Implementation of ISO 27002:2017 Cyber Security Risk Management guide

Krista Johansen

2020 Laurea

Laurea University of Applied Sciences

Implementation of ISO 27002:2017 Cyber Security Risk Management guide

Krista Johansen
Security Management
Bachelor's Thesis
June 2020

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Thesis

Krista Johansen

Abstract

Implementation of ISO 27002:2017 Cyber Security Risk Management guide

Year 2020 Pages 33

The utilization of cyber dimensions in the operational activities of organizations has grown exponentially in recent years. As functions are networked, their dependence on the functionality of cyber environments is also increasing. Protecting the cyber environment is paramount to business continuity, and the integrity of corporate information. Efforts are often made to protect the cyber environment with technical resources, and the weakest link, the user of the systems might be forgotten. Human error is the cause of over 95 % of data breaches and the weakest aspect of cyber security. Employee awareness of cyber security risks and vulnerabilities should be promoted, and the capacity of cyber security expertise should be increased through training.

The objective of this thesis was to produce a Cyber Security Risk Management guide for a certain Data Center. The guide is based on the ISO 27002 standard. The purpose of the guide is to serve as a tool for increasing the cyber security awareness and competence development of the employees of the organization.

The research methods used were literature review and dialogical discussion. The literature review is based on elements extracted from the ECHO-framework, that have been considered to best support the objective of this thesis. The dialogical discussion was utilized in the form of review meetings with company representatives during the production process of the guide. The concrete outcome of this thesis is the Cyber Security Risk Management guide. The analysis of the materials, and the reviews by the company representatives enabled continuous development. The compilation of the guide has considered the purpose and necessity of each control from several perspectives, in order to achieve the most relevant outcome for the organization.

It can be concluded that the guide produced meets the set objectives. The guide will be included into the cyber security training designed by the company and will serve as part of the training material. Since this thesis did not follow the introduction of the cyber security training, the effectiveness of the guide is difficult to evaluate. Properly utilized the guide will, however, increase the capacity of employee risk awareness and cyber security expertise, and thus enhance the organization's protection against cyber threats.

Keywords: cyber security, ISO 27002 standard, training

Table of Contents

1 Introduction

The field of cyber security has been rapidly evolving over the past few years. With the proliferation and development of cyber threats, organizations have started to pay more attention to information security, technology protection and personnel security expertise. The EU General Data Protection Regulation (GDPR), which came into effect in 2018, updates of SFS standards like ISO 27002:2017, and ECHO project launched at spring 2019 are some great examples of the recent developments in the field of cyber security in Europe.

Hackers and their ways are evolving and the scope of cyberattacks is expanding. Sources of the cyber threats are constantly finding new and more effective ways to attack and disrupt organizations. One of the biggest issues are blackmail programs and their rapid growth. Other significant cyber threats focus on hardware's, exploiting vulnerabilities, destroying business operations and stealing information. (Lehto et al 2017, 12, 21-22.) Therefore, risk awareness based on cyber security and particularly skills and tools to manage it, should be actively promoted.

This thesis is based on assignment to create a Cyber Security Risk Management guide, leaning on ISO 27002:2017 for certain Data Center in Finland. The wish of the organization was to get a guide ready for use to help increase employee knowledge about managing cyber security risks. The guide is provided for the sole use of the company management and internal employees. The company management intends to create a cyber security training course to their internal web, utilizing the guide created by the author of this thesis as a part of a training material. Internal employees must complete the cyber security training course at regular intervals to maintain the level of cyber security expertise the organization requires. The cyber security training course will be updated whenever necessary, and in line with new regulations and updates. To support the effective implementation, this thesis also provides method suggestions for executing the cyber security training course.

The first chapter covers the introduction together with key concepts and definitions. The second chapter builds the knowledge base around ECHO-derived framework. The areas selected to examine the development of cyber security expertise are Cyber skills, Cyber range and Certification scheme. The third chapter is dedicated to methodology that includes the description and the implementation process of the Cyber Security Risk Management guide. The fourth chapter presents the results, and the fifth chapter contains conclusions and self-assessment.

1.1 Key concepts and definitions

Referring to Vilkka (2015, 37) the theoretical framework and concepts chosen for the research should always be explained and defined clearly and precisely to the reader of the text. This section introduces shortly the key concepts related to this thesis.

Cyber security

Cyber security can be described as a target state, where the operating environment can be trusted and secured. Cyber security covers measures that proactively manage and if necessary, tolerate various cyber threats and their effects. (Vocabulary of Cyber Security 2018, 22.)

Information security

Information security refers to the arrangements that are made to ensure availability, integrity and confidentiality of information. It can also mean conditions where security risks are under control. (Vocabulary of Cyber Security 2018, 15.)

ECHO:

The ECHO abbreviation comes from the words European network of Cybersecurity centres and competence Hub for innovation and Operations. The project is launched by European Comission and it was officially published in February 2019. The purpose of the project is to establish and operate a cyber security competence network across the EU. (European Comission 2019.)

ISO 27002:2017

The ISO 27002:2017 is information technology related standard, which includes security techniques and code of practice for information security controls. The standard is intended for use in developing information security management guidelines, takin into account the company's industry-specific risk environment. (ISO 27002:2017.)

For the relevance of this thesis, it is important to understand the differences between cyber- and information security. According to Ellis & Mohan (2019, 119) cyberspace refers to a geographically unlimited virtual space where transactions take place regardless of time, distance or location. Cyberspace refers not only to the space constituted by information and communication technologies (ICT), networks, and ICT-infrastructures, but digitally interconnected human and organization activities. Cyber security contains the process and the result of making cyberspace secured. Where cyber security includes everything in cyber dimension, information security contains the protection of information, hardware, software,

telecommunications and operations (Vocabulary of Cyber Security 2018, 15). Although ISO 27002:2017 focuses on information security, the wider expression of cyber security is mainly used in this thesis in order to achieve conformity and the holistic approach.

2 Literature

2.1 The ECHO project

ECHO (European network of Cybersecurity centres and competence Hub for innovation and Operations) is a four-year long project to develop, model and demonstrate a network of cyber research and competence centres. The project was launched in February 1, 2019 and is scheduled to be completed by the end of January 2023. The overall budged is 15,9 million euros and the project is coordinated by Royal Military Academy of Belgium (European Comission 2019). The project consortium consists a total of 30 partners from different fields including health, technology, industry, education, research and defence (ECHO 2019a). Laurea University of Applied Sciences is also participating the research as one of thirty project partners.

ECHO's main objective is to improve proactive cyber defence of the European Union by enhancing Europe's technological sovereignty through effective multi-sector and domain collaboration (ECHO 2019a). With the ECHO Governance model as the centre, the framework presents in addition five sections, which are shown in the Figure 1 below.

