 37% respondents who work in the production have not been trained to know how to act if they meet a visitor without a host in manufacturing area. A visitor without a host is one example of a security incident in the case company. Security incidents are defined during the introduction sessions but in the Security and Safety guidebook is not indicated what security incidents are and how those should be handled. In the guidebook is written that the employees will be provided with training regarding security incidents but during the research the author was not able to identify this kind of training to be held or planned to have held.

ISO/IEC27001 (2017) sets many requirements for the case company's training in information security. The current state research points out that there are improvement opportunities in the case company's security training in information security. The best coverage for the information security topics is in the corporate's eLearning system. The case company does not have tools to follow how many of their employees have completed training sessions in the corporate's eLearning system. The case company seems to be lacking mobile device, remote working and crypto graphic's policies. Also, during the research it couldn't be identified that the case company had clearly communicated disciplinary processes to their employees in a case if an employee has committed an information security breach. All the latter are requirements of ISO/IEC27001 (2017). The standard also recommends the companies to implement a clear desk and screen policy. This policy is shared with employees in the corporate's eLearning but locally the case company has not decided to implement it.

Many of the KATAKRI's (2015) guidelines are from ISO/IEC27001 and therefore some of the KATAKRI's guidelines are overlapping with ISO/IEC27001's requirements. In KATAKRI (2015) there is a requirement to train employees in threats of malwares. In the current state research, the author was not able to identify any local training related to risks of malwares. In the corporate's eLearning there is information of different malwares.

ISO14298 standard gives only overall requirements for the company related to security training. The requirements can be seen fulfilled in the case company's current security training system.

PCI's both physical (2016) and logical (2016) standards set requirements for the case company to train the employees who work as part of any payment card processes and the security guards of the premises. According to the PCI's requirements the employees should be trained reporting of abnormalities and any observed breaches of the company's security policies. These requirements are covered in some parts of the current trainings. There is a requirement to train employees to be familiar with the company's password policy. In the current state research, the author was not able to identify any local training existing on the topic.

5 Conclusions and recommendations for improvement

In this chapter are defined what actions the company could consider taking to improve their current security training system. The recommendations are based on the current and desired state researches and to the author's improvement ideas that are based on the conducted gap analysis.

The case company's security training system covers most of the required topics at some point of the employee's life cycle. The major opportunity is to implement a security training system that provides employees with continuous training on security by using different training

methods. This can be reached by running training needs assessment and by having a security training plan or year clock. The security training does not always have to be too serious and to be held by having one person speaking in the front when the others are listening. What comes to educating adults, they should be able to identify to the topics they are trained for. Not all employees need to be trained on same topics, but it must be ensured that legal requirements are always met.

The case company is strongly focused on security and it has a comprehensive security management system. The company itself targets educating employees comprehensively in security annually. The gaps between of the current and desired states of the company's security training system are not explained due bad security governance but the gaps can be seen due the lack of implementation of the security training program. The company's own documentation indicates widely on which topics the employees should be trained but the actual training implementation is inadequate. The insufficiency can be seen because of the case company does not have a plan how, when and what the employees should be trained for. Now the employee's security training builds from the new employee induction and knowledge pieces coming from here and there.

The company needs to run regular security training to be compliant with internal and external security requirements and make sure their employees have current and relevant knowledge of changing requirements. The security training needs not to be a massive information package that is shared to the employees at once.

In the following are described how the case company could improve their security training system.

Security training planning

According to the current state analysis the case company seems to be missing a clear plan, how and when employees are trained in security. The plan need not be too exact, but exact enough to track what training is held and should be provided at which time of the year to which employees. One of the PCI logical (2016) and physical (2016) security requirements is to provide employees and guards security training at least annually.

Training needs assessment

According to studies of comprehensive employee security trainings, it is important to do training needs assessment to recognize which topics should be trained to which employees. The training needs assessment should be done regarding to employees' tasks. Based on the current state research there are some specified trainings provided to the employees, but the

training needs assessment doesn't cover the whole personnel at the moment. The training can be built from pieces, but it should be tracked what has been trained to whom and when.

'Welcome to Company X'

'Welcome to Company X' sessions are meant to be part of all employees work orientation. During the research it was noted that the case company has not been able to provide this training as regularly as would have been ideal and some new employees are missing this important security training. The case company could consider having a substitute option for the training. If 'Welcome to Company X' training sessions can't be held for any new employee during the first months of their contract could there be an alternative option for the training to ensure same awareness level of all the new employees. The substitute training is recommended to be in video format.

