jamk.fi

Suitability of EQF-4 Level Education for Improving Cyber Labor Shortage in Finland

Janne Jaurimaa

Master's thesis
May 2021
School of Technology
Master's Degree Programme in Information Technology
Cyber Security

jamk.fi

Description

Author(s)	Type of publication	Date
Jaurimaa, Janne	Master's thesis	05 2021
		Language of publication: English
	Number of pages: 61	Permission for web publication: X

Title of publication

Suitability of EQF-4 Level Education for Improving Cyber Labor Shortage in Finland

Degree programme

Master´s Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Sampo Kotikoski; Jari Hautamäki

Assigned by

Karo Saharinen, JAMK, CyberSec4Europe-project

Abstract

Jyväskylä University of Applied Sciences (JAMK) is participating the Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project. One of the projects main technical objectives is to reform cybersecurity education models by developing a new framework for use by education providers as well as employers. The model aims to improve the suitability of the cyber security workforce graduating from education programs to the requirements of working life.

The main purpose of the study was to find out the current suitability of the Vocational Education in Information and Communications Technology for the Finnish cyber related industry. The study was conducted in two phases. Phase one started with the compare between Vocational qualification in Information and Communications Technology qualification titles and the work roles of the NCFW. In the second phase, a survey was conducted on the employer sector. A conference paper was formed from the results of the survey, it was published as part of European Conference on Cyber Warfare and Security (ECCWS), and it is incorporated in its entirety into this thesis.

Similarities were identified between the curriculum content and the framework work roles only at the rough heading level. The descriptions of the course contents have been made very broadly and their comparison with detailed descriptions of the work roles does not give an exact result. Based on the results of the survey, in EQF4-level, employers believe that the emphasis should be placed on basic technical skills and adherence to guidelines, while choosing more detailed specific areas of expertise is less important at this level of education. Based on the responses, in general cyber security related work has higher education level requirements than EQF4-level could provide.

Keywords/tags (subjects)

Education, cyber security, EQF, NCFW

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Jaurimaa, Janne	Opinnäytetyö, ylempi AMK	05 2021
		Julkaisun kieli Englanti
	Sivumäärä 61	Verkkojulkaisulupa myönnetty: x

Työn nimi

Suitability of EQF-4 Level Education for Improving Cyber Labor Shortage in Finland

Tutkinto-ohjelma

Master´s Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Sampo Kotikoski; Jari Hautamäki

Toimeksiantaja(t)

Karo Saharinen, JAMK, CyberSec4Europe-projekti

Tiivistelmä

Jyväskylän ammattikorkeakoulu (JAMK) osallistuu CyberSec4Europe-projektiin, jonka yhtenä teknisenä päätavoitteena on uudistaa kyberturvallisuuskoulutuksen mallit kehittämällä uusi viitekehys koulutuksen tarjoajien sekä työantajien käyttöön. Mallin avulla pyritään parantamaan koulutusohjelmista valmistuvan kyberturvallisuustyövoiman soveltuvuutta työelämän vaatimuksiin.

Tutkimuksen pääasiallisena tavoitteena oli selvittää, miten hyvin suomalainen toisen asteen ammatillinen ICT-koulutus vastaa työelämän tarpeita kyberturvallisuusalan näkökulmasta. Tutkimus toteutettiin kahdessa vaiheessa. Ensimmäisessä vaiheessa vertailtiin koulutusohjelman sisältöä NICE Cybersecurity Workforce Framework (NCWF) -viitekehyksen työrooleihin ja niistä pyrittiin tunnistamaan yhteneväisyyksiä. Toisessa vaiheessa kohdistettiin kyselytutkimus työnantajasektorille. Kyselytutkimuksen tuloksista muodostettiin erillinen julkaisu European Conference on Cyber Warfare and Security (ECCWS) -seminaariin ja se on liitetty kokonaisuudessaan osaksi tätä opinnäytetyötä.

Koulutusohjelmien sisällön ja viitekehyksen roolien väleiltä tunnistettiin yhteneväisyyksiä ainoastaan karkealla otsikkotasolla. Kurssien sisältöjen kuvaukset on tehty erittäin laveasti ja niiden vertailu roolien yksityiskohtaisempiin kuvauksiin ei anna tarkkaa lopputulosta. Kyselytutkimuksen tulosten perusteella työnantajat näkevät, että toisen asteen koulutuksen painotus pitäisi kohdistaa teknisiin perustaitoihin sekä työohjeistuksien noudattamiseen, kun taas yksityiskohtaisempiin erityisosaamisalueisiin painottuminen nähtiin vähemmän tärkeäksi. Tulosten perusteella kyberturvallisuuteen liittyvällä työllä on yleisesti korkeamman koulutustason vaatimukset kuin mitä toisen asteen koulutus tarjoaa.

Avainsanat (asiasanat)

Koulutus, kyberturvallisuus, EQF, NCFW

Muut tiedot

Contents

Figures

Tables

1 Introduction

1.1 The Finnish Cyber Security Strategy

The first version of Finnish Cyber Security Strategy was published on 24 January 2013 in the form of a government resolution. It specifies the main goals and operations models to respond to the challenges in the cyber domain and ensuring its functionality. The strategy includes descriptions of cybersecurity vision and strategic guidelines for reaching the desired end state of the vision. To reach the desired end state, the first implementation programme was adopted on 11 March 2014 by Security Committee, and it has regularly evaluated its realization since that. (Implementation Programme for Finland's Cyber Security Strategy for 2017–2020 2018, 4.) The vision is opened more specifically below in Figure 1.

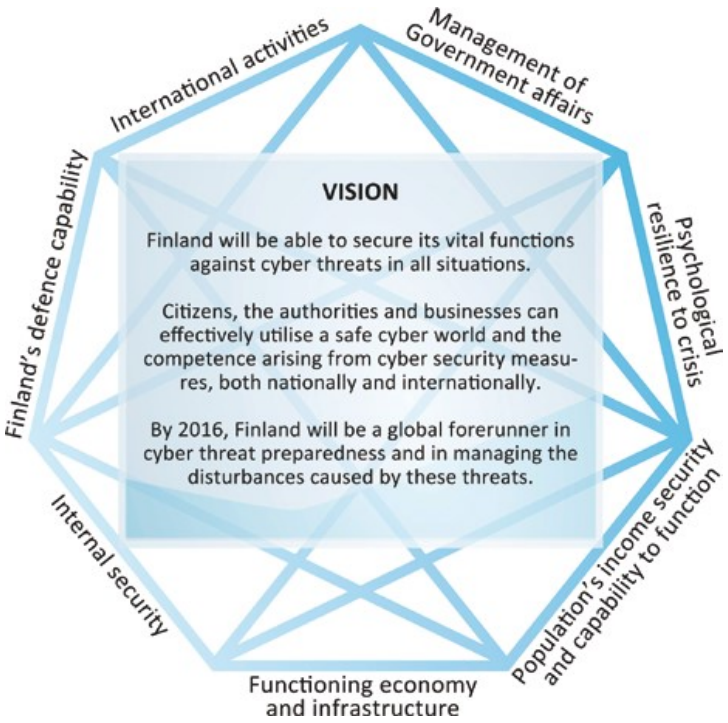


Figure 1. Vision for cyber security on 2013

Finland is described in the strategy as a small, capable and cooperative country which has great potential to rise as one of the leading countries in the field of the cyber security. Implementations of research, development and education on

different levels aimed at cyber security, strengthens national know-how and Finland as an information society. (Finland´s Cyber security Strategy 2013, 3-5.)

Because of the changes in the operating environment of the cyber domain, updated version of the Implementation programme was published on 10 April 2017. It's called Implementation Programme for Finland's Cyber Security Strategy for 2017–2020. The implementation program concerns the development of cyber security within the service complex covering public sector, business sector and the third sector, and where the customer is the individual citizen. (Implementation Programme for Finland's Cyber Security Strategy for 2017–2020 2018, 4.)

The constant change in operating environment drives again updates in the strategy and new version was published in 2019. Strategy launched the preparation work to the National Cyber Security Development Programme. It aims to enhance the cyber security situation picture and integrate planning with other functions. (Finland´s Cyber security Strategy 2019, 4.)

1.2 Cyber related education in Finland

The educational key points of the above-mentioned Finnish cyber security strategies related to this thesis are the following:

- *"The study of basic cyber security skills must be included at all levels of education. The learning requirements of cyber security must be included on the curricula of basic education (comprehensive school), vocational upper secondary education, general upper secondary education and higher education." (Finland's Cyber security Strategy 2013, 31.)*
- *"Training programmes related to cyber and information security, software and application development, information networks and telecommunications in vocational education, universities of applied sciences and universities will be strengthened." (Finland's Cyber security Strategy 2019, 9.)*

In comprehensive education level students should have sufficient skills to deal with the digital environment as well as they should understand and protect themselves from the basic cyber security related threats. In this level they should be given the

fundamentals of media literacy and a basic understanding of information operations. In upper secondary school these above-mentioned skills should be strengthened. (Lehto & Niemelä 2019, 25.)

Curriculum of the Finnish vocational qualification in information and communications technology introduced in August 2020 contains an optional module “Maintaining cyber security” and it’s possible to include in every qualification program in area of expertise. (Finnish National Agency for Education: OPH-2596-2019 2020.)

Cyber related education is widely available in Finnish universities of applied sciences and universities. In 2019 there were at least 10 universities and 9 universities of applied sciences where it was possible to complete cyber related studies. Cyber security related degree programs can be divided in two ways. The first way is majoring cyber security degree program which produces in-depth cyber security professionals to the field of cyber security. Another way is to include cyber security related studies in some other major subject degree program, and by that way increase general cyber security awareness in that area. (Niemelä 2019, 13-14.)

The effects of digitalisation are strongly visible in the direction of different educational institutions, the teaching of information technology is becoming an important part of almost all other fields. As the cyber security sector continues to spread, specialize and grow, at the same time, it poses a huge challenge to education which is still in the developmental stage. While education is taking its shape, research shows that labor adequacy is a problem in the industry. (Niemelä 2019, 47.)

1.3 Cyber workforce needs in Finland

A research published by Niemelä in 2019 states that there is a clear shortage of suitable labor in the cyber sector in Finland. Employers' expectations about the level of competence of applicants are not met. Employers expect education to produce more skilled professionals, but the lack of quantity is so significant, forcing employers to recruit students in the field even before graduation. The expected level of competence of the applicants has been lowered, and it is hoped that in the future, applicants will have basic knowledge of the cyber branch and deep expertise in one of the key areas of cyber. (Niemelä 2019, 47–48.)

The Digibarometer 2020 publication mentions a survey conducted by the Finnish Information Security Cluster (FISC). Based on the answers of that survey, 60% of respondents experienced a lack of skilled cybersecurity professionals or knowledge in their business area. In that publication, this shortage of skilled cybersecurity professionals is seen as the biggest challenge for the cyber security business growth in Finland. (Digibarometri 2020: Kyberturvan tilannekuva Suomessa 2020.)

Based on these starting points it can be said that there should be a significant demand at least for skilled labor in Finnish cyber field. From a global perspective, Cybersecurity Workforce Study published by the International Information System Security Certification Consortium (ISC)² was seen for the first time that the workforce gap was decreased from 4 million to 3.1 million in year 2020. (Cybersecurity Workforce Study, 2020; (ISC)². 2020.) The gap is still huge, but the direction is right, hopefully this will be the direction in the future as well.

2 Research methodology

2.1 Research Objective

The purpose of this research was to find out the current suitability of Finnish cyber security education for different critical infrastructure industry in Finland.

The main research question:

- Is EQF-4 level education suitable for improving cyber labor shortage in Finland?

Following sub questions were derived from the main question of the research:

- Is there equivalencies between NICE Cyber Security Workforce Framework (NCFW) work roles and Vocational qualification in Information and Communications Technology qualification titles?
- Will those identified roles with the secondary degree level of experience match to the demands of employers in Finland?
- What kind of cyber related employees do employers currently need in Finland, level of education, level of experience, direction of competence?