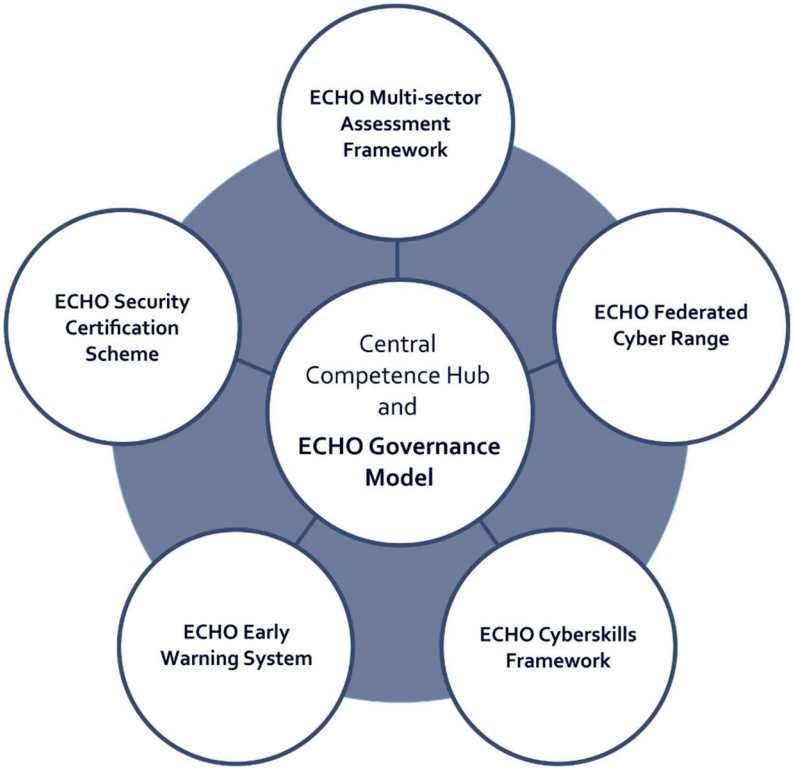

Figure 1 ECHO framework

Multi-sector Assessment Framework refers to challenge and opportunity analysis in sector-specific cyber security use cases (European Comission 2019). It focuses on horizontal technologies and cyber security in selected critical sectors, addresses inter-sector dependencies and transversal security aspects. The framework provides a foundational approach for organizations to assess their current position of security and to develop a roadmap to investments, technological advancements, training and process innovations aimed to protect the assets against cyberattacks. (ECHO 2019b.)

Federated Cyber Range includes operation of a Multi-sector simulation for training. Multipurpose virtual environment is used to develop and demonstrate the technology roadmaps. It provides a safe environment for practical cyber skills development and realistic simulations to improve system assurance. (ECHO 2019c.)

Cyber Skills Framework provides the foundation of developing cyber security education and definition of transversal, and inter-sector skills and qualifications (European Comission 2019). A learning-outcome based competence framework includes a set of skills and knowledge, professional profiles, three sample training programmes, methodology and content for blended trainings, monitoring and assessment framework. (ECHO 2019d.)

Early Warning System refers to precaution and incident response. It is a security operations support tool, which enables members to coordinate and share cyber relevant information in real-time ensuring secure information sharing between organizations. System coordinates incident management workflows and retains the control of cyber-sensitive information. (ECHO 2019e.)

Security Certification Scheme in turn provides methodology used to achieve sector specific status of technologies compliant with the ENISA and EU defined approach for cyber security certification framework (ECHO 2019f).

The ECHO framework is used as a basis for building the theoretical part of this thesis. The original frame has been reduced to three areas that have the best capacity to support the appropriate implementation of the Cyber Security Risk Management guide. Table 1 below shows the selected areas, and topics covered in each section. The topics covered in each section have been selected to correspond the aim of the thesis as well as possible. The main three areas selected under consideration are Cyber skills, Cyber range and Certification scheme. The first section, Cyber skills includes cyber security related national competence development. Second section, Cyber range reviews different training methods- and techniques associated with cyber security. The final section, Certification scheme focuses on ISO 27002:2017. (Table 1.)

Table 1 ECHO-derived framework of the Cyber Security Risk Management guide (Modified from ECHO 2019b)

2.2 Cyber skills: National competence development

According to Lehto et al (2017, 34) cyber security expertise is not only a separate professional area of expertise, but it covers capabilities from civil skills to excellence. Finnish society needs versatile cyber security expertise in both public administration and business to manage cyber security risks. At national level need to ensure that companies have sufficient availability to top professionals and other skilled personnel. Competence development is also emphasized in cooperation between industry and research. Collaboration, exchanging information on customer needs and improving service development, significant new knowledge can be created within the national internal market. Companies whose actual business is outside the cyber security field, but whose operations are significantly affected by cyber security and related disruptions will play an increasingly important role in the future. Such areas like telecommunications, energy production and distribution, finance and insurance and health care have been outlined particularly in the legislative projects on network and information security. (The Finnish cyber security strategy 2019, 8-9.)

Other strategic measures to promote cyber security expertise are (1) strengthening training programs related to cyber and information security, software and application development, and computer networks and telecommunications in vocational education, polytechnics and universities, (2) ensuring the high level of education required for nationally critical cyber expertise areas (3) strengthening national cyber security research, development and testing activities (4) raising awareness of the security of new services and products and (5) developing a national digital security education and training system as part of public

administration digital security education that develops the skills of public administrations, businesses, other stakeholders and citizens. (The Finnish cyber security strategy 2019, 9.)

The level of competence is one key indicator of the state level cyber security. Finland has a good reputation in international cyber security market. Finnish expertise, however, must be increased in order to become a pioneer in the field of cyber security. It is also about recognizing the skills needed in a rapidly changing technological development. The key challenges for cyber security industry are lack of skilled personnel and recruitment difficulties. Training of experts requires better coordination between fragmented education, and research institutions, as well as the diversification of research activities. For example, the importance of human sciences in technological development and interdisciplinary cyber security research are emerging trends around the world, but still very limited in Finland. It is important that the areas of cyber security competence and research can be shared in a coordinated way between universities, colleges, educational institutions and research institutes. Cyber security education, research, technology development and innovations are national differentiating factors in the pursuit of pioneering. (Lehto et al 2017, 71-72.)