- The simplest option is a PowerPoint show with voice record (more advanced to have test in the end of the video/after each section to test employees' understanding on the topics)
- Easy to manage and modify
- It is recommended to be HR's responsibility to make sure all new comers watch the video if any new employee has not participated 'Welcome to Company X' session during the first months (exact duration to be decided) of the employment.
- Employees who don't have their personal workstations at the work could be guided to complete training sessions on company's common workstations
- Language options Finnish and English

All expatriates coming from different sites to work in the case company for longer time period could benefit from the video format 'Welcome to Company X'. It has been recognized that expatriates' security training to the company's local security practices has been insufficient (The HR assistant manager, 2018).

Annual training

The company targets to train 80% of their current employees in security annually. Now the case company's annual security training carried by asking employees to read the Security & Safety manual and sign a form that they have done this. Based on the Neil Fleming's VARK model, people can be divided into four groups depending on their dominant learning style

(VARK learn, 2018). This means reading might not be the most efficient learning method to every employee. Also, can be asked, how to ensure that employees really familiarize themselves with the Security & Safety guidebook and do not just sign the form? In the security training questionnaire three most preferred training methods were classroom training, eLearning and workshops. The case company is recommended to use these methods in the future while educating their employees in security.

There also seems to be missing a close follow up about employees who should be trained annually. ISO/IEC27001 (2017) requires to regularly train employees to be familiar with the company's security policies and procedures. KATAKRI (2015) guides companies to train employees on the proper processing and handling of confidential information. Training should be regular and employees who have participated trainings are documented. Recommendations for improvement:

- Annual training sessions for all employees and monitor who have participated. Possibly separate training sets for production and office workers
- language options Finnish and English
- different formats can be used, video, PowerPoint, classroom, workshops etc.
- Share information more purposively about company's different security policies and guidelines and where employees can access them. During the current state research, it was noted that there are employees who don't know where to find company's security manuals and other related documents.
- include environmental and occupational safety matters also to annual training and for employees working in office environment
- If the case company can get a comprehensive eLearning system, could employees be required to complete security related tests with satisfactory results every one or two years

Employees can never be explained too carefully what there are behind of the security policies and guidelines they are supposed to comply with. For example, all the company employees are aware that they should have their ID badge visible, picture side up, always when inside of the company's premises. When employees understand this requirement is based on an external security requirement and isn't just 'something that the security team tells to do' it is easier for the employees comply with the requirement.

Regular security related updates

The respondents' answers indicate that the employees would like to receive security related updates from frequently and therefore the case company's security team is recommended to start launch current security related topics and other educative material regularly.

According to the questionnaire results the respondents would be interested on receiving some current and regular security themed updates. The case company's security team (in co-work with internal communication personnel) could launch local security related newsletters (or similar) to share current security related information with the employees. The publications do not need to be 'too serious' but still educative and informative.

Remote working and mobile device policies

42% of the questionnaire respondents work remotely and 74% have been on a business trip. One of the requirements of ISO/IEC27001 (2017) is to have remote working and mobile device policies, which should be communicated to the employees. The author could not identify these policies existing during the current state research. Therefore, the company is recommended to form local guidelines for employees working outside of the company's premises. The guidelines could clearly point general rules for remote working and describe how employees should protect information that is accessed, stored and processed when working outside of the company's premises.

Crypto graphic's controls policy

ISO/IEC27001 (2017) includes a requirement of training employees in the company's crypto graphic policy. This kind of training could not be recognized during the current state research and there can be identified a gap between of the case company's current and desired states of the security training system.

Social media

There are pages long corporate social media guidelines. Social media best practices are included in the new employees' Welcome guide but are also recommended to be added to 'Welcome to Company X' session materials, Security & Safety guidebook and to future annual training materials.

Managing security incidents

There is a guideline in KATAKRI (2015) and there is a section in Occupational Safety and Health Act that employees should to be trained managing security incidents and the training should be documented and practised. This is the topic the most respondents wanted to have

further training of and the average result in the questionnaire for the respondents training level in security incidents was 1.8. Managing of security incidents is recommended to be included in the case company's Security & Safety guidebook more comprehensively or otherwise provide employees with training on the topic.