Two phases are taken to find out the answers to these questions. Phase one starts with a comparison between Vocational qualification in Information and Communications Technology qualification titles and the work roles of the NCFW. The

second step of this phase is to perform a comparison between the Knowledge, Skills, Abilities (KSA's) and tasks of the selected work role and skill requirements of the degree modules.

In the second phase, employers are surveyed to determine the need for identified roles from their point of view. Survey responses also clarify their opinions on what kind of education they think would benefit their business, as well as what kind of professionals are currently in demand in their business area.

2.2 Earlier research

Secondary level cyber project for the Jyväskylä Educational Consortium, 2016. Jarmo Nevala and Jouni Aho assessed teachers 'perceptions in cyber security and cyber training needs in small businesses at the Central Finland area.

Nils Willberg, Current and future needs of the cyber expertise in public sector organizations, University of Jyväskylä, 2017. Willberg uses NCFW-framework in gategory and speciality area levels when assessing the needs of cyberprofessional expertise in two public sector organizations.

Jukka Niemelä, Demand, availability and development of the cyber security workforce respond to the need for labor in Finland, University of Jyväskylä, 2019. Publication examines the availability of cyber work in Finland, from the recruiting organizations point of view. In the study, the profile of a cyber professional employee is formed from the requirements collected from employers. Cyber education in Finland is also evaluated, concentrating mainly in the universities and the universities of applied sciences. This study has also been used as one source in the publication of Martti Lehto and Jukka Niemelä, Kyberalan tutkimus ja koulutus Suomessa, University of Jyväskylä, 2019. Publication describes cyber security research and education in the universities and the universities of applied sciences in Finland.

A Design Model for a Degree Programme in Cyber Security, Saharinen, Karo; Karjalainen, Mika; Kokkonen, Tero 2019. Article describes a design model of a cyber security degree programme, it's aimed to engineering education in information technology on university level.

Jaakko Backlund, Examination of contempory cyber security education, JAMK Univesity of Applied Sciences, 2020. The research focuses on how cyber security degree programmes meet the demands of stakeholders, and to determine the role of the cyber security area in degree curriculums. The NCWF-framework is utilized by matching the courses in curriculums to main categories of the framework. The research focused on the university level in the EU and the United States.

As seen in the above, cyber education, frameworks comparison and labor availability have been earlier researched, but they have not previously been aimed to Finnish vocational qualification curriculums or “apply” level workforce needs on which this study focuses.

2.3 Research methods

In the first phase of the research a comparison is performed between the curriculum of the Finnish Vocational qualification in Information and Communications Technology and NCWF work roles. This phase is implemented with a descriptive comparison method. In this case both definitions recognize quite similar competences to the candidate, but the requirements have been created by different organizations in different countries (Rautio 2007). The primary goal is to find similarities from the subjects. This data is gathered from the existing curriculums and framework.

The second phase of the research is carried out with quantitative methods. Quantitative research is a method which gives an overview of the relations and differences between the subjects to be measured. It answers for example the questions how much or how often. Structuring means that the subject under study and its properties are designed and standardized. In structuring, the issues to be examined are standardized on the form into questions and alternatives in advance so that everyone understands the question in the same way and questions can be asked from all respondents in the same way. (Vilkka 2007, 13-15.) The data is collected from a structured survey which is addressed to the Finnish employers of the critical infrastructure.

From the ethical point of view, NCWF-framework and the vocational curriculums have been used to obtain the data, they both are available for free from open public sources. These sources are well known, published releases can be found from official web pages, and they are available to everybody without any registration. Answering the questionnaire survey has been voluntary. Data from the questionnaire survey is collected, stored and analyzed in such a way that it remains anonymous. Any kind of identification information is not gathered so regulations of personnel data handling are fulfilled. (Kuula 2015.)

3 Theoretical Basis

3.1 Cybersecurity Workforce Framework

National Intitute of Standards and Technology (NIST) has been executor of National Initiative for Cybersecurity Education (NICE) with cooperation between the United States industry, government and academia. At the strategy definition phase, NICE was given the target audience goals presented in the Figure 2. (National Initiative for Cybersecurity Education: Strategic Plan 2016.)

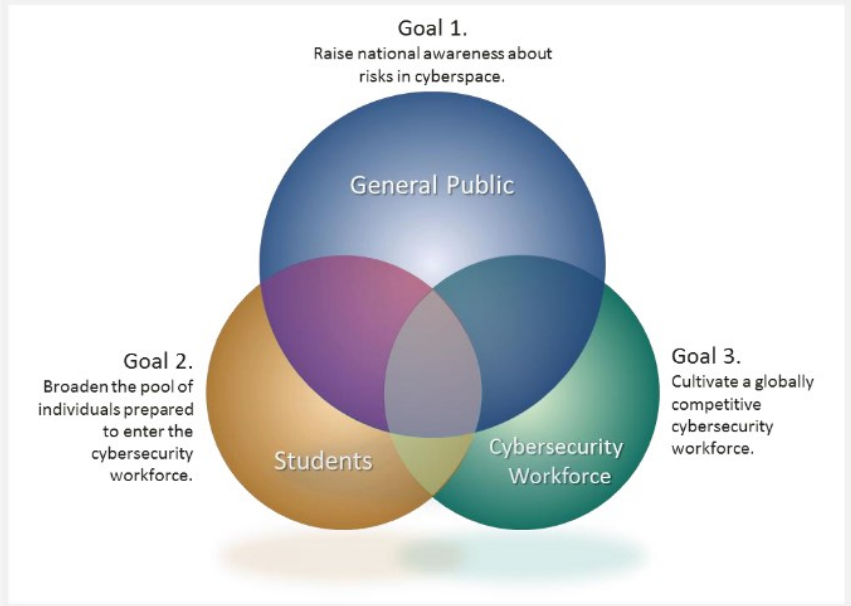


Figure 2. NICE goals

Since 2010 NICE has developed working document draft of the NICE Cybersecurity Workforce Framework (NCWF), and in August 2017 it was published as a NIST Special Publication 800-181. NCWF is created to categorize and describe cyber security related work roles and tasks. It is designed to serve support to many different parties including employers, employees, students, educators and technology providers. Framework is providing a common lexicon as well as taxonomy for the cyber security organizations and the workforce regardless of where or for whom the work is done. (The National Cybersecurity Workforce Framework 2017.)

At the highest level of the framework, cyber security work is divided into seven categories, which are more specifically opened in Figure 3 below.

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Figure 3. NCWF Categories

This thesis concentrates on particular Securely Provision and Operate and Maintain categories. These can be considered as the most appropriate benchmarks with EQF4 level functions.

Inside the categories there are 33 separated areas of cyber security work, which are called Specialty areas. Each of them illustrates concentrated work, or function in cyber security. The specialty areas contain 52 groupings called work roles. The work roles consist of a set of specific knowledge, skills and abilities (KSA) that are required to accomplish different tasks. The whole model is visualized in the Figure 4. (The National Cybersecurity Workforce Framework 2017.)

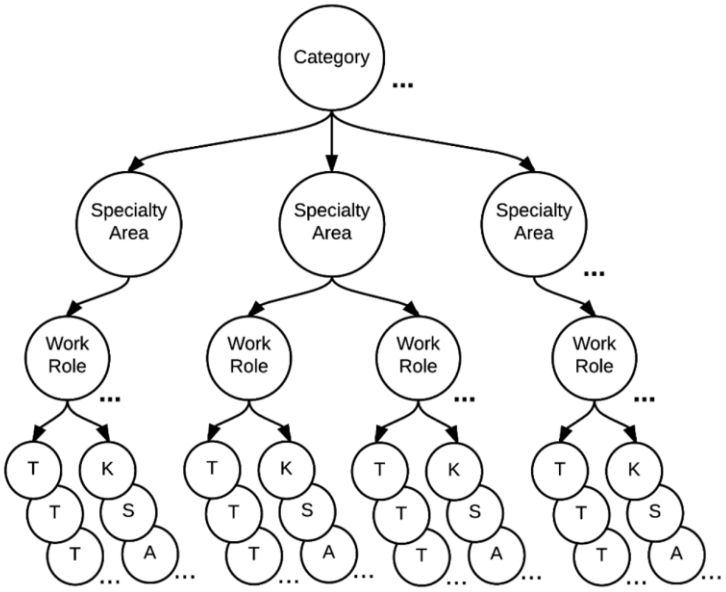


Figure 4. NCWF model

In November 2020 NIST has published Revision 1 version of the NICE Framework. In this version structures are organized in a new way to simplify Categories and Specialty Areas. This should provide a simpler approach for user organizations. Model offers more straightforward way to present agility, flexibility, interoperability, and modularity than the earlier one. Revision 1 describes terms “the work” and “the learner” in generic way that can be applied for the use of every organization. Revision 1 is not used in this thesis due to its late publication. (The National Cybersecurity Workforce Framework Revision 1 2020.)

It must be remembered that the NCWF is not a solution model which is set in stone; it’s a good guidance collection to describe different cyber security work, compiled by one governmental organization in United States. However, it offers opportunity to compare the results of this study with the future studies, by providing a common, well-known and widely used benchmark.

3.2 Finnish Vocational Qualification in Information and Communications Technology

Finnish vocational qualification is on level 4 at European Qualifications Framework (EQF). EQF is an 8-level framework which is designed to facilitate the comparison of national qualifications. More detailed descriptor of the EQF4-level of requirements is seen in Figure 5 below. (Finnish National Agency for Education.)

Level ***4***	***European Qualifications Framework*** *Descriptors*
• General upper secondary education certificate / syllabus • Matriculation examination • Vocational upper secondary qualifications • Further vocational qualifications • Basic Examination in Prison Services • Fire Fighter Qualification • Emergency Response Centre Operator Qualification	Factual and theoretical knowledge in broad contexts within a field of work or study A range of cognitive and practical skills required to generate solutions to specific problems in a field of work or study Exercise self-management within the guidelines of work or study contexts that are usually predictable, but are subject to change; supervise the routine work of others, taking some responsibility for the evaluation and improvement of work or study activities

Figure 5. EQF4 Descriptors

A person who has completed the Vocational Qualification in Information and Communications Technology has the required expertise and knows how to work collaboratively in ICT related tasks and is able to communicate with ICT branch glossary and knows how to work in the customer field. The person must also be able to ensure that the result meets the requirements of the work performance. (Finnish National Agency for Education: OPH-2596-2019 2020.)

The updated curriculum of Finnish Vocational qualification in Information and Communications Technology was introduced during August 2020, it consists 180 competence points. The qualification is divided into vocational units (145 competence points) and common units (35 competence points). Vocational units are again divided in compulsory units (70-115 competence points) and optional units (30-75 competence points). The vocational qualification produces five different

qualification titles, more detailed descriptions of titles are seen in Figure 6 below.

(Finnish National Agency for Education: OPH-2596-2019 2020.)

Range of occupations accessible to the holder of the certificate
Electronics Assemblers can perform installation, testing and servicing tasks related to electronic installations. They know how to handle the components and materials required in electronic installations and use the required tools and measuring devices.
Welfare technology installers are able to work according to the operating principles and values of the social and healthcare sector. They know how to install safety device systems and wellbeing technology systems and how to use wellbeing technology to maintain the customer's functional capacity. They guide the customer in the use of wellbeing technology and ensure that the equipment can be used safely.
Network installers are able to install the cabling for data networks according to the customer's requirements and instructions. They pay attention to the structures of the data networks and the materials used and carry out the measurements and tests required to ensure the operation of the system.
IT support specialists are able to work in an information and communications technology environment consisting of workstations, network devices and accessories and areas of operation. They work as part of information management and help users in different technical problems in the customer's premises or through a remote connection.
Software developers are able to carry out programming, utilise interfaces, handle data and use version management. When working as members of a software development team, they communicate with the customer, plan the implementation of the software and ensure the quality of the implemented functionalities.
The structure and content of the vocational qualification in information and communications technology has been designed so that qualification holders who have completed the unit Operating in the field of electrical engineering and automation technology have a training that has been determined applicable for limited Electrical qualification 3.