Finland has all the prerequisites for developing the cyber security industry and expertise, due to its high level of research, development and innovation activities carried out in cyber security field. High-level expertise can be found, for example, in virus protection, identification and identity management, firewalls, cryptology, mobile security and cyber security services. Finland has also been internationally at a forefront of developing a national cyber security strategy. International competition, however, has intensified and many countries such as Estonia, Netherlands, United Kingdom, Germany and Israel have made significant investments in cyber security. Although Finland has a high level of expertise, the top of research and enterprise centralizes on quite small number of operators. A significant phenomenon in the Finnish cyber security field has also been the sale of companies abroad. The transfer of top companies to foreign ownership may pose a risk from national cyber expertise and self-sufficiency point of view, as knowledge is transferred out of Finland through acquisitions. Synergies may affect Finland's international competitive position. (Pelkonen et al 2016, 66-67.)

Despite the high-level of Finnish technical expertise, there are also clear deficiencies that can be identified in three areas. The first relates to theoretical cryptology, which knowledge is very narrow. The second is cyber security sales, marketing and export expertise. The lack of marketing and export expertise is particularly evident in the fact that export activities do not correspond to the advanced technical solutions of the industry. The third skill gap concerns the cyber security perspective as a cross-cutting, multidisciplinary and strategic issue. More comprehensive and diversified expertise is needed to address cyber security related issues. (Pelkonen et al 2016, 67.)

2.3 Cyber range: The cyber security training

As business operations becomes more reliant on cyber security the education and training must follow the development and meet the ever-increasing expectations and requirements (Irons 2019, 136). Education and training are often used interchangeably, even though they differ in purpose. Education helps to build awareness by explaining the concept in theory but does not necessarily lead to behaviour changes that would be the desired outcome. Training on the other hand aims precisely to that. Theoretical knowledge alone is not enough, if one doesn't know how to apply it. Training is about putting that knowledge into action. (Crumbaugh 2019, 23.)

According to Irons (2019, 145) the balance between the theoretical and conceptual knowledge is important in order to develop the cyber security proficiency and practical skills that supports the application of the knowledge. The hands-on experience is suggested to be the best way of learning. The challenge of cyber security training is to reflect the complexity of reality, and design activities that can be successfully achieved in relatively short time periods. (Irons 2019, 146.)

Maintaining the sufficient information security level is relevant for keeping organizations data safe from malicious affect. Information security is used to ensure networked computers and servers being reliably available to users and securing the data of these devices. To ensure a security of a network, threats are required to be responded immediately as they appear. This requires training for different aspects of network security and strong knowledge base of various network services. (Chapman, Smith, Maglaras, Janicke 2017, 1.)

According to Chapman et al (2017,1) one usual method of training is to create cyber defence exercises consisting the minimum of two teams. One team is defending a computer network and the other one is attacking it. This type of exercise has been found to be effective, because it offers valuable practical experience of making decisions under pressured environment. It is also suggested that the teamwork element characteristic to these types of exercises may affect the efficiency of the training method. (Chapman et al 2017, 3; Topham, Kifayat, Younis, Shi, Askwith 2016, 59-61.) Compared to the long-term use of such exercises, research data gathered from the simulated network attacks is however, relatively limited.

Grant (2015, 43) emphasizes that simulation is effective technology to gain understanding on how to conduct operations. For conducting professional offensive cyber operations, it is important to perceive how the attack process works. To succeed, attention must be paid on what resources are required, what doctrine should be followed, how cyber and kinetic action can be integrated and how to control and manage these integrated operations. Professional offensive cyber operations research to the tools and techniques has addressed that simulation has several roles to play. Simulation can be used to plan and rehearse cyber operations in the

attack process, to detect and diagnose abnormal situations in managing operations or to provide assistance in the process of decision making in the form of wargaming or operations research. (Grant 2015, 43.)

According to Aldawood & Skinner (2019, 6) training and awareness programs have been in development, as cyber threats and social engineering attacks have been increasing. Modern security training and information security awareness programs are incorporating techniques of simulations, games, virtual labs, themed awareness videos and modules. Despite the progress of modern techniques, Aldawood & Skinner (2019, 6) are pointing out that there are still limitations in enhancing employee preparedness. Social engineers are namely specialized in creating exceptional need for employees to act by using reverse psychology. Methods of awareness training as themed videos and modules are creative approaches but might not have the ability to predict the uncertainties and the psychological aspects behind the socially engineered attacks.

Real-life simulations aim to provide awareness of social engineering and how the attacks are operated. Simulations are used to train employees to think strategically in the attack situations. The simulations do not however take into account the individual differences of the employees. Individuals are essentially different by personality and may understand the same message in multiple ways. Instincts are leading one's way of responding situations. Through their own experiences, individuals have also different levels of trusting and awareness towards the potential of being tricked. These behavioural aspects pose a challenge in designing programs. The simulation should be customizable, rather than preparing similarly for all employees. (Aldawood and Skinner 2019, 6-7.)

Another challenge to modern training techniques is that they are often expense and time consuming (Topham et al 2016). Employees need to set aside their normal professional tasks to complete the required training programs and it may limit the productivity at work. However, if the training is held outside working hours, the participation rate may be low. (Aldawood and Skinner 2019, 7.)

Adams and Makramalla (2015, 6) are pointing out that cyber security skills training is generally offered to IT personnel instead of all employees, while awareness and education programs are targeted to whole staff. Training approaches such as web-based classrooms, teleconferencing and newsletters have been found to be ineffective methods due to large amount of information in short period of time. The overload of information gets participants passive, overwhelmed and uncommitted towards the training. The learning experience should be immersive and interactive in order to engage employees and to achieve more lasting learning outcomes. (Adams and Makramalla 2015, 6.)

Solutions that utilize gaming in cyber security skills training are promoting active learning and motivation while increasing the retention of learned skills. Concept of gamification is described as a process of enhancing a specific service by implementing game design elements in a non-game context to enhance the user's overall value creation and experience. (Adams and Makramalla 2015, 6; Cook, Smith, Maglaras, Janicke 2016, 109.)

Gamification is combining different elements from game design such as progress mechanics, player control, problem solving and background story. It is important to define training goals, when designing games for training and educational purposes. Effective and relevant game design requires the selection of appropriate elements that supports the training. The following recently mentioned elements are upholding cyber security skills training. Progress mechanics provides tools for progress, such as points to motivate the player. Player control signifies the use of avatars. It has been found that the use of different roles through third-person perspective influences behaviour. Problem solving, in turn is a crucial element of learning and retaining new information. To develop strong problem-solving skills and translating them into practical knowledge outside the training environment, it is essential to identify the need of cooperation and goal of common purpose. Finally, stories help player to attach with the avatar, and reinforce the commitment to the game. (Adams and Makramalla 2015, 6-7.)

Gamification incorporates the pursued components like achievements, success and attainment of rewards that naturally motivate people to act. Gaming can increase employee engagement and improve teamworking by transforming routine tasks into game- and competition situations. (Adams and Makramalla 2015, 6.)