Clear table and screen policy

In ISO/IEC27001's Appendix A there is a recommendation for the companies to implement clear table and screen policy. The company is recommended to implement clear table/screen policy because there are open plan offices in the company's premises and it has been unofficially observed that people leave papers lying on their desks and laptops unlocked when leaving their workstations.

6 Summary

This bachelor's thesis project was started in spring 2018 after discussions with the case company's human resources assistant manager and with the company's security manager. The security manager of the company had recognized one function in the company's security management system, security training, that would need some improvement actions and at the same time to be suitable subject for bachelor's thesis.

The time related goal was to have the most critical part of the work done by the end of September 2018. This goal was partially reached. The objectives of this bachelor's thesis were to research the case company's security training systems current and desired states and to identify gaps and improvement opportunities between of the states. The researches were conducted using gap analysis's methodology.

The security training questionnaire, which was conducted during June and July 2018, was a part of the current state analysis and one of the first actual completed tasks of the research. After the questionnaire the author of this study started analysing requirements and documentation of learning and security training systems that formed the theoretical framework of the security training and describes the desired state too. Unstructured interviews were held in September 2018 after the author had analysed the results of the security training questionnaire. The interviewees were picked from the recommendations of the case company's security manager. The objectives of the interviews were to gain further knowledge of how the security training is implemented and to get supportive data to the security training questionnaire results and to gain better understanding of the roles the roles and responsibilities of the managers educating employees in security. The desired state of the security training was mainly formed by using qualitative data analysis to research standards, acts and other relevant documents that the case company aims to comply with. The qualitative data analysis

was done by using a four-staged content analysis. Most of the actual writing was done during autumn 2018.

This bachelor's thesis did not include implementation tasks. It is the case company's decision, which parts of the recommendations for improvement they implement to their security training system. As a part of the implementation the case company could also build metrics to measure the functionality of the security training. As the case company's security manager (2018) said that the provided quantity of the security training does not tell anything about the quality of the training. Therefore, the possible metrics could be considered on measuring both the quality and quantity of the security training in the future.

In the author's point of view the research problems were solved and the objectives reached. The collaboration with the case company was seamless and the representative of the case company, the company's security manager, showed their commitment to the project by giving their support at all the phases of the project to ensure its successful results. The project taught the author more about security management, security standards, security training systems and self-management. After completing this project, the author is more capable to participate long-term projects and has gained further knowledge on many phases of security management.

References

Printed sources

Brown RB. 2006. Doing Your Dissertation in Business and Management: The Reality of Research and Writing. London: Sage Publications

Carnell, E & al. 2000. Learning about Learning: Resources for Supporting Effective Learning. Routledge, 2000. ProQuest Ebook Central ä

Creswell J. & 67 Clark V. 2011. Designing and conducting mixed methods research. 2nd edition. London: Sage

Hennink M. & Hutter I., Bailey A. 2011. Qualitative Research Methods. London: Sage

ISO 14298:2013 Graphic technology — Management of security printing processes

ISO/IEC 27001:2017 Information technology — Security techniques — Information security management systems — Requirements

Kovacich D. & Halibozek E. 2003. The Manager's handbook in corporate security. Establishing and managing a successful assets protection program. Amsterdam: Butterworth-Heinemann

Kumar R. 2014. Research methodology – a step by step guide for beginners. 4th edition. London: Sage

Leppänen J. 2006. Yritysturvallisuus käytännössä. Helsinki:Talentum

379/2011 Rescue Act

738/2002 Occupational Safety and Health Act

Electronic sources

Bengtsson, M. 2016. How to plan and perform a qualitative study using content analysis. Accessed on 2nd of September 2018. https://ac.els-cdn.com/S2352900816000029/1-s2.0-S2352900816000029-main.pdf?_tid=03697671-027c-4a35-8904-6c0d500f0139&acdnat=1535899241_07cf42a0d5ef96fb77e028961eba4174

Cherry, K. 2018. Overview of VARK learning styles. Accessed 1st of September 2018. https://www.verywellmind.com/vark-learning-styles-2795156

Dapzury V. & Pallavi S. 2018. Interview as a Method for Qualitative Research. Accessed on 25th of August 2018. https://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf

DeFranzo S. 2011. What's the difference between qualitative and quantitative research? Accessed on 26th of August 2018. https://www.snapsurveys.com/blog/qualitative-vs-quantitative-research/

FoodRisc resource centre. 2018. Mixed methods research. Accessed on 18th of August. http://resourcecentre.foodrisc.org/mixed-methods-research_185.html

Hall, S. 2018. How to do content analysis. Accessed on 14th of August 2018. https://classroom.synonym.com/content-analysis-2670.html

Hight, S. 2005. The importance of a security, education, training and awareness program. Accessed on 9th of September 2018. http://www.infosecwriters.com/Papers/SHight_SETA.pdf

GDPR Association. 2018. Understanding GDPR Fines Breaking down the Penalties, Fines and Liabilities. Accessed on 12th of August 2018. https://www.gdpr.associates/what-is-gdpr/understanding-gdpr-fines/

European Commission. 2018. Data protection in the EU. Accessed on 12th of August 2018. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Koppa. 2010. Quantitative research. Accessed on 26th of August 2018. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/strategies/quantitative-research

Koppa 2. 2010. Case Study. Accessed on 26th of August 2018. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/strategies/case-study

McLeod, S. 2014. The interview method. Accessed on 16th of August. https://www.simplypsychology.org/interviews.html

McLeod, S. 2018. Questionnaire. Accessed on 26th of August 2018. https://www.simplypsychology.org/questionnaires.html

McIlwraith, A. 2007. Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness. Routledge ProQuest Ebook Central. Accessed on 10th of August 2018. http://ebookcentral.proquest.com/lib/laurea/detail.action?docID=429792

Mortman, D. 2009. End-user Compliance: Creating a security awareness training program. Accessed on 9th of September 2018. https://searchsecurity.techtarget.com/tip/End-user-Compliance-Creating-a-security-awareness-training-program

Payment Card Industry (PCI). 2016. Card Production and Provisioning. Version 2.0. Logical Security Requirements. Accessed on 17th of November 2018. https://www.pcisecuritystandards.org/documents/PCI_Card_Production_Logical_Security_Requirements_v2_Nov2016.pdf?agreement=true&time=1484176101208

Payment Card Industry (PCI). 2016. Card Production and Provisioning. Version 2.0. Physical Security Requirements. Accessed on 17th of November 2018. https://www.pcisecuritystandards.org/documents/PCI_Card_Production_Physical_Security_Requirements_v2_Nov2016.pdf?agreement=true&time=1484176101226

Puolustusministeriö. 2015. Katakri. Accessed on 6th of October 2018. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Robert Wood Johnson Foundation. 2008. Unstructured interview. Accessed on 16th of August. http://www.qualres.org/HomeUnst-3630.html

Rouse, M. 2011. Security awareness training. Accessed on 9th of September 2018. https://searchsecurity.techtarget.com/definition/security-awareness-training

Stephanie D. 2005. The importance of a security, education, training and awareness program. Accessed 4th of August 2018. http://www.infosecwriters.com/Papers/SHight_SETA.pdf

Study.com. 2018. Writing research questions: Purpose & Examples. https://study.com/academy/lesson/writing-research-questions-purpose-examples.html

VARK Learn. 2018. The VARK modalities. Accessed on 1st of September. http://vark-learn.com/introduction-to-vark/the-vark-modalities/

Youchum, C. 2018. Conducting A Gap Analysis: A Four-Step Template. Accessed on 5th of October. https://www.clearpointstrategy.com/gap-analysis-template/

Crosby, P. 2017. 5 Common Pitfalls in Current State Analysis. Accessed on 25th of August 2018. https://www.bobtheba.com/blog/2017417/5-common-pitfalls-in-common-state-analysis