Figure 6. Qualification titles

From the qualification titles, electronics assembler and welfare technology installer are marked out of this research. This research focuses on Network Installer, IT Support Specialist and Software Developer programs. They will be compared to NCWF work role attributes. The curriculums used in this study have been compiled according to the Table 1.

Table 1. Curriculums, unit level

		IT Support Specialist	Network Installer	Software Developer
Common units		35	35	35
Compulsory	Basic tasks of information and communication technology	25	25	25
	Operating in technical support service	45		
	Operating in system support	45		
	Network cabling		45	
	Installation of network equipment		45	
	Programming			45
	Operating as a software developer			45
Optional	Maintaining cyber security	30	30	30
Total		180	180	180

In the Publication of the Ministry of Economic Affairs and Employment: Growth from digital security, Roadmap for 2019–2030, Lauri Kämppi describes Finnish education levels with the Bloom's taxonomy, levels of competence combined with the competence produced by educational institutions. In that publication, vocational qualification is combined with Bloom's taxonomy apply-level.

Anderson & Krathwohl described Bloom's revised taxonomy Apply-level with sentence: "*carry out or use a procedure in a given situation*". They also divide apply-level in two entireties, executing and implementing. (Anderson & Krathwohl 2001, 67.) Both taxonomy entireties fit well together with earlier presented EQF4-level descriptors.

4 Research implementation

4.1 Comparing curriculum contents to the framework

Comparison was performed between with the selected curriculums of the Finnish Vocational qualification in Information and Communications Technology and the NCWF work roles. Based on the competence classifications of the previous chapter, the first goal was to select framework categories that include apply level work roles which are compatible with their content to vocational qualification titles. The second goal was to identify suitable role –title pairs.

4.1.1 Defining the scope of the Categories and qualification titles

Securely Provision category description includes "*procures, and/or builds secure information technology (IT) systems"*, build is suitable action for apply level. Operate and Maintain gategory is as the name implies support and administration based, also suitable for apply level.

Oversee and Govern category includes leadership and management, those are more at least EQF6-level matters. Work roles in Protect and Defend, Analyze, Collect and operate and Investigate gategories contains more specific competence requirements from the cyber field than apply level covers, they are more in analyze or evaluate levels.

For the Software developer qualification title, the same named and similar work role was found from securely provision category. From the operate and maintain category found two suitable work role - qualification tile pairs, Network operations specialist-Networks installers and Technical support specialist-IT support specialist.

4.1.2 Comparing qualifications titles to roles

Comparison was made by searching for corresponding entries between work roles KSA's against curriculum contents. The findings are described at three levels, mentioned, partially mentioned, not mentioned. Baseline was work roles list of KSA's and tasks, whose requirements were sought from the curriculum descriptions. At the beginning of the comparison the content of the curriculums were not available in English, so they have been freely translated for comparison by the writer. Entirety of comparison is in the appendix 1.

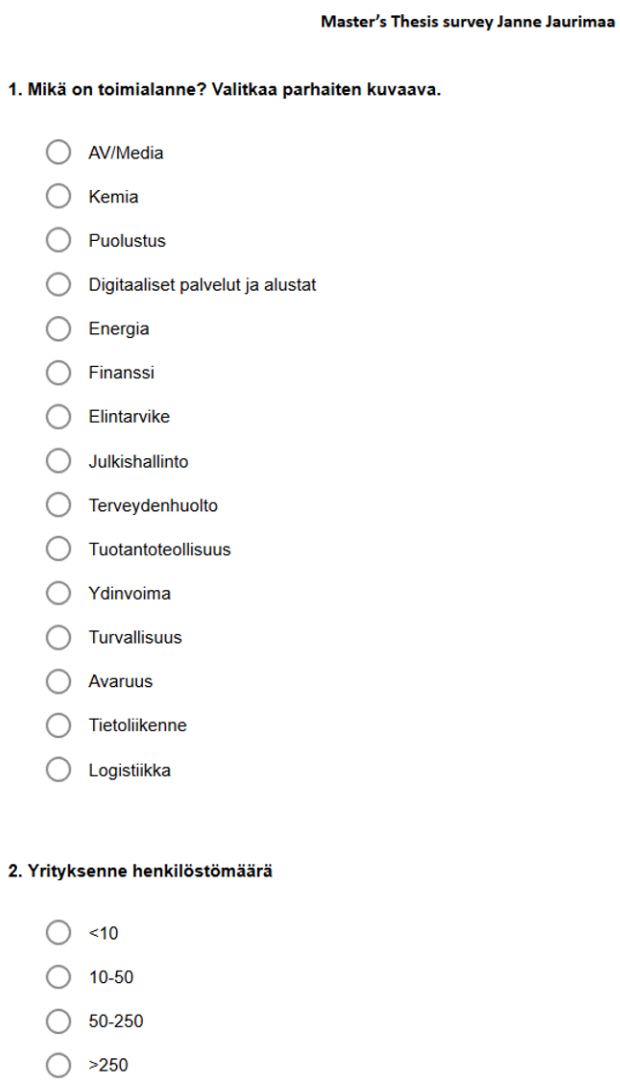
4.2 Survey research

The purpose of the survey is to find out the current suitability of Finnish cyber security education for different industries. The main focus of the survey is on Finnish vocational qualification in information and communications technology and more specifically on the work roles of the framework, identified in the previous paragraph. In addition, the importance of the level of education and work experience is inquired in cyber related recruitment of jobs and the near future labor needs of the cyber sector in Finland. The survey was aimed at the organizations operating in Finland, according to sectorial division of the Proposal for a European Cybersecurity Taxonomy. (Joint Research Centre (JRC), the European Commission's science and knowledge service; A Proposal for a European Cybersecurity Taxonomy 2019.) The personnel size classification of companies is derived from an EU publication: The new SME definition. (Publications Office of the EU; The new SME definition 2005.) These commonly used classifications were used in the study to allow comparison with potential future studies on the same topic.

The survey link was anonymous and it was same for the all participants. Link was distributed to the sectoral scoped organizations through the author's own contacts and JAMK's cooperation channels. The software used to collect and analyze the

responses was Webropol survey tool. The questions in the survey are mainly implemented using structured model to gather quantitative data.

The questionnaire survey consisted of 12 questions, it is structured as follows. At the beginning, questions one and two are for collecting background information of respondents, visual model of the questions is seen in Figure 7 below.



Master's Thesis survey Janne Jaurimaa

1. Mikä on toimialanne? Valitkaa parhaiten kuvaava.

- ○ AV/Media
- ○ Kemia
- ○ Puolustus
- ○ Digitaaliset palvelut ja alustat
- ○ Energia
- ○ Finanssi
- ○ Elintarvike
- ○ Julkishallinto
- ○ Terveydenhuolto
- ○ Tuotantoteollisuus
- ○ Ydinvoima
- ○ Turvallisuus
- ○ Avaruus
- ○ Tietoliikenne
- ○ Logistiikka

2. Yrityksenne henkilöstömäärä

- ○ <10
- ○ 10-50
- ○ 50-250
- ○ >250

Figure 7. Survey questions 1 & 2

Third question clarifies the significance of the measures of the Finnish cyber security strategy from the perspective of respondent organizations. Questions four and five are the most important topics from the study point of view, and they focus on cyber related modules in EQF 4 and 6 level curriculums. Questions from six to nine are for

gathering information about the needs of selected work roles, the needs of competence and experience, and target educational levels of recruitment. Question ten focuses on success of recruitments in cyber related recruitment, it was possible to supplement a possible no-answer with free text as seen in Figure 8 below. The near future workforce needs per NCWF category is clarified in question eleven. Lastly respondents were asked to describe development trends of Finnish cyber security education from their business perspective, this one was as a free text field, but its responses were categorized under similar topics in the results. A complete questionnaire is introduced in the appendix 2.

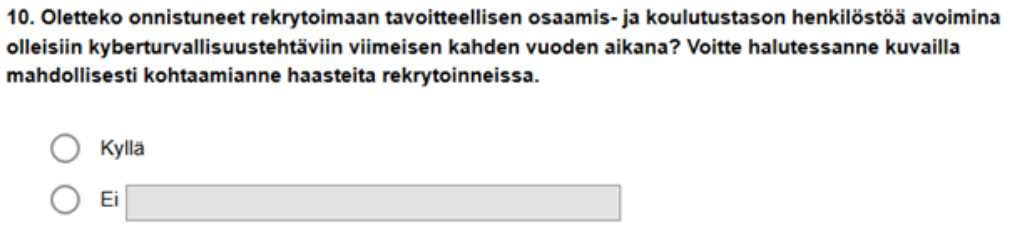


Figure 8. Survey question 10

5 Results

5.1 Results of Comparison

At the beginning of the comparison, it was first intended to pick up keywords from the KSA and task areas of the framework and target them to the curriculums. After getting to know the curriculums in more detail, this was a forgettable and changeable approach to manual comparison. The content of the curriculum has been described as so extensive that the comparison by keywords would have been very weak.

5.1.1 Network Operations Specialist and Network installers

Network Operations Specialist work role consists of 39 Knowledge attributes, 11 skill attributes, 8 abillity attributes and task 11 attributes. Spesific curriculum equivalences are seen in Figure 9 below.

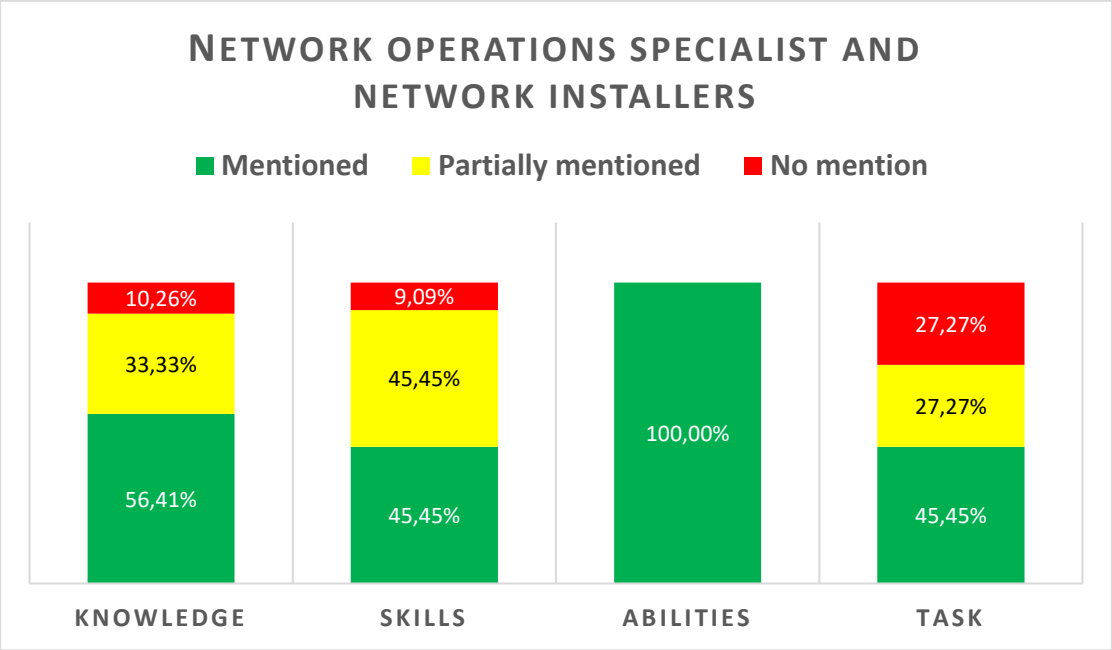


Figure 9. Comparison 1

The network operations specialist work role is purely to design and operate network services, while the qualification has a strong emphasis on physical network construction. In the work role, different protocols and network functionalities are highlighted when the curriculum deals with the title level, which may possibly contain certain content about those.