2.4 Certification scheme: ISO 27002:2017

ISO (International Organisation for Standardization) and IEC (International Electronical Comission) form a global standardization system. Parties involved to the compilation of standards are technical committees of national member organizations of ISO and IEC, international authorities and other co-operation organizations. ISO 27002:2017 has been prepared by ISO/IEC JTC1 subcommittee SC 27. (ISO 27002:2017, 5.)

ISO 27002:2017 is an international standard intended to be used in the implementation process of an information security management system based on ISO 27001:2017 or as an instructional document for organizations that are implementing commonly accepted information security controls. ISO 27002:2017 is also intended for use in the development of industry or organisation-specific information security management guidelines, their security risk environment considered. (ISO 27002:2017, 6.)

Changes in business processes and systems as well as external changes such as laws and regulatory provisions, may expose new information security risks. While information security risks are impossible to completely avoid, effective information security however, reduces risks by protecting the organization from threats and vulnerabilities. Information security can be achieved by implementing an appropriate management system that incorporates policies, processes, procedures, organizational structures and software/hardware functions. Controls need to be established, implemented, monitored, reviewed and improved when necessary in order to reach security and business objectives defined by the organisation. (ISO 27002:2017, 6.)

It is vital that the organization recognizes its security requirements, which main sources are

- Risk assessment performed by the organization, which considers business strategy and overall business objectives. Risk assessment includes the identification of threats to the protected property and evaluation of vulnerabilities, likelihoods and potential impacts.

- The legal, statutory, regulatory and contractual requirements, which the organization must adhere to.

- The principles, objectives and business requirements developed by the organization to support its operations, regarding information handling, storage, communication, and archiving.

The resources used to implement controls need to be dimensioned against the business disadvantages propably resulting from the absence of controls. The results of the risk assessment can be used to determine appropriate management measures and controls. The choice of controls depends on organizations decisions based on the risk acceptance criteria, risk treatment options and the risk management approach generally applied in the organization. Noteworthy is that all the controls and guidance in the ISO 27002:2017 may not be applicable to every organization and on the other hand, controls and guidelines that are not covered in this code of practise may be required. (ISO 27002:2017, 6-7.) The structure and content of this standard are discussed more detailed in Chapter 3.4.

3 Methodology

The starting point of the development project is identifying the object of development and understanding the factors related to it. Conventionally development project focuses on the business or working life. The object of the development may be for example the introduction

of a new business model, renewal of processes, or the development of new operating models and methods. (Ojasalo, Moilanen, Ritalahti 2014, 23.)

This thesis is a case study research, which aims to produce material and recommend actions for eventually developing the level of intern employee cyber security expertise of the organization. Consequently, it does not aim for immediate change during the process but strives to produce tools for the development of new operating models. The case itself is built on the company-specific targeted application of ISO 27002:2017 recommendations in the form of Cyber Security Risk Management guide. The research is qualitative, due to the subject under study. The data collection methods used in this thesis are narrative literature review and dialogical discussion. The development method exploited to achieve the project objective is ISO 27002:2017 standard.

The objective of this thesis is to produce a comprehensive Cyber Security Risk Management guide to Data Center management. The guide is based on ISO 27002:2017 for the desire of management to adopt and implement the standard as part of the company's procedures in the future. The development of personnel cyber competence takes place through a cyber security training course that management will create utilizing the guide produced. Relying on the theoretical framework and the process of carrying out the Cyber Security Risk Management guide, this thesis also gives proposals for the creation of the cyber security training course. The main purpose of the produced guide and the course later to be designed and implemented, is to develop the cyber security expertise of personnel. The skills acquired are intended to be incorporated into everyday practical working life.

In terms of organization risk management, the subject is limited to cyber security related risks only. This paper covers a review of national competence development and addressing and reducing cyber risks through effective training and ISO 27002:2017 best practices. This thesis does not take a wider view on the organization security policy or the implementation of it. This thesis covers only the implementation of the Cyber Security Risk Management guide, to be later exploited in the planning and implementation of the cyber security training course. The course remains to be carried out by the Data Center management and will be referred only in the context of content formatting of the guide, and in terms of development proposals.

3.1 Case study

According to Ojasalo et al (2014, 53) the development work always relies on theories, methods and previous research. Several scientific disciplines are using the case study from a variety of basis and with different objectives. It is common research strategy especially in business economics. Eriksson & Koistinen (2014, 4) are defining case study as “the

examination of one or more cases for, which the identification, analysis and resolution of the case is the main objective".

Although case study is often linked to qualitative research and methods, it may also have features of quantitative research. Sources characteristic to case study can include interviews, media files, statistics, observation and various documents. Thus, the first prerequisite of the case study is the use of multi-source material. Triangulation is often combined to case study referring to its feature of collecting information from several different sources by using both qualitative and quantitative approach. (Eriksson & Koistinen 2014, 9, 30; Kananen 2012, 34-35.)

The unit under research may be for example a company, service, product or process. The case study provides information concerning the phenomenon of the present time in its real operating environment. The study aims to produce profound and detailed information, therefore orientating into narrow topic is recommended and more profitable than exploring a broad one. (Ojasalo et al 2014, 52.)

In the case study researcher does not participate in the activity of the phenomenon being studied. The case study remains at the detection level. (Kananen 2012, 37.) According to Ojasalo et al (2014, 52-53) case study is suitable for development approach when seeking in-depth understanding of the subject and the aim is to produce new development proposals. In the development of working life, the subject of research is always selected guided by the practical need, and the objective set for the development research.

3.2 Data collection methods

Literature reviews can be divided into three main types, which are narrative reviews, systematic reviews and meta-analysis. The narrative literature review is one of the most commonly used and it can be characterized as an overview without exact boundaries. Although the materials are extensive and their selection is not limited by methodological rules, the phenomenon under investigation can be comprehensively described. (Salminen 2011, 6.) According to Latvala & Tuomi (2020) the literature review is used to outline the subject area of the thesis. It provides an insight into how much research information is available, from what perspectives the subject has been studied and in, which methods. To assist the planning of the literature review, also conceptual analysis can be used. The resulting concept map can be useful in systematic information retrieval. (Latvala & Tuomi 2020.)

The first data collection method used in this thesis is narrative literature review. A concept map, or framework built from the ECHO project (Table 1) supports carrying through the data

collection. The main purpose of the literature review in this context is to examine the subjects related to ISO 27002:2017 content. The areas addressed in the literature review will be applied to the production of the Cyber Security Risk Management guide and the suggestions for implementing the cyber security training course. The exploitation of the ECHO project will provide a sufficiently comprehensive perspective on the subject regarding to the literature review.