Unpublished sources

The HR assistant manager. Company X. 28.9.2018. Interview. Finland

The production manager. Company X. 12.9.2018. Interview. Finland

The QHSE manager. Company X. 10.9.2018. Interview. Finland

The security manager. Company X. 6.9.2018. Interview. Finland

Figures

Tables

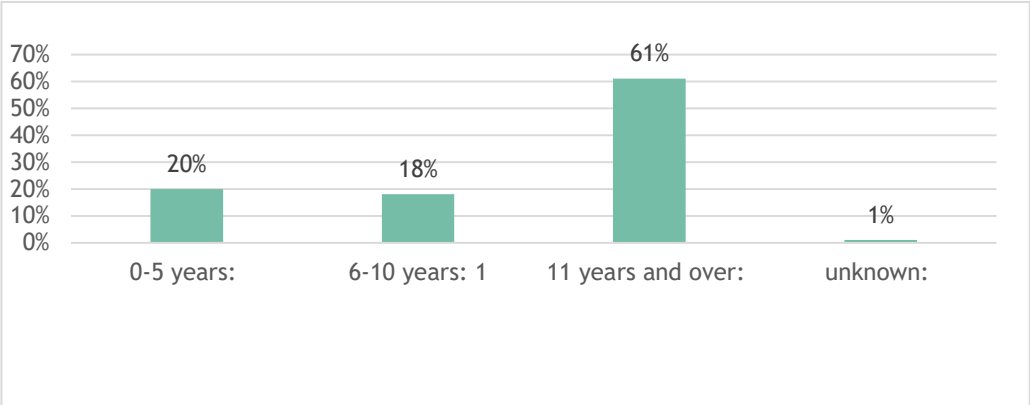
Appendices

Appenidix 1. Security training questionnaire results

Security training questionnaire results (100%=117)

Section 1

1. Duration of employment *



2. Work department *

Production	29 %	
Other		71 %

Section 2

1=no training 2=initial training 3=comprehensive training

1. Have you been trained for the following fire safety and evacuation practices? *

	x̄
How to act if you notice a fire	2,3
How to act if you hear fire alarm	2,5
Location of emergency exits	2,5
Location of fire extinguishers	2,3
Practice to keep emergency exits clear	2,3

2. Have you been trained for the following physical security practices? *

	x̄
How to act if you lose your access card	2,2
How to act if you forget your access card home	2,3
Visitor notification	2,1
Hosting visitors	2
How to act if you meet a suspicious person in the company's premises (for example, a visitor without a host in production area)	2

3. Have you been trained for the following security matters when working outside of company's premises? *

	x̄
Safe business travel practices	1,7

Guidelines for working remotely	1,6
Safe use of Wi-Fi networks	1,7

4. Have you been trained for the following occupational safety matters? *

	x̄
Hazards and risks in your own work	1,8
Safe use of machines and devices	1,9
Duties and responsibilities related to occupational safety in your own organization	1,9
Safe use and storage of chemicals	1,6
Reporting of near miss situations	1,8
How to act in a case of work place/commute accident	1,9

5. Have you been trained for the following environmental safety practices? *

	x̄
Reducing consciously environmental impacts	1,6
Reporting of environmental damages	1,5
Sorting and disposing of waste	1,9

6. Have you been trained for the following information security practices? *

	x̄
Company's data classification policy	2,2
Company's social media guidelines	2,1
Identifying information security threats	2,2
Confidentiality in your own work	2,4

7. Do you handle personal data in your work? *

Yes	49 %
No	51 %

8. If you answered 'no' on the previous question, you can continue to question number 9. Have you been trained on the following two requirements concerning personal data?

	x̄
Requirements of EU's General Data Protection Regulation (GDPR)	2
Requirements of Finnish Personal Data Act	1,7