In the Knowledge section, one could say that all the networking skills could be put under these two curriculum sections: *knows the structure and protocols of a data network (1377)* and *understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)*. However, an attempt has been made in the comparison to break down directly relevant points from side hits, with percents 56.41% and 33.33%. Same pattern rises up in Skills section, under *configures the active device to be secure and ready for use (1372)* section could target quite a lot of doing. On the other point of view yellow could be green and vice versa, an exact opinion is difficult to form. Abilities section contains lots of basic network tools and they can be found in the curriculum sections painlessly. With a more detailed understanding of the content of the curriculum, all partially mentioned sections could be in the Yes side, in Task's section.

5.1.2 Technical Support Specialist and IT support specialists

Technical Support Specialist work role consists of 25 Knowledge attributes, 5 skill attributes, 3 abillity attributes and 12 task attributes. Spesific curriculum equivalences are seen in Figure 10 below.

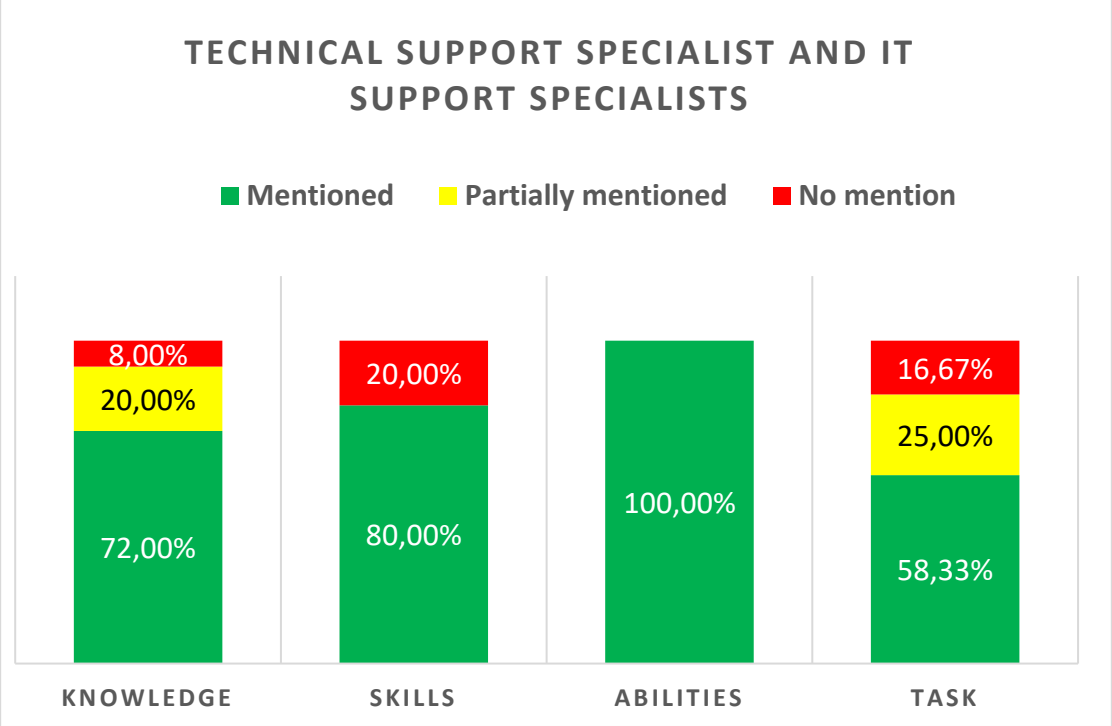


Figure 10. Comparison 2

In the Technical Support Specialist work role description, the clear emphasis is on the operational processes, while the qualification emphasis more in concrete doing and acting in the interactive technical support tasks. Here again, the descriptions of the qualification are very broad, and they are much more specific in the roles of the framework.

Knowledge sections came quite accurately filled, with the exception of a couple of more detailed wordings. The same pattern continued in Skills section, only one cloud based requirement was left out. Abilities match perfectly, and even Tasks with almost 60% accuracy.

5.1.3 Software developers qualification and Software developer role

Software developer work role consists of 44 Knowledge attributes, 13 skill attributes 5 abillity attributes and 25 task attributes. Spesific curriculum equivalences are seen in Figure 11 below.

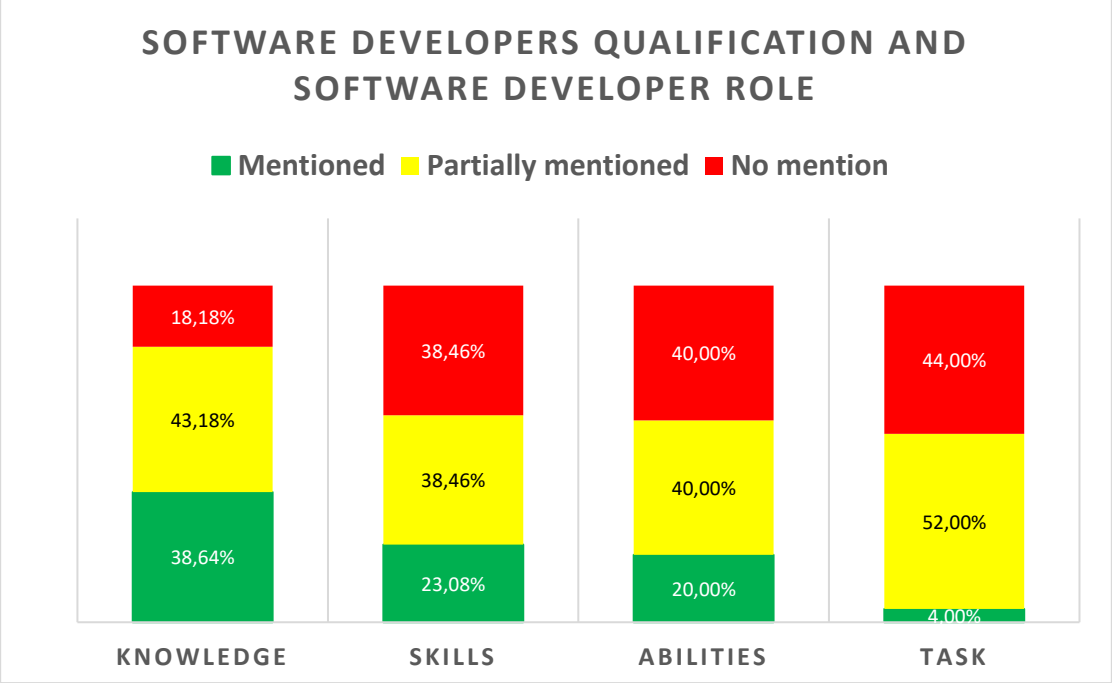


Figure 11. Comparison 3

In the Software Developers work role description, the emphasis is obviously on the technical skills of the individual and in the qualification there is a very strong emphasis placed on team work as well as communication with the customer. The work role goes often deeply to the specific coding skills, while the qualification uses an upper level of doing in its descriptions, this became the most obvious in task comparison. The comparison of the whole role-title pair is challenging precisely because of this.

Extensive descriptions are well seen in Knowledge section, “is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)” module hits 8/17 Yes-answers of the section. In Skills section accuracy of definitions continues, evaluates, interprets plans, and writes maintainable program code are quite big areas when they are currently being

compared to creating some well-defined part of coding process or exact code language. Abilities and Tasks areas are almost “Partly “or “No mention” due to difficult interpretation, accurate identifications between these are very difficult to make.

5.2 Survey research

The questionnaire survey was active 10.6.2020 - 26.7.2020 and it received a total of 50 responses. The responses came mainly from telecom operators, ICT service providers, defense sector and other governmental actors. Two respondents reported challenges in the survey publishing system and a few questions remained unanswered. The largest group of respondents were the large enterprises, which employ more than 250 employees. The survey was conducted mainly in Finnish, the results are presented in English.

The primary conclusions of the questionnaire survey will be published in European Conference on Cyber Warfare and Security 2021 (ECCWS), with the conference paper *Critical infrastructure protection - Employer expectations for cyber security education in Finland*. The conference proceedings have an ISSN (2049-9870) and will be assigned an ISBN on publication. The final version of this publication with the detailed analyzes of the survey research results can be found in the next section below in publication format.

5.2.1 The conference paper

Author’s contributions were as follows: K. Saharinen conceived the original idea. J. Jaurimaa designed and implemented the questionnaire survey, analyzed the results and wrote the paper in consultation with K. Saharinen who provided feedback and helped shape the research and the paper. All authors reviewed the final paper.

Critical infrastructure protection - Employer expectations for cyber security education in Finland

Janne Jaurimaa, Karo Saharinen, Sampo Kotikoski
JAMK University of Applied Sciences, Jyväskylä, Finland
m1270@student.jamk.fi
karo.saharinen@jamk.fi
sampo.kotikoski@jamk.fi

Abstract: In the human factor of cyber security, high level technical experts are considered as multidisciplinary technical gurus who are familiar with every aspect of IT environments including operating systems, code languages and protocols. University curricula and guiding frameworks, such e.g. NICE Cyber Security Workforce Framework, are designed to produce professionals to match the endless needs of working life. The cornerstones of achieving good working results can be considered as the level of expertise competence of the employee performing the task, as well as combining personal skills and abilities with the competence profile of the given task. Does the cyber domain need slightly lower educated, vocational level employees? As part of the National Security Policy in Finland, the vocational qualification in information and communications technology has recently started to produce suitable workforce for cyber labor on the European Qualifications Framework level 4 (EQF-4).

In this research paper we answer the question how well the vocational education meets the demands of the employers as suitable workforce in cyber security in Finland. The study also investigated what kind of cyber security employees the Finnish employers currently need; what is the required level of education, level of experience and direction of competence. The research data was collected through a structured questionnaire survey, which was directed to critical national infrastructure protection companies such as Finnish telecom operators, ICT service providers, defense sector, and other governmental actors. The questionnaire results were examined with quantitative methods.

Based on our results, regarding the content of education at EQF4-level, employers believe that the emphasis should be placed on basic technical skills and adherence to guidelines, while choosing more detailed specific areas of expertise is less important at this level of education. Based on the responses, in general cyber security related work has higher education level requirements than EQF4-level could provide. The results of the study can be used as guidelines for the development of the future curricula and in the strategic leadership of companies employing cyber security professionals.

Keywords: Human factor, Security Policy, Critical infrastructure protection, Strategic leadership

1. Introduction

Finnish Cyber Security Strategy was published on 24 January 2013 in the form of a government resolution (The Security Committee of Finland, 2013). It specifies the main goals and operation models to meet the challenges in the cyber domain and ensure its functionality. In this first version, strategy is mentioned: *"The study of basic cyber security skills must be included at all levels of education"* and in the update it is stated that all cyber and information and communications technology (ICT) related training programs, including vocational level, will be strengthened (The Security Committee of Finland, 2019).

The EQF is an eight level framework which is designed to facilitate the comparison of national qualifications between EU countries (European Union, 2017). Finnish vocational qualification has been placed in level 4 of the EQF. The updated curriculum of Finnish Vocational Qualification in Information and Communications Technology introduced in August 2020 consists 180 competence points (Finnish National Agency for Education, 2020). The vocational qualification program graduates' students with five different qualification titles. In all of them, the module related to maintaining cyber security can be selected as an optional module.

The National Institute of Standards and Technology (NIST) has been the executor of National Initiative for Cybersecurity Education (NICE) in cooperation with the industry, government, and academia in the United States. Since its establishment in 2010, NICE has developed a working document draft of the NICE

Cybersecurity Workforce Framework (NCWF), and in August 2017 it was published as NIST Special Publication 800-181 (NICE, 2017). The Framework is created to categorize and describe cyber security related work roles and tasks. It is designed to support many different parties including employers, employees, students, educators and technology providers. The framework provides a common lexicon as well as a taxonomy for the cyber security organizations and the workforce regardless of where or for whom the work is done.