Dialogical discussion, or meetings (Salonen 2013, 22) with the client may considered to be the second method of collecting data. Within the dialogical discussion the common goal becomes clearer and more material can be produced to support and promote the execution of the work. Presence may also increase the trust between the client and the author of the thesis.

The aim of the dialogue is to provide an understanding of the views of others and to create meanings for the object of action. Prerequisites for a successful dialogue are equality of participants, active and compassionate listening to other people's perspectives, consideration and questioning of one's own background assumptions, and mutual trust. By listening and striving to understand the views of others, one is also involved in the process of self-development. (Holm, Poutanen, Ståhle 2018.)

In order to illustrate the progress of the process and to demonstrate the application of the methods at different stages of the process, the following Figure 2 incorporates also the methods. The literature review is linked to step 3. Writing/Editing, and the dialogical discussion is linked to steps 1. The first meeting/planning, and 3. Review. The content gathered with the literature review is utilized in parallel with the ISO 27002:2017 to produce the Cyber Security Risk Management guide. The dialogical discussion is utilized in every interacted situation with the client from the first meeting to the last. Instead of brainstorming and other ideation methods, the author and the client strive for an honest and constructive conversation around the subject.

3.3 The Cyber Security Risk Management process

This section describes the general process of producing the Cyber Security Risk Management guide. The guide has been written alongside the thesis for scheduling reasons. The following Figure 2 presents the execution process of the guide.

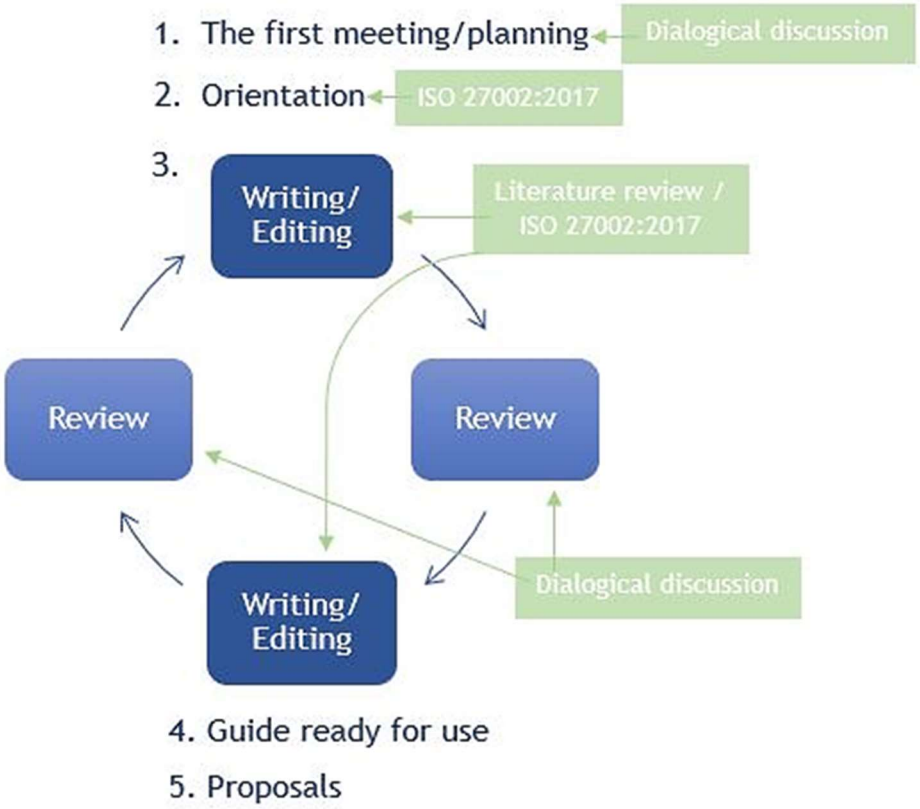

Figure 2 The process of creating the Cyber Security Risk Management guide

The first planning meeting with Data Center Manager (DCM) and Site Security Manager (SSM) was held on company's premises on September 5th. At the first meeting we discussed the interest of the organization management in ISO 27002:2017 and options for starting to implement the standard. The objective of the organization is to increase employee cyber risk awareness by raising the level of cyber security expertise. Thus, the critical area for operations of the Data Center could be covered and secured.

Currently, the cyber security guidelines of the company are limited to Risk Assessment Table and the Operations Manual. The Risk Assessment Table covers general instructions for handling malware and cyberattacks, accessing to systems and applications, accessing to network and network services, unnecessary retaining of storage media, disclosure of information, and teleworking (Risk Assessment Table 2019). The Operations Manual covers only the physical security threats (Operations Manual 2019).

The method of implementation became more precise with the design. Eventually the company representatives and the author of this thesis ended up with a written guide due to its versatile usability and formability. The author took notes through the discussion, and the preliminary dates for material reviews were selected and agreed at the end of the meeting.

The second phase was accessing and orientating to the base material by reading it through. The author used Laurea University's licence to access the ISO 27002:2017. The third phase, writing and editing the guide started in October 2019. The notes taken at the first meeting provided support for the early stages of writing. The notes contained simple guidelines for compiling the guide. The most important precepts were:

- informative and proposing style
- compact and relevant content
- the perspective of question-creation

(The Notes 5.9.2019.)

Content produced by the author was reviewed twice during the process by DCM and SSM of the Data Center. The meetings were held in November 2019 and February 2020 as agreed. The main topics of the dialogical discussion in November 2019 were subdivision of the standard from the perspective of cyber security training for employees and close integration of important aspects. The February 2020 dialogical discussion focused more on re-delimiting the content already produced and cutting back the excess text. On the table were also the structure of table of contents and other finishing touches.

The process of compiling the Cyber Security Risk Management guide is described more detailed in Chapter 3.4. The result the Writing/Editing > Review circle is providing can be found from Chapter 4. The development proposals regarding the cyber security training course are assessed in Chapter 5.

3.4 Implementation of the ISO 27002:2017 Cyber Security Risk Management guide

ISO 27002:2017 includes 14 main security control categories containing 35 security categories and 114 controls. The Figure 3 below shows the basic structure of the management system. Each clause defining security controls contains at least one main security category. The main security categories comprise control objectives, and one or more controls. The structure of control descriptions consists of a control, implementation guidance and if necessary, other information. (ISO 27002:2017, 8-9.)

After the headline, control objective offers a brief description of the purpose of the control, while the control defines the specific control statement in order to achieve the control objective. The implementation guidance provides more detailed information on how the implementation of the control and reaching the control objective should be promoted. However, the guidelines should be considered on an individual basis. Other information may provide further information related to the subject. (Figure 3; ISO 27002:2017, 8-9.)