9. Have you been trained for the following security incident practices? *

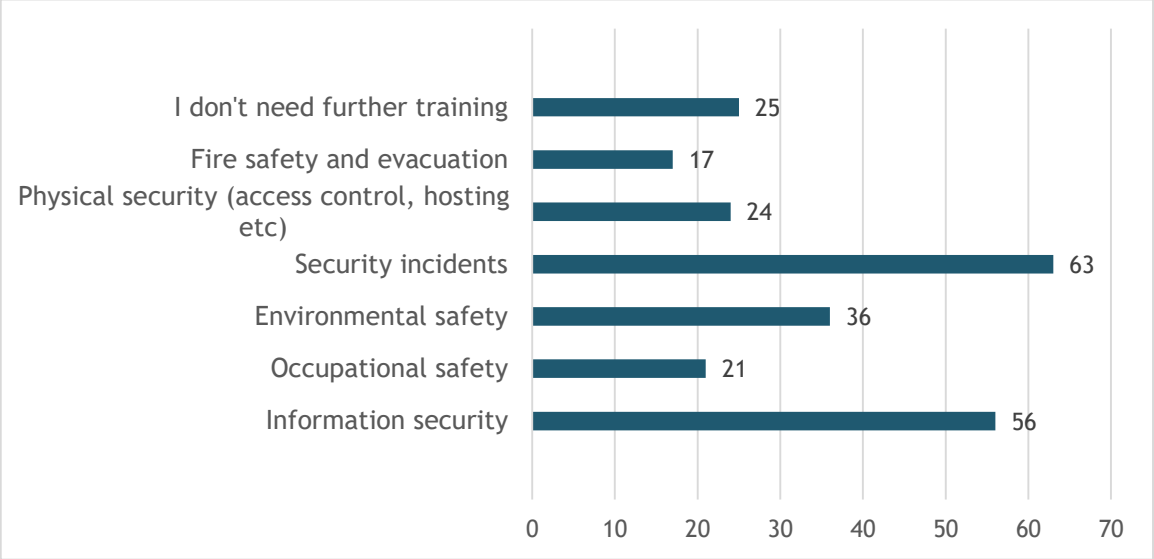
	x̄
Definition of security incident (What is security incident?)	1,8
How to act if you notice a security incident	1,8
Reporting of a security incident	1,8

10. Have you been trained to act according to security requirements? *

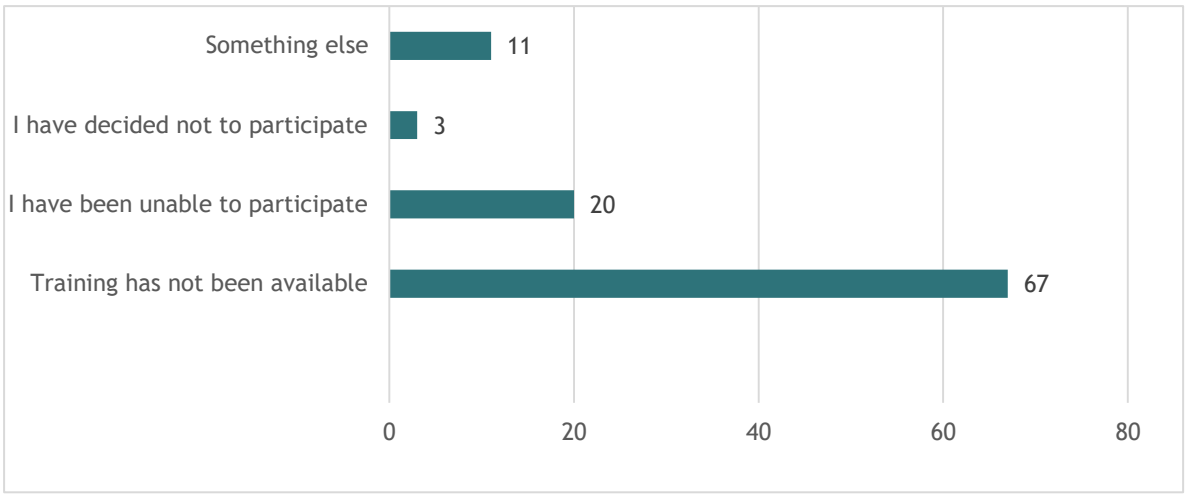
x̄

Security requirements in your own work 2,1

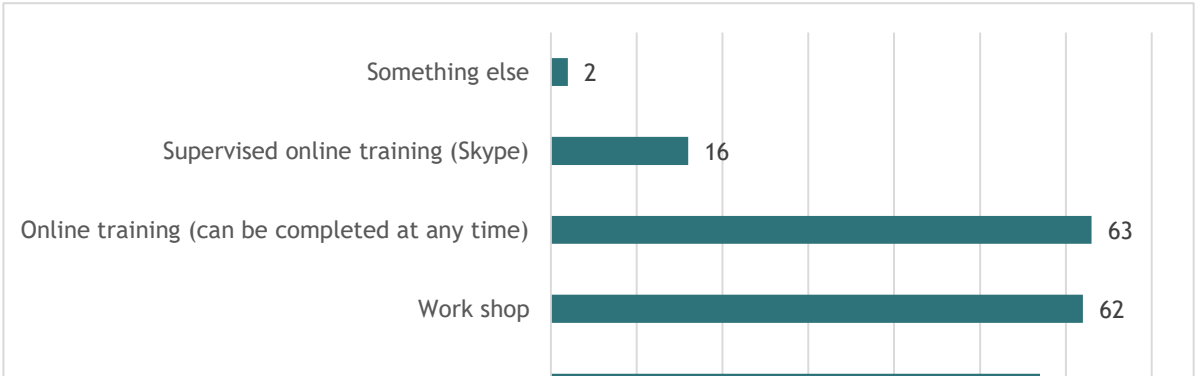
11. Which of the following topics would you like to get further training for? * (Multiple choices possible)