At the highest level of the framework, cyber security work is then divided into seven categories. Inside the categories, there are 33 separate areas of cyber security work are called specialty areas. Each of them illustrates concentrated work or function in cyber security. The specialty areas contain 52 groupings called work roles, which consist of a set of specific knowledge, skills, and abilities (KSA) required to accomplish different tasks.

To create easier comparability for future researchers globally, in this research, the Finnish vocational qualification titles are converted to match the nearest corresponding NCFW work roles. For the Software Developer qualification title, a work role with the same name and similar work role was found in Securely Provision category. In the Operate and Maintain category two suitable work roles were found: qualification title pairs Network Operations Specialist-Networks Installers and Technical Support Specialist-IT Support Specialist. The mapping used in this research between the NICE framework and the Finnish vocational education can be illustrated in Figure 1.

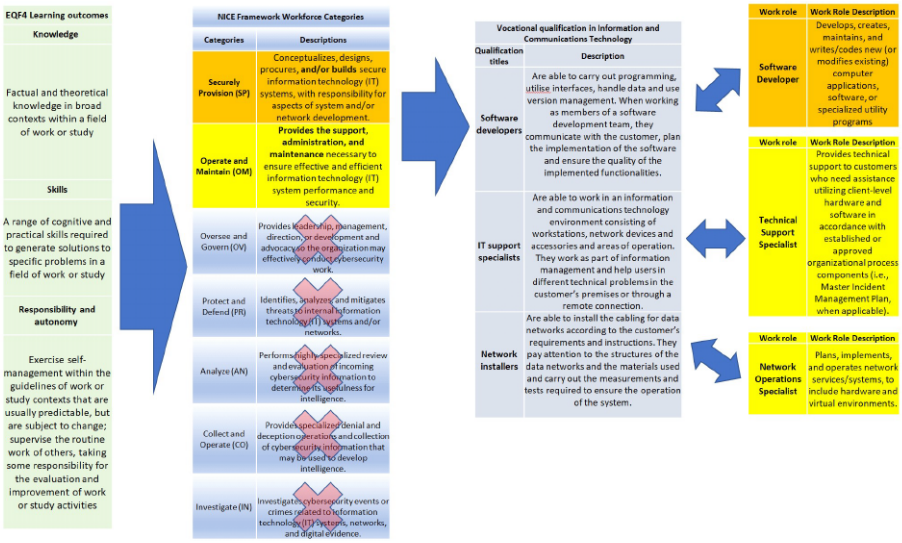


Figure 1: NCFW work roles and vocational qualification titles

2. Earlier research

The NICE framework has been used to develop degree programme structurization through *A Design Model for a Degree Programme in Cyber Security* to provide better targeted work role education for students on the Master's and Bachelor's Degree (Saharinen K., Karjalainen M., Kokkonen T., 2019). The emphases of different quantitative specialty areas have been researched regarding degree programme structuration (Backlund, J., 2020). The NCWF framework was utilized by matching the courses in curricula with the main categories of the framework. The research focused on the university level in the EU and the United States. The research contains a section on how the stakeholder demands between the industry and university education match one another.

Further influence was found in Jyväskylä Educational Consortium researched on the need for cyber security education in 2016 concentrating on Central Finland's SMEs. Simultaneously, also the teachers' perceptions of

cyber security and cyber training were researched (Nevala, J., 2018). Similarly, the *Current and future needs of the cyber expertise in public sector organizations* publication researched two public sector organizations and their needs for cyber professional expertise through NCFW framework (Willberg, N., 2017).

Demand, availability and development of the cyber security workforce respond to the need for labor in Finland examined the availability of cyber work in Finland from the recruiting organizations' point of view (Niemelä, J., 2019). In the study, the profile of a cyber professional employee is formed according to the requirements collected from employers. Cyber education in Finland is also evaluated focusing mainly on the universities and the universities of applied sciences.

As seen in the aforementioned paragraphs, there has been previous research on comparison of cyber education and frameworks with labor availability; however, the focus has not been on Finnish vocational education curricula or "apply" level workforce needs. This paper focuses its research on these sections, answering the question: Is vocational level cyber security education necessary as mandated in the Finnish Cyber Security Strategy?

3. Survey research from critical infrastructure the industry

The purpose of this survey was to find out the current suitability of Finnish cyber security education for different critical infrastructure industry in Finland. The main focus of the survey was on the Finnish Vocational Education (or qualification) in Information and Communications Technology. The survey also inquired and measured the importance of the education level and the amount of work experience required from the employer perspective in cyber related recruitment of jobs. Additionally, the labor needs for the cyber sector in Finland concerning near future were inquired about. As mentioned earlier, this research focuses on Network Installer, IT Support Specialist and Software Developer degree programmes and how necessary they are deemed.

The survey aimed at the organizations operating in Finland, which were classified according to sectorial division of the Proposal for a European Cybersecurity Taxonomy (JRC, 2019). The personnel size classification of companies is derived from an EU publication: The new SME definition (Publications Office of the EU, 2005). These commonly used classifications were used in the research to allow comparison with potential future research on the same kind of topic. The survey was conducted anonymously. The questions in the survey were implemented using a structured model to gather quantitative data. The questionnaire survey was active between 10 June 2020 - 26 July 2020 and it received a total of 50 responses. The responses came mainly from telecom operators, ICT service providers, defense sector and other governmental actors. The largest group of respondents were the large enterprises, which employ more than 250 employees. A sufficient number of Finnish actors in the field of critical infrastructure protection was involved. Figure 2 demonstrates the quantitative division of the respondents.

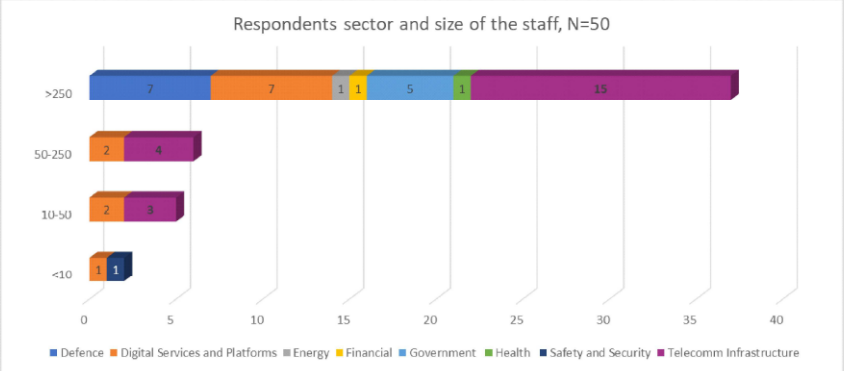


Figure 2: Respondents' sector and size of the staff

4. Results

The respondents were asked to classify the qualification requirements of the cyber security maintenance related module of the curriculum of vocational qualification in Information and Communications Technology (ICT), according to importance of their business.

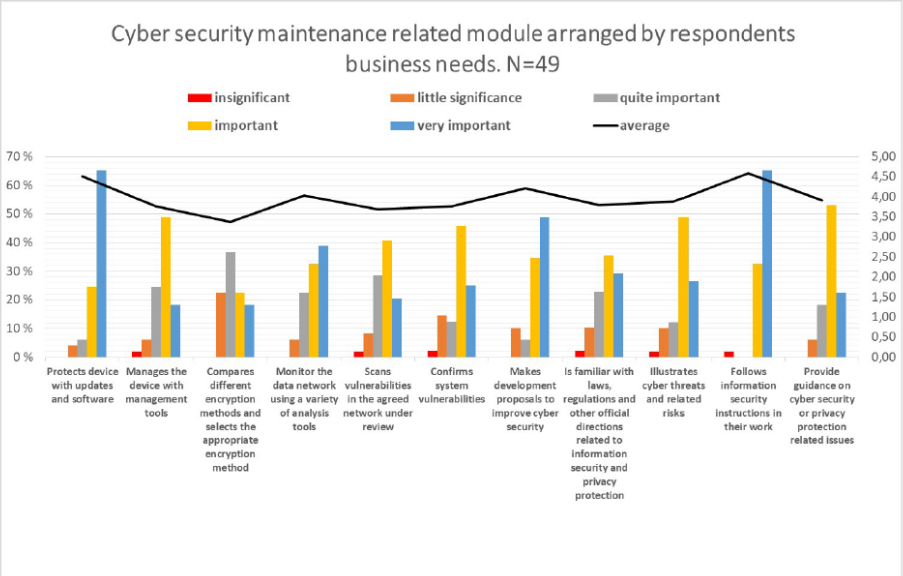


Figure 3: EQF4 Cyber security maintenance related module

On a scale of 1-5, the mean of the responses was 3.96. Two modules even exceeded the 4.5 average, *Follows the information security instructions in their work* was considered the most important topic with 4.59 result, and the second most important topic was *Protects device with updates and software* with 4.51. More than four averages were also reached by topics *Makes development proposals to improve cyber security* 4.22 and *Monitor the data network using a variety of analysis tools* 4.04. Based on the responses, *Compares different encryption methods and selects the appropriate encryption method* 3.37 and *Scans vulnerabilities in the agreed network under review* 3.69 were considered as less important sections. In summary, citing the results it can be stated that respondent organizations highly appreciate that at this level of education daily basic cyber security functions are carried out in accordance with the instructions.

The respondents were asked to classify the relevance of the cyber security modules in JAMK University of Applied Sciences' Information and Communication Technology degree program according to their importance to their business. The following Figure 4 demonstrates this distribution of answers.

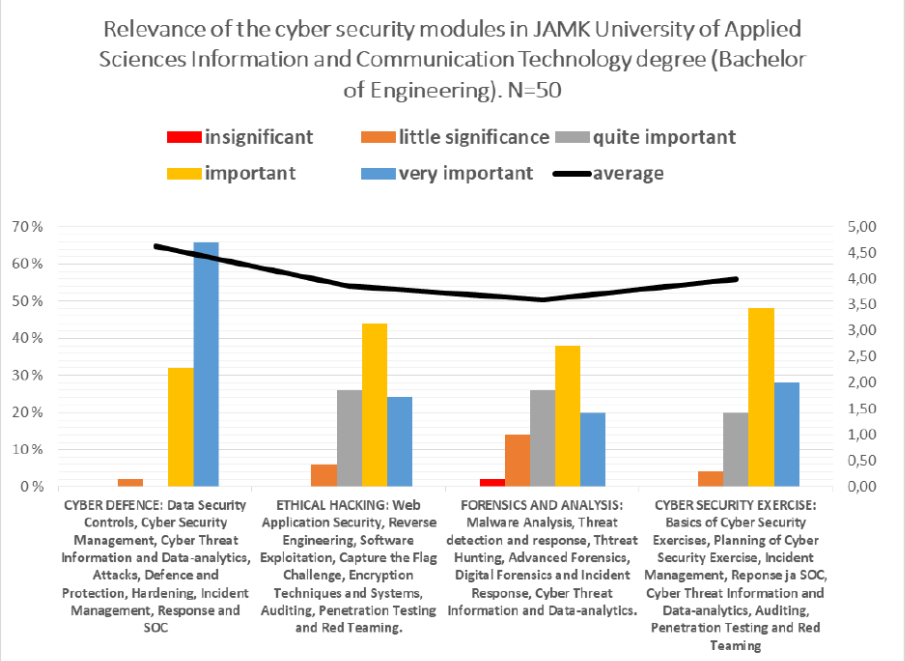


Figure 4: EQF6 Cyber security modules

Based on the responses, the same trend as earlier can also be seen in the content of the EQF6-level cyber security related modules; the modules are broader in content than at the EQF4 level, but there are fewer of them. In this section on a same scale of 1-5, the mean of the responses was 4.02. One module exceeded the 4.5 average: *Cyber defence* was clearly considered as the most important topic with a result of 4.62, and the second most important topic was *Cyber security exercise* with 4.00. *Ethical Hacking* with a 3.86 result and *Forensics and analysis* 3.60 were considered as less important sections. According to the responses, fundamental knowledge of the cyber branch and practical hands-on doing seem to be important, and parts where more in-depth expertise is needed, are seen less relevant at this education level.