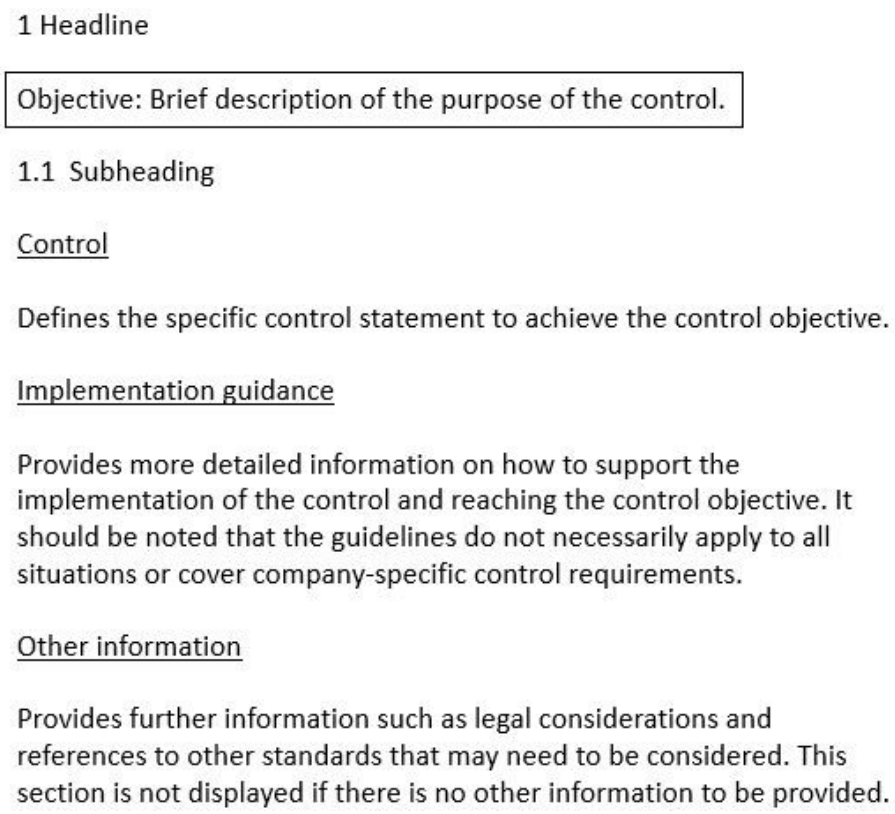

Figure 3 An example of the standard structure

Kohnke, Sigler & Shoemaker (2017, 134) are presenting an illustrative model in Figure 4 showing the main contents of ISO 27001 and ISO 27002 frameworks (Figure 4). As the standard was to be condensed and customized for the use of designated organization, certain parts of the standard were excluded as unnecessary. These certain parts were Information Security Policies, Human Resource Security, Physical and Environmental Security and lastly Information Security Aspects of Business Continuity Management.

Information Security Policies, Physical and Environmental Security and Information Security Aspects of Business Continuity was left out because they have already been outlined on the Operations Manual of the organization (Operations Manual 2019). At the meetings also Human Resource Security was considered redundant sub-region in order to raise the cyber security awareness of personnel. The remaining ten main security categories have been included in the guide. The areas and their weightings were selected based on the meetings, notes taken, and the materials of the organization, such as Operations Manual and the Risk Assessment Table.

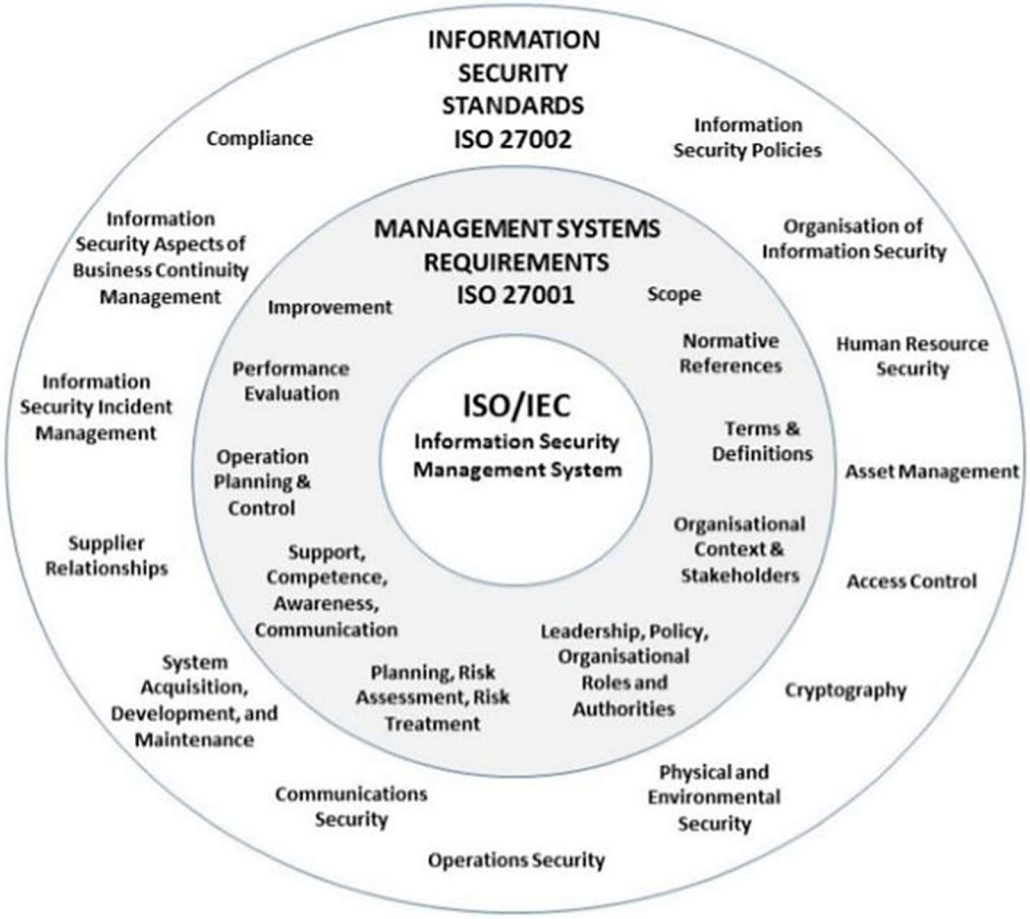

Figure 4 ISO 27001 and 27002 frameworks model (Kohnke et al 2017, 134)

The basic structure of the Cyber Security Risk Management guide is simple, and the layout mainly repeats. Due to the weightings of subject areas, exceptions also exist. Since the activities of the Data Center focus on technology all controls related to network security and data protection were paramount. Therefore, the guide is focused more on Asset Management, Access Control, Cryptography, Operations Security and Communications Security. For effective coverage and integrity of the standard other required categories are briefly mentioned with an eye to the end-use of the guide.