12. If you think your security training has been insufficient, what is the reason why? (Multiple choices possible)



13. Which of the following is the best learning method for you? * (multiple choices possible)



Online training (can be completed at any time)	63
Supervised online training (Skype)	16
Something else	2

1. Do you ever work remotely? *

Yes	42 %
No	58 %

2. Have you been on a business trip? *

Yes	74 %
No	26 %

3. Have you hosted vistors?

Yes	62 %
No	38 %

4. Have you participated to an evacuation from the company's premises during the past 12 months?

Yes	85 %
No	15 %

5. Did you participate to Safety Day training in 2017 or 2018? *

Yes	44 %
No	56 %

6. Have you completed security training modules in eLearning portal? *

Yes	68 %
No	32 %

Appendix 2. Gap analysis chart

GAP ANALYSIS CHART	Current					
Desired state's requirements	1st day introduction by HR	Supervisor/ manager training at the workplace	Welcome to Company X session	Turvakansio/Safety &Security guidebook	Corporate's eLearning (voluntary)	Safety day (voluntary)
Occupational health and safety act						
know what hazards and risks are in their work	-	X	X	-	-	X
have knowledge on work, work environment, safe production practices and tools	-	X	X	-	-	X
be familiar with safe work practices especially before starting in new job/position or when employee's position changes	-	X	-	-	-	-
know how to reduce risks and hazards in the work	-	X	X	/	-	X
know how to avoid harms and hazards	-	X	X	/	-	X
know how to practice during maintenance, repair or cleaning processes	-	X	-	-	-	-
know how to operate in a case of a security incident	/	X	X	/	/	/
improve work safety in co-operation with the employer	-	X	X	-	-	X
follow employer's instructions and take care of own and other employees' safety and health	X	X	X	/	-	X
correctly use personal protective equipment (when needed)	/	X	/	-	-	/
know how to handle hazard substances correctly	-	X	X	-	-	X
know how to act in a case of workplace accident or sickness	X	X	X	/	-	X
Rescue Act						
know how to act if observed or received information about a fire or other accident	/	X	X	X	-	X
avoid the risk of a fire or other accident and the damage it causes	-	X	X	X	-	X
prevent accidents and know what actions to take in accidents and dangerous situations.	/	X	X	X	-	X
ISO/IEC 27001:2017						
classification of information policy	/	/	/	/	X	-
data labelling policy	-	/	/	/	X	-
remote working policy	-	/	-	-	/	-
mobile device policy (risks related to use of different mobile devices)	-	/	-	-	X	-
disciplinary process if an employee has committed an information security breach	-	/	-	-	/	-
cryptographic's controls policy	-	/	/	-	/	-
clear desk and screen policy	-	/	-	-	X	-
ensure that unattended equipment (laptops, mobile devices etc.) has appropriate protection	-	/	-	-	X	-
know that information security must be addressed in project management	-	/	-	-	X	-
Katakri 2015						
security guidelines are trained and available for all employees	X	X	X	X	/	/
managing security incidents	/	X	X	/	/	/
proper processing and handling of confidential information	X	/	X	X	X	-
visitor procedures	X	/	X	X	-	-
threats of malwares	-	/	-	-	/	-
information security policy	X	/	X	X	X	-
ISO14298:2013						
security policies	X	/	X	X	X	X
employee's work's influence to company's security objectives	X	X	X	X	-	X
security rules and procedures	X	X	X	X	X	X
PCI CP physical and logical						
company's security manual (content and where to find it)	/	X	/	X	-	-
reporting of abnormalities	X	X	X	/	/	/
reporting of observed breaches of the established security policy	X	X	X	/	-	/
mobile device policy (HSA)	X	X	X	X	-	X
visitor procedures	X	/	X	X	-	-
password policy	/	/	/	-	X	-