The respondents were asked about the near future labor needs of the selected work roles with EQF4-level experience. In this section, Finnish vocational qualification titles are converted to match the nearest corresponding work role in the NICE Cyber Security Workforce Framework work role. The following sample of results is seen in Figure 5: Near future work role needs for the EQF4-level experience

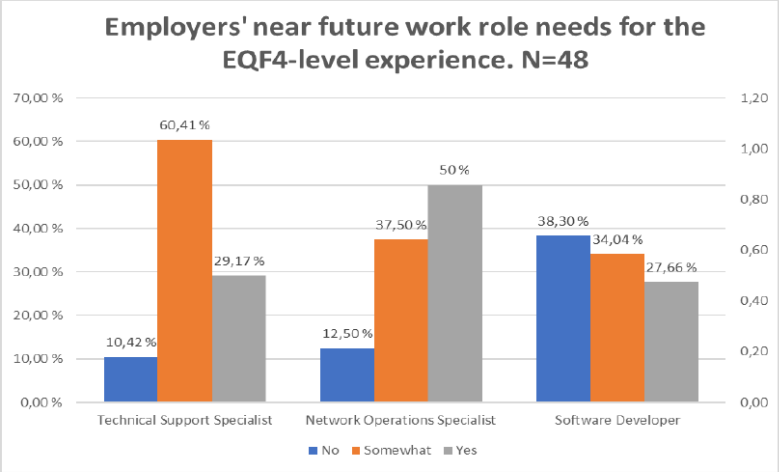


Figure 5: Near future work role needs for the EQF4-level experience

The greatest need for employees at this level of education is for network operations specialist and there may be a demand for technical support specialists. Software developers were the least needed at this level of education. High "Somewhat" bar might be explained by Technical support specialist role, which is often thought of as a helpdesk function, and many companies have outsourced this kind of role over the years. The respondents were asked about the target level of education when recruiting cybersecurity focused staff. In this question, it was possible to select multiple education level choices.

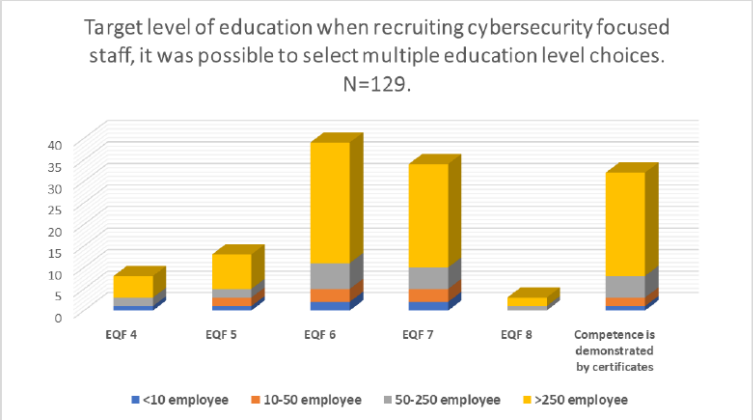


Figure 6: Target level of education

Based on the responses, cyber security related work in general have much higher education level requirements than EQF4-level could provide. University degrees and performed certificates are highly appreciated in the recruitment process. In addition to education level, another significant part in the selection process of the employee is the job applicant's work experience. The respondents were asked about the needed level of experience when recruiting cyber security focused staff. The distribution of target experience levels for recruitment is shown in Figure 7: Target level of experience.

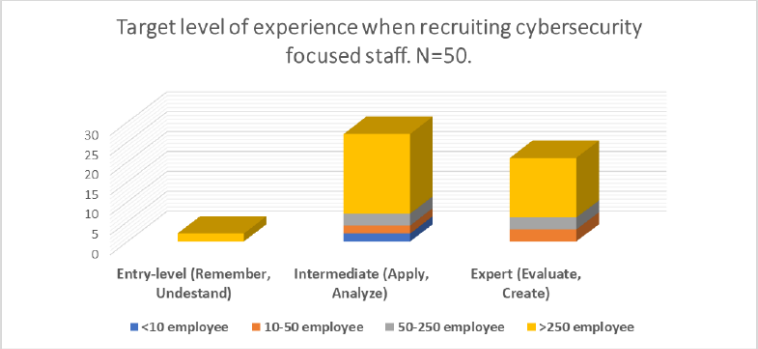


Figure 7: Target level of experience

The recruitment of entry-level employees is seen possible only in large companies. Career paths starting from the entry-level might be too challenging to smaller companies because they usually bind more experienced staff to the orientation process of a new entry-level employee. Based on the answers, intermediate experience level is the most popular class, but also the expert level is quite close to it.

Lastly, the respondents were asked to assess the distribution of their company's near future workforce needs based on the NCFW categories. The vocational qualification titles researched are divided into categories as follows: Securely Provision (SP) category includes vocational qualification title Software Developer. Operate and Maintain (OM) category includes titles Networks Installer and IT Support Specialist.

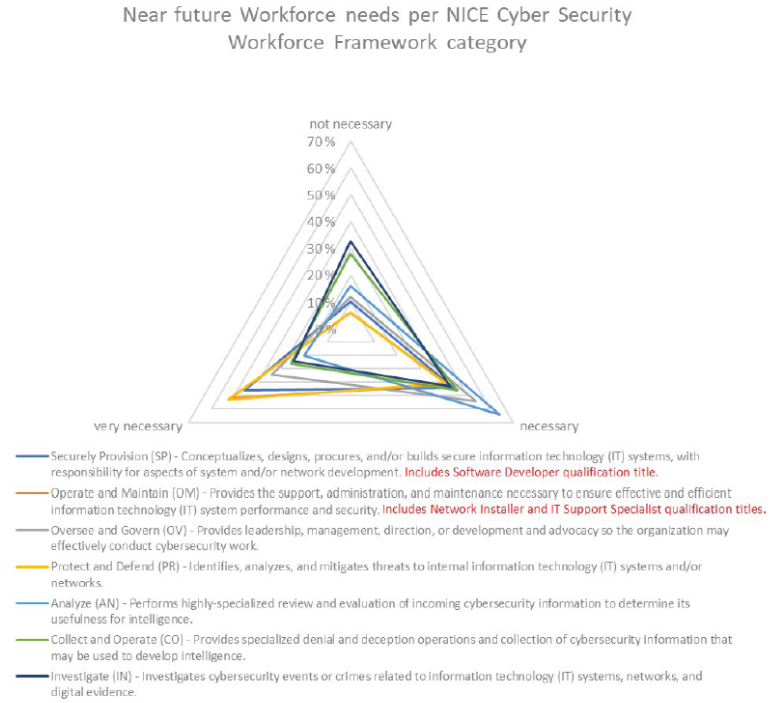


Figure 8: Near future workforce needs per NCFW category

The direction of the desired competence is strongly in Protect and Defend (PR) and Operate and Maintain (OM) categories; Securely Provision (SP) still fits in the top three categories. Analyze (AN) and Oversee and Govern (OV) clearly share the visions of respondent organizations; they both are seen necessary but also not necessary bar is high. Investigate (IN) and Collect and Operate (CO) categories are clearly seen as the least necessary.

Overall, from the employer's view, cyber security related subjects are seen as an important part of Information and Communication Technology education on both EQF-4 and EQF-6 levels. On a scale of 1-5, both modules were seen as averaging around four. Based on our research, on EQF-4 level it can be stated that the respondents consider compliance of their information security policies to be a very important part of their IT asset protection and expect this from every employee as well. Protection of devices with updates and software can be considered as one of the easiest ways to protect your environment against cyber threats, and this basic protection function seems to be appreciated by employers. Deviation notifications or any security development proposals are always valuable, especially if they are made proactively to mitigate potential threats. Situational awareness is again one of the basic functionalities of protecting an organization's most valuable data assets. Based on these results, the focus of education at this level should be on matched with basic security operations in accordance with the instructions, and more specific specializations should be given little less attention. For comparison, the same trend can be also seen in the content of the EQF-6 level cyber security related modules. The respondents' top rated module covers the basic techniques of cyber security field, and the module rated second goes through them in realistic hands-on exercise.

According to the responses, EQF-4 level education was not seen very appropriate for cyber related labor needs in Finland due to the higher level of education required for the cyber security focused staff. Overall, the chosen work roles were seen moderately appropriate. Generally, the greatest need for employees, out of the chosen degree specializations, at EQF-4 level of education is for Network Operations Specialist. Somewhat perhaps surprisingly, Software Developers were the least needed. Possibly the knowledge of basic techniques is valued more on this level of education, and the competence requirements of Software Developers are on a higher level in the surveyed organizations. The most suitable level of education when recruiting cybersecurity focused staff in Finland was EQF-6 and close to it was EQF-7; also the competence demonstrated in the certificates was considered appropriate.

The experience level of cyber security related employees is expected to be at least intermediate level; entry-level recruitment was only seen possible in two large companies. If the employee has got the ability to apply knowledge and skills in routine work situations without continuous guidance, the employee does productive work at least most of the time and does not appear as a mere expense during work induction. On the other hand, the expert level could be higher if there were enough qualified candidates available for the open cyber related vacancies.

The most needed direction of competence seems to be under Protect and Defend (PR) and Operate and Maintain (OM) categories. Identification, analysis, and mitigation of threats seem to be phenomena that responder companies still want to strengthen internally to have better cyber resilience. This research shows that they are willing to recruit their own employees to enhance the capability. Applications and devices are constantly evolving; hence admins must update and patch existing systems while new features or systems are introduced. They also want to keep these basic functions in their own hands, and an operator for these responsibilities would also be needed internally. These responses describing labor needs show a clear link to needs related to education priorities, strong basic knowledge of computing and information security, and practical hands-on skills are valuable. From the research data of the surveyed companies it can be concluded, that if they use more advanced cyber security services, like forensics, advanced analysis, or ethical hacking services, they might mainly outsource them to high-tech partners and do not recruit these employees themselves. This would explain the low demand for labor in these sectors.

5. Conclusion and Future Research

Based on our research, the profile of most wanted cyber employees' direction of competence is strong system/network administrator who knows how to operate, maintain, and mitigate threats in the environment for which they are responsible, and they should have at least EQF-6 level education and a minimum of intermediate level work experience. The competences demonstrated with certificates were considered very important, so they can be seen as a significant part of professionalism also in the cyber field. An earlier research published in 2019 by Jukka Niemelä states that there is a clear shortage of suitable labor in the cyber sector in Finland. The expected level of competence of the applicants has been lowered, and it is hoped that in the future applicants will have a basic knowledge of the cyber branch and deep expertise in one of the key areas of cyber security (Niemelä, J., 2019). On this basis, vocational qualification does not solve the problem encountered in the previous research, and in order to gain deep expertise further education or specialization in working life are still needed.

As mentioned earlier, there are no open cyber related vacancies for EQF4-level graduates as inspected by the authors of this paper. However, vocational qualification gives a good starting point for vocational work tasks, as well as the keys for life lasting learning in further education and in career progression. Strong practical hands-on skills should be achieved during vocational training, whether they consist of network technology, programming, or different operating systems. If it is desired to steer career pathway from the basic ICT tasks to the direction of cyber security, the options are either to carry out industry certifications or accomplish further education. The aim of further education should be to deepen strong basic skills to the specialization in the chosen cyber expertise area.

For future research, it would be interesting to investigate how cyber security has been implemented in other countries "on all levels of education" as Finland's cyber security strategy mandates. The qualitative research data also emphasized the 'soft skills' of sought out employees, not just the 'hard technical skills'. It is also a debatable subject, where the subject of cyber security should be sectioned and emphasized as an own educational field, as many of the curriculum proposals currently entangle it along every subject. This could be investigated through the workforce demand for different levels of education.