As previously mentioned, the guide is built of ten main security categories and in addition a total of 16 subcategories. Some categories contain more information, and with some it has not been considered necessary. However, all categories contain at least a description of the purpose of the control, or a list of recommended actions related to the subject. Categories may, for example explain why the control should be implemented in, which the control is based, and what guidelines should be considered, to cover the control objective.

The following extract from chapter 3.3 System and application access control of the Cyber Security Risk Management guide contains both, a description of the purpose of the control and a list of recommended actions:

“To prevent unauthorized access. Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy. The following guidelines should be considered in order to support access restriction requirements:

- providing menus to control access to application system functions
- controlling the access rights of users
- limiting the information contained in outputs
- providing physical or logical access controls for the isolation of sensitive applications, data or systems”

(Cyber Security Risk Management guide 2020, 7.)

The order progresses from general to individual. The System and application access control presented above extends to log-on procedure, password management system, use of privileged utility programs and up to the program source code. The complete Cyber Security Risk Management guide contains 16 pages, and the full table of contents of the guide produced can be found in the appendices (Appendix 1).

4 Results

An overview to national competence and future goals provided perspective on Finland's position as a prominent figure of cyber security. Finland strives to be a pioneer in cyber security, which requires active development of co-operation in research, education and working life. Efforts must be made to increase the capacity of cyber security education and to lower the threshold of applying to studies. In ever increasing networked world, the cyber security basics should be offered flexibly already from primary school onwards. Investments should also be made to increase the multidimensionality of expertise, and particularly to develop identified weaknesses and technological solutions.

An overview to cyber security training opened doors to various training techniques and their shortcomings. Already at the beginning of the information search, the author encountered a problem of narrowness on the topic. It was unexpected and surprising. Universally validated theories were difficult to find, as the articles focused mainly on creating and testing new

training techniques than reinforcing old ones. However, similarities that can confirm the functionality of certain types of training techniques were eventually found.

Simulations built in the form of divergent games have found to be functional and practical for training purposes. The advanced technology of simulations allows the emulation of real cyber-attack. The inclusive and interactive training is perceived meaningful. Competitive situation is a natural way to influence trainee's motivation on increasing the performance and concentration. Simulations should be customizable according to the intended use. The purpose and need for training should be justified to employees and included in the work as a concise package, so that employees do not feel forced to be flexible about their own work assignments. When well-designed training is incorporated as a recurring part of company's procedures, the questioning of its necessity is reduced. The company is best at knowing its own employees. If sufficient expertise and resources are available, company could plan and execute the training itself, or at least participate the planning and implementation of the training in cooperation with the service provider, if the function is outsourced.

The review to ISO 27002:2017 standard was done at a general level, as it was difficult to find information from the application of it. The overview of the standard served as basis for writing the guide. Writing the guide was a long and complex process. Controls had to be included in the document with the end use in mind. The goal of condensing the standard also brought its own challenge, in which case the necessity of the content had to be assessed and the essential things had to be extracted from the standard. To ensure this, the documents of the organization were also exploited in writing the Cyber Security Risk Management guide. By analysing and comparing the contents of the documents an understanding of the processes already existing in the company was formed, which could be excluded from the guide.

On the other hand, examining the areas derived from ECHO alongside writing of the guide provided different and fresh perspectives on what kind of expertise is needed and how to increase it. The author mirrored the ECHO-derived framework to the guide through text formatting, as the core content of the guide consists exclusively the frame of reference provided by ISO 27002:2017. Therefore, inspired by the information emerged through the ECHO-derived framework, the structure of the guide was kept simple and the author sought to use neutral language and easily understandable phrases. Also, few memory rules and abbreviations were created inside the text, which might help the reader remember the content read.

The Writing/Editing > Review circle in Figure 2 on page 18 produced results as being a continuous circle of development. The standard was processed piece by piece during writing, and the Cyber Security Risk Management guide was to be compiled in a logical order relative to the ISO 27002:2017. As the process advanced, two versions were reviewed by the company

representatives. Company representatives gave their counterpart to the versions during dialogical discussions used as a method in this thesis and offered valuable corporate perspective on building the guide and specifying the content. Based on the received comments and the discussions in the first review meeting, the author strived to adopt functional patterns for compiling guidelines and developing the content more appropriate.

The second review meeting covered the inspection of the first corrections and additions. In addition, the new guidelines produced were discussed, and the author received again comments and recommendations. The guide was again edited by applying the means learned from the first round and considering the new comments and recommendations. After two review rounds the raw version was critically examined as a whole; the relevance of the content of the sections and the ability to produce the required information were analysed, the overlaps and the necessity of repetition of certain guidelines were assessed in terms of risk management and the sections concerned, and the validity of the layout and spelling, as well as the correctness of the table of contents were all revised. Due to the dialogical discussions and reviews, the author and the output evolved throughout the process.

5 Conclusions and self-assessment

The implementation of the Cyber Security Risk Management guide described in this thesis alone is not enough to increase the capacity of employee cyber security expertise. Learning something new requires repetition, as well as remembering things already learned requires recapitulation. Thus, the course under design by the company, which employees must complete at regular intervals, is the optimal choice to support the internalization of the guide. Based on the review of the selected ECHO components and the results summarized in the previous Chapter 4, the development proposals are provided for the further design of the cyber security training course. In the light of the various training techniques discussed in this thesis, the author proposes including a game aspect in the implementation of the course. The argument of the conclusion is the features of gamified approach that have been shown to be effective way of learning.

However, complex simulations and strategic games require special expertise in design and practical implementation. They are also time consuming and financially more challenging to implement. The urge for competition is built-in and feeds the motivation to succeed, the competition perspective is somehow connected to every game. Therefore, the game aspect could be included in the cyber security training course in a form of slight competition. The course could be implemented in a way of being organized together and simultaneously for all employees, for example in connection with a meeting. Thus, employees would also not experience an individual compulsion to interrupt their own work assignments and overall

attitude towards the completion of the course might improve. Everyone would be on the same starting line and get the same amount of time to complete the course. Peer pressure could, in turn, promote concentration and increase the motivation of the respondent to cope. Completion of the course could be scored and the one earning the most points could redeem a small prize agreed by the work community.

When the course is repeated at intervals defined by the company and integrated into the recurring activities of the organization, the course situation may later become an internal matter of the company, which is perceived as a positive and unifying factor for the work community.

The author evaluates the overall implementation of the Cyber Security Risk Management guide as successful. The schedule was flexible on behalf of the client, allowing the leisurely assembly of the guide. The objectives of the organization for the end-use of the guide were comprehensively taken into account throughout the process. Regular reviews of the raw versions guided the progress and changes were made according to the management's wishes. The author managed in listening the client and realizing their vision. Although there was no strict timetable requirement, the author believes that by better self-scheduling the project implementation interval could have been shorter. Also, more detailed advance planning could have facilitated the compilation of the guide. In the end however, the author is satisfied with the execution of this thesis.