Acknowledgements

This work has been done in Jyväskylä University of Applied Science (JAMK) which is participating the Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project of the Horizon 2020 SU-ICT-03-2018 program. https://cybersec4europe.eu/about/

The authors would like to thank Tuula Kotikoski for her contribution in proofreading the English language on the paper.

References

Backlund, J. (2020) Examination of contemporary cyber security education [Online]. Available at http://urn.fi/URN:NBN:fi:amk-2020060416851 [Accessed 25 August 2020].
European Union (2017) Description of the eight EQF levels [Online]. Available at https://europa.eu/europass/en/description-eight-eqf-levels [Accessed 5 September 2020].
Finnish National Agency for Education (2020) Qualification requirements entered into force on 01.08.2020 (OPH-2596-2019) [Online]. Available at https://eperusteet.opintopolku.fi/eperusteet-service/api/dokumentit/6941346 [Accessed 25 August 2020].
Joint Research Centre (JRC), the European Commission's science and knowledge service (2019) A Proposal for a European Cybersecurity Taxonomy [Online]. Available at https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf [Accessed 5 September 2020].
National Initiative for Cybersecurity Education (2017) Cybersecurity Workforce Framework [Online]. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf [Accessed 1 August 2020].
Nevala, J. (2018) Cybersecurity situation analysis - Survey in Central Finland 2016-2018 [Online]. Available at http://urn.fi/URN:NBN:fi:amk-2018121721956 [Accessed 19 September 2020].

Niemelä, J. (2019) Demand, availability and development of the cyber security workforce respond to the need for labor in Finland [Online]. Available at http://urn.fi/URN:NBN:fi:jyu-201906032891 [Accessed 25 August 2020].
Publications Office of the EU. (2005) The new SME definition [Online]. Available at https://op.europa.eu/en/publication-detail/-/publication/10abc892-251c-4d41-aa2b-7fe1ad83818c [Accessed 5 September 2020].
Saharinen K., Karjalainen M., Kokkonen T., (2019) A design model for a degree programme in cyber security [Online]. Available at https://doi.org/10.1145/3369255.3369266 [Accessed 25 August 2020].
The Security Committee of Finland (2013) Finland's Cyber security Strategy [Online]. Available at https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf [Accessed 29 August 2020].
The Security Committee of Finland (2019) Finland's Cyber security Strategy 2019 [Online]. Available at https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf [Accessed 29 August 2020].
Willberg, N. (2017) Current and future needs of the cyber expertise in public sector organizations [Online]. Available at http://urn.fi/URN:NBN:fi:jyu-201706243034 [Accessed 25 August 2020].

5.2.2 Complementary analysis of the survey research

This chapter reviews a few complementary analysis from the questionnaire survey data. The following strategic objectives have been defined In the 2019 version of Finnish cyber security strategy, for the development of the national cyber security competence. Respondents were asked to define the relevance of the actions regarding to their organization. Results can be illustrated in Figure 12.

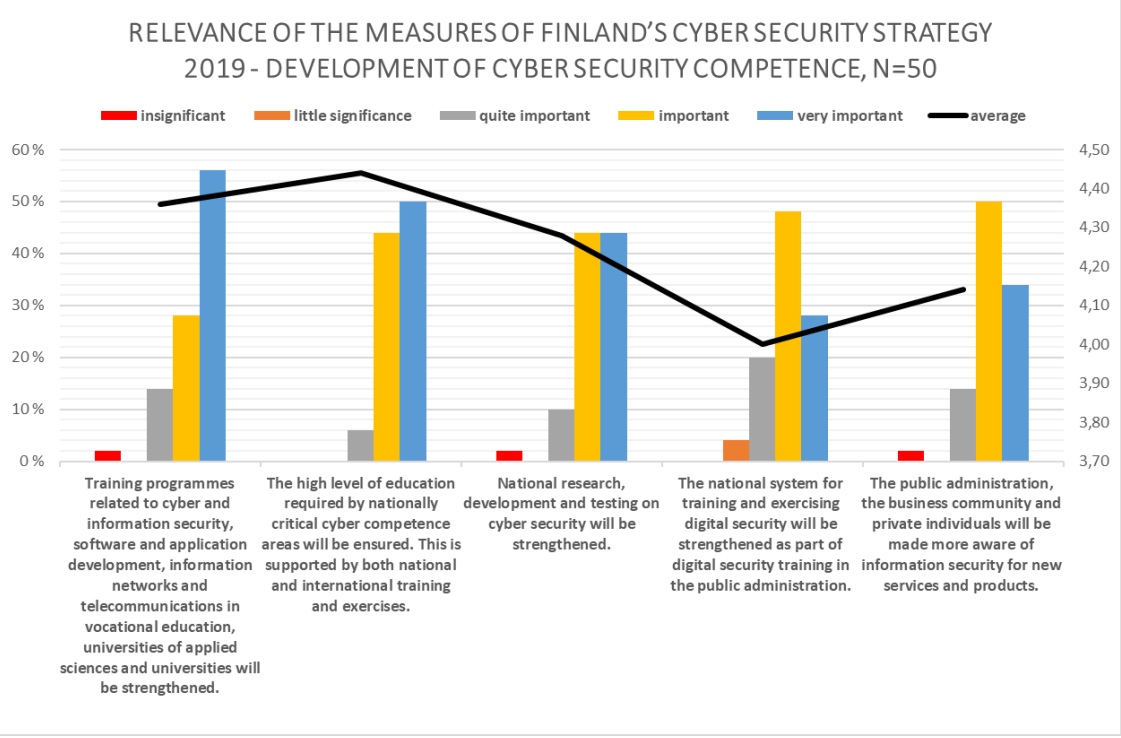


Figure 12. Relevance of the measures of the strategy

On a scale of 1-5, the mean of the responses was 4.24. *The high level of education required by nationally critical cyber competence areas will be ensured* was considered the most important topic with 4.44 result, and the second most important topic was *Training programmes related to cyber and information security, software and application development, information networks and tele-communications in vocational education, universities of applied sciences and universities will be strengthened* with 4.36. Every objective reached over 4 average so on this basis it can be concluded that the measures are in the right direction.

Respondents were asked for their opinion on how long professional growth will take for to reach an expert level in selected work roles. Details shown in Figure 13 below.

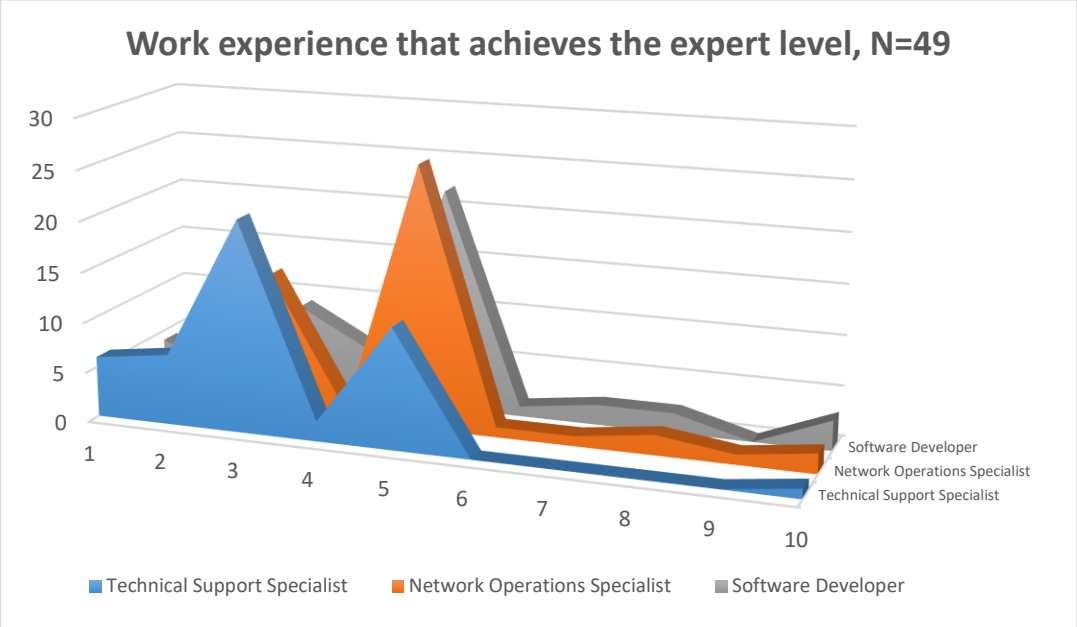


Figure 13. Expert level achieving

According to the respondents, competence development to the expert level happens the most quickly in technical support Specialist role, the development of competence takes an average 3.29 years of work experience. Competence development in Networks Operations specialist and Software developer roles take a bit longer and the expert level is achieved in average 4.80 and 4.67 years of work experience.

From the respondent companies point of view, successful recruitment of the cyber security related open positions in the last two years is seen in Figure 14 below.

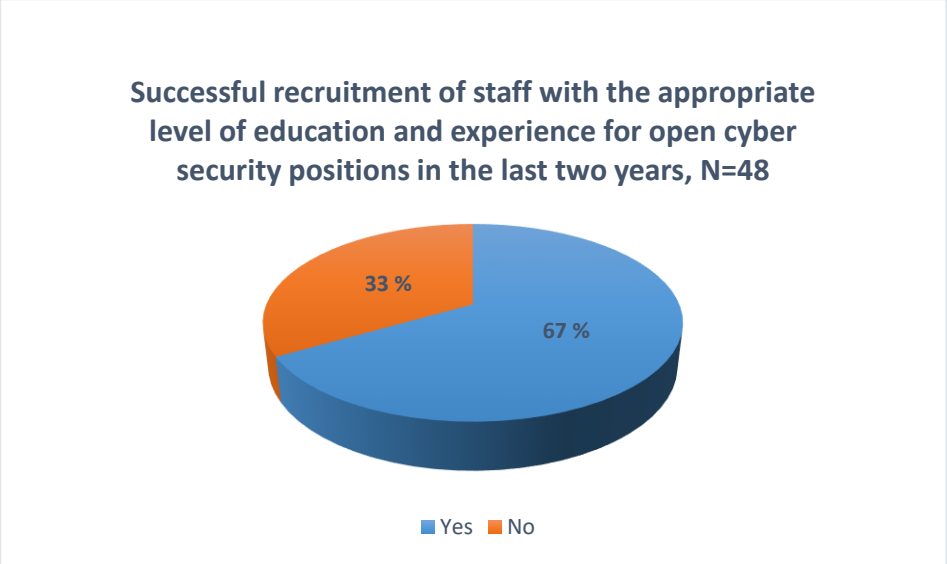


Figure 14. Successful recruitment

This question also included an additional information field for a possible NO answer, a total of 10 responses were entered in the field and they are summarized as follows:

- There is a shortage of experts and there is a strong demand for them, the job seeker can afford to choose from, and experienced professionals doesn't move so much.
- When looking for a hand-on expert, it has been found that the level of education is too low even if the competence is correct.
- Have had to recruit personnel for general ICT-positions and internally further train them in cyber related tasks.

Lastly respondents were asked to describe the best way to improve cyber security related education in Finland, to meet the needs of their organizations. In this question, the answers were implemented using a free text field. The free text field answers are combined under similar topics, a summary can be seen in the Figure 15 below.