The theoretical part compiled based on ECHO framework is reproducible. The sampling of references is relatively diverse and comprehensive, therefore the literature review of the alike subject groups is likely to end up with the similar results. The repeatability of the thesis assignment, however, is unfortunately weak due to its individuality. Low repeatability is advocated by customization for the company and the use of company materials and their influence on defining the project content.

The results are relatively reliable. This argument is supported by the use of peer-reviewed material and documents published by Finnish government agencies. The correctness of the produced guide is advocated by the use of updated, latest version of the ISO 27002:2017 standard, and the approval received from the client.

References

Printed sources

ISO/IEC 27002:2017. Information technology. Security techniques. Code of practice for information security controls. Helsinki: Finnish Standards Association SFS; Geneva: International Organization for Standardization.

Vilkka, H. 2015. Tutki ja kehitä. Keuruu: Otavan kirjapaino.

Kohnke, A., Sigler, K. & Shoemaker, D. 2017. Implementing Cybersecurity. A Guide to the National Institute of Standards and Technology Risk Management Framework. Great Britain: Taylor and Francis Group.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Tampereen yliopistopaino – Juvenes Print.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Uudistettu 3. painos. Helsinki: Sanoma Pro.

Electronic sources

Adams, M. & Makramalla, M. 2015. Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review. Vol. 5, Iss. 1. Accessed 9.11.2019. https://search-proquest-com.nelli.laurea.fi/central/docview/1676102408/892EBA7E167F4FF1PQ/5?accountid=12003

Aldawood, H. & Skinner, G. 2019. Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues. Future Internet. Vol. 11, Iss. 3. Accessed 16.10.2019. https://search-proquest-com.nelli.laurea.fi/central/docview/2231534036/fulltextPDF/B8BD5B3170E24703PQ/1?accountid=12003

Chapman, S., Smith, R., Maglaras, L. & Janicke, H. 2017. Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training? Journal of Sensor and Actuator Networks. Vol. 6, Iss. 3. Accessed 16.10.2019. https://search-proquest-com.nelli.laurea.fi/central/docview/1952219072/468A336E559E459APQ/5?accountid=12003

Cook, A., Smith, R., Maglaras, L., Janicke, H. 2016. Measuring the Risk of Cyber Attack in Industrial Control Systems. BCS Learning & Development Ltd. Accessed 9.11.2019. https://pdfs.semanticscholar.org/eaed/881c3fc7be8cedd853e031d1d83cd29a07be.pdf

ECHO. 2019. European Union. Accessed 2.10.2019. https://echonetwork.eu/project-summary/

Ellis, R. & Mohan, V. 2019. Rewired – Cybersecurity Governance. Wiley. Laurea Lib Guide. Accessed 9.9.2019. https://ebookcentral.proquest.com/lib/laurea/reader.action?docID=5761058&query=cyber%2Bsecurity

Eriksson, P. & Koistinen, K. 2014. Monenlainen tapaustutkimus. Kuluttajatutkimuskeskuksen tutkimuksia ja selvityksiä. Accessed 8.10.2019. https://helda.helsinki.fi/bitstream/handle/10138/153032/Tutkimuksia%20ja%20selvityksiä_11_2014_%20Monenlainen%20tapaustutkimus_Eriksson_Koistinen.pdf?sequence=1&isAllowed=y

European Comission. 2019. European network of Cybersecurity centres and competence Hub for innovation and Operations. Accessed 20.11.2019. file:///C:/Users/Asus/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/CORDIS_project_830943_en%20(1).pdf

Furnell, S. & Vasileiou, I. 2019. Cybersecurity Education for Awareness and Compliance. IGI Global. Accessed 16.10.2019. file:///C:/Users/Asus/Documents/Harjoittelu%20ja%20ONT/Cybersecurity_Education_for_Awareness_and_Complian...%20(1).pdf

Grant, TJ. 2015. Specifying Functional Requirements for Simulating Professional Offensive Cyber Operations. Journal of Information Warfare. Vol. 14, Iss. 3. Accessed 6.10.2019. https://search-proquest-com.nelli.laurea.fi/central/docview/1967316780/fulltextPDF/754B229E61049D4PQ/15?accountid=12003

Holm, R., Poutanen, P. & Ståhle, P. 2018. Mikä tekee dialogin: Dialogisen vuorovaikutuksen tunnuspiirteet ja edellytykset. Sitra. Accessed 15.10.2019. https://www.sitra.fi/artikkelit/mika-tekee-dialogin-dialogisen-vuorovaikutuksen-tunnuspiirteet-ja-edellytykset/

Latvala, E. & Tuomi, S. 2020. Opinnäytetyön ohjaajan käsikirja. Jyväskylän ammattikorkeakoulu. Accessed 15.10.2019.
https://oppimateriaalit.jamk.fi/yamk-kasikirja/kirjallisuuskatsaukset/

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Accessed 6.9.2019.
http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila%2c__tavoitetila_ja.pdf?sequence=1&isAllowed=y

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Salonen, J., Savola, R., Savolainen, P., Suominen, A., Toivanen, H., Kyheröinen, J. & Remes, J. 2016. Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016. Accessed 20.1.2020.
http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79562/Kyberosaaminen%20Suomessa.pdf

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopisto. Accessed 15.10.2019.
https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Salonen, K. 2013. Näkökulmia tutkimukselliseen ja toiminnalliseen opinnäytetyöhön. Opas opiskelijoille, opettajille ja TKI henkilöstölle. Tampere: Suomen yliopistopaino – Juvenes Print. Accessed 15.10.2019.
http://julkaisut.turkuamk.fi/isbn9789522163738.pdf

The Finnish cyber security strategy. 2019. The security committee. Accessed 15.1.2020.
https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Topham, L., Kifayat, K., Younis, Y., Shi, Q., Askwith, B. 2016. Cyber security teaching and learning laboratories: A survey. Information and Security. Vol. 24, Iss. 1. Accessed 15.11.2019.
https://search-proquest-com.nelli.laurea.fi/central/docview/1928331945/fulltextPDF/386D2CBD9BF9497APQ/2?accountid=12003

Vocabulary of Cyber Security. 2018. The security committee. Accessed 7.9.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Unpublished sources

Cyber Security Risk Management guide 2020, 7.

Operations Manual 2019.

Risk Assessment Table 2019.

The Notes 5.9.2019.

Figures

Tables

Appendices

Appendix 1: The Cyber Security Management guide table of contents

Table of Contents