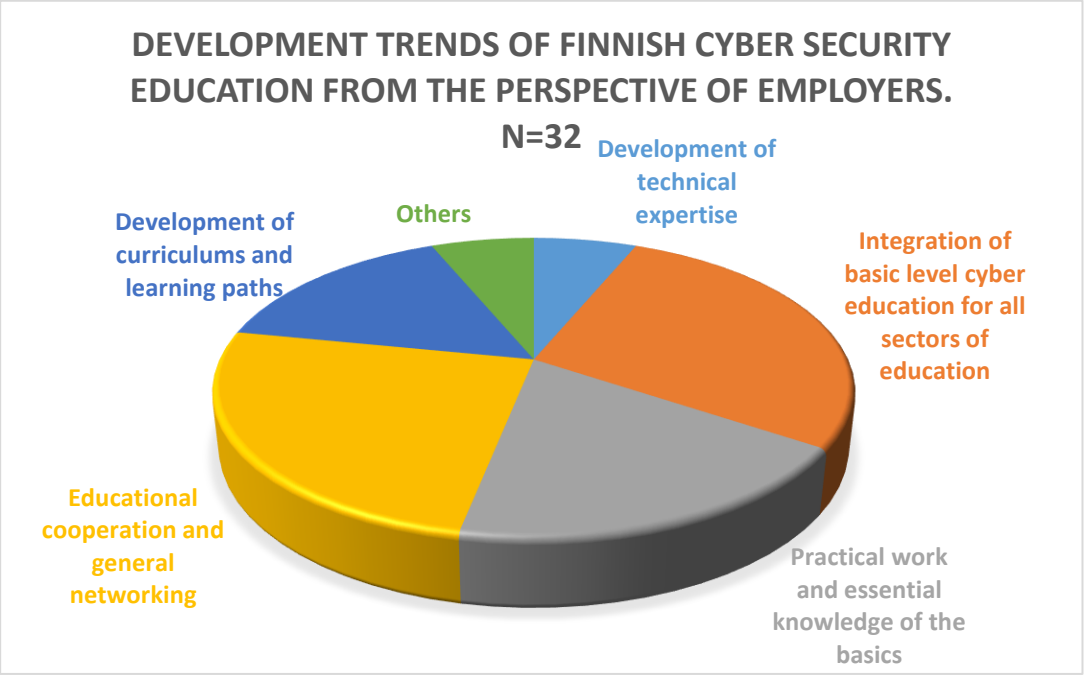


Figure 15. Development trends

28% Integration of basic level cyber education for all sectors of education. 25% Educational cooperation and general networking. 19% Practical work and essential knowledge of the basics. All free text field answers are seen in Appendix 3.

6 Complementary conclusions and further ideas

In conclusion, identifiable similarities can be seen between work roles and the content of vocational qualification. In the descriptions of the vocational qualification courses have been used so extensive descriptions that more detailed comparison is almost impossible. If it were desired to compare the content of the Finnish degree program with the framework values at a bit deeper than the title level, the study should conduct a survey or interviews with students who have completed the degree program and possibly with their teachers too. That is a interesting topic for the further research in Finland. In this study, comparison of curriculum and framework was made to facilitate comparison in possible further researches in the European area. There might be different professional titles in EQF4-level education, but framework titles and employers' experience demands still stay the same. This is also a nice subject for a research on its own, European wide vocational qualification

comparison. A few other future research ideas also emerged. First, in what way the strategy statement "*The study of basic cyber security skills must be included at all levels of education*" is implemented outside ICT-education sector in Finland? Second, how well "*quickly trained work-ready talents*" education programs produced by recruitment companies help the employers in this lack of cyber workforce quantity?

As the publications conclusion says, in working life, there seems to be demand for employees with secondary level degree in those identified work roles. However, it should be noted, that when the cyber is included in the job description, the education requirements are at the higher level. Hopefully the results of this study can be used to help the development of the future curricula and strengthening the strategic leadership of companies employing cyber security professionals.

References

(ISC)². 2020. Cybersecurity Workforce Study. Accessed 17 December 2020. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx

Anderson, L. Krathwohl, D. 2001. A taxonomy for learning, teaching and assessing: A revision of Bloom's taxonomy of educational objectives.

Backlund, J. 2020. Examination of contemporary cyber security education. Accessed 25 August 2020. Retrieved from http://urn.fi/URN:NBN:fi:amk-2020060416851

European Union. 2017. Description of the eight EQF levels. Accessed 5 September 2020. Retrieved from https://europa.eu/europass/en/description-eight-eqf-levels

Finnish National Agency for Education. 2020. Qualification requirements entered into force on 01.08.2020 (OPH-2596-2019). Accessed 25 August 2020. Retrieved from https://eperusteet.opintopolku.fi/eperusteet-service/api/dokumentit/6941346

Finnish National Agency for Education. The Finnish National Qualifications Framework, The European Qualifications Framework, The Framework for Qualifications of the European Higher Education Area, DESCRIPTORS. Accessed 25 August 2020. Retrieved from https://www.oph.fi/sites/default/files/documents/tutkintojen_viitekehysten_osaamistasokuvaukset_fi_sv_en.pdf

Joint Research Centre (JRC), the European Commission's science and knowledge service (2019) A Proposal for a European Cybersecurity Taxonomy. Accessed 5 September 2020. Retrieved from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Kuula, A. 2015. Tutkimusetiikka, Aineistojen hankinta, käyttö ja säilytys. Accessed 28 March 2021. Retrieved from https://janet.finna.fi/Record/janet.328266

Lehto, M. Niemelä, J. 2019. Kyberalan tutkimus ja koulutus Suomessa 2019. University of Jyväskylä, faculty of information technology. Accessed 25 August 2020. Retrieved from https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

National Initiative for Cybersecurity Education. 2016. Strategic Plan. Accessed 1 August 2020. Retrieved from https://www.nist.gov/system/files/documents/2020/10/26/2012_NICE-strategic-plan_withcover.pdf

National Initiative for Cybersecurity Education. 2017. Cybersecurity Workforce Framework . Accessed 1 August 2020. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

National Initiative for Cybersecurity Education. 2020. Cybersecurity Workforce Framework, Revision 1. Accessed 17 December 2020. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Mattila, J. Mäkäräinen, K. Pajarinen, M. Seppälä, T. Ali-Yrkkö, J. Tervo, E. 2020. Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Accessed 17 December 2020. Retrieved from https://ek.fi/wp-content/uploads/digibarometri_2020.pdf

Ministry of Economic Affairs and Employment. 2019. Growth from digital security, Roadmap for 2019–2030. Accessed 1 August 2020. Retrieved from http://urn.fi/URN:ISBN:978-952-327-405-1

Nevala, J. (2018) Cybersecurity situation analysis - Survey in Central Finland 2016-2018 . Accessed 19 September 2020. Retrieved from http://urn.fi/URN:NBN:fi:amk-2018121721956

Niemelä, J. (2019) Demand, availability and development of the cyber security workforce respond to the need for labor in Finland. Accessed 25 August 2020. Retrieved from http://urn.fi/URN:NBN:fi:jyu-201906032891

Publications Office of the EU. (2005) The new SME definition. Accessed 5 September 2020. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/10abc892-251c-4d41-aa2b-7fe1ad83818c

Rautio, P. 2007. Descriptive Comparison. Accessed 25 August 2020. Retrieved from http://www2.uiah.fi/projects/metodi/172.htm

Saharinen K., Karjalainen M., Kokkonen T., (2019) A design model for a degree programme in cyber security. Accessed 25 August 2020. Retrieved from https://doi.org/10.1145/3369255.3369266

The Security Committee of Finland (2013) Finland's Cyber security Strategy. Accessed 29 August 2020. Retrieved from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

The Security Committee of Finland (2019) Finland's Cyber security Strategy 2019. Accessed 29 August 2020. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Vilkka, H. 2007. Tutki ja mittaa - Määrällisen tutkimuksen perusteet.

Willberg, N. 2017. Current and future needs of the cyber expertise in public sector organizations. Accessed 25 August 2020. Retrieved from http://urn.fi/URN:NBN:fi:jyu-201706243034

Appendices

Appendix 1. Roles VS Titles

Software Developer (SP-DEV-001): Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.		Software developers are able to carry out programming, utilise interfaces, handle data and use version management. When working as members of a software development team, they communicate with the customer, plan the implementation of the software and ensure the quality of the implemented functionalities.		
Knowledge		**YES**	**Partial**	**No**
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.		is familiar with the basic structure of the Internet and the home and small business network (1551)	
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).		illustrates cyber threats and related risks (1322)	
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0004	Knowledge of cybersecurity and privacy principles.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0005	Knowledge of cyber threats and vulnerabilities.	confirms system vulnerabilities (1325)		
K0006	Knowledge of specific operational impacts of cybersecurity lapses.		illustrates cyber threats and related risks (1322)	
K0014	Knowledge of complex data structures.		uses structured programming in implementations (1470)	
K0016	Knowledge of computer programming principles	writes maintainable program code (1469)		
K0027	Knowledge of organization's enterprise information security architecture.		provide guidance on cyber security or privacy protection related issues (1320)	

K0028	Knowledge of organization's evaluation and validation requirements.		participates in the version review (1460)	
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.		is familiar with the basic structure of the Internet and the home and small business network (1551)	
K0051	Knowledge of low-level computer languages (e.g., assembly languages).			**No mention**
K0060	Knowledge of operating systems.	uses operating systems which are required for work (1553)		
K0066	Knowledge of Privacy Impact Assessments.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0068	Knowledge of programming language structures and logic.	writes maintainable program code (1469)		
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	illustrates cyber threats and related risks (1322)		
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).		evaluates software security (1452)	
K0079	Knowledge of software debugging principles.	finds and fixes errors from the program code (1472)		

K0080	Knowledge of software design tools, methods, and techniques.		publishes the program in a production environment (1449)	
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).		tests program functions (1471)	
K0082	Knowledge of software engineering.	interprets plans and implements software functions (1467)		
K0084	Knowledge of structured analysis principles and methods.		uses structured programming in implementations (1470)	
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	uses a programming editor or development environmen (1473)		
K0105	Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).			**No mention**
K0139	Knowledge of interpreted and compiled computer languages.			**No mention**
K0140	Knowledge of secure coding techniques.	evaluates software security (1452)		
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).		evaluates software security (1452)	
K0153	Knowledge of software quality assurance process.		tests program functions (1471)	
K0154	Knowledge of supply chain risk management standards, processes, and practices.			**No mention**
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.			**No mention**
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).		scan for vulnerabilities in the agreed network under review (1326)	
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).			**No mention**
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).		makes development proposals to improve cyber security (1324)	

K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0262	Knowledge of Personal Health Information (PHI) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.		illustrates cyber threats and related risks (1322)	
K0322	Knowledge of embedded systems.			**No mention**
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.		is familiar with the basic structure of the Internet and the home and small business network (1551)	
K0342	Knowledge of penetration testing principles, tools, and techniques.		confirms system vulnerabilities (1325)	
K0343	Knowledge of root cause analysis techniques.			**No mention**
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)		confirms system vulnerabilities (1325)	
		17	19	8
Skills				
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.		confirms system vulnerabilities (1325)	
S0014	Skill in conducting software debugging.	finds and fixes errors from the program code (1472)		
S0017	Skill in creating and utilizing mathematical or statistical models.			**No mention**

S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.		interprets plans and implements software functions (1467)	
S0022	Skill in designing countermeasures to identified security risks.		evaluates software security (1452)	
S0031	Skill in developing and applying security system access controls.			**No mention**
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.		makes development proposals to improve cyber security (1324)	
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	writes maintainable program code (1469)		
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).		evaluates software security (1452)	
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).			**No mention**
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.			**No mention**
S0174	Skill in using code analysis tools.		tests program functions (1471)	
S0175	Skill in performing root cause analysis.			**No mention**
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	follows information security instructions in their work (1321)		
		3	5	5
Abilities				
A0007	Ability to tailor code analysis for application-specific concerns.		develop the operating logic of the software (1456)	
A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).			**No mention**
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.		evaluates software security (1452)	
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	follows information security instructions in their work (1321)		
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.			**No mention**

		1	2	2

Technical Support Specialist (OM-STS-001): Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).		**IT support specialists are able to work in an information and communications technology environment consisting of workstations, network devices and accessories and areas of operation. They work as part of information management and help users in different technical problems in the customer's premises or through a remote connection.**		
Knowledge		**YES**	**PARTIAL**	**NO**
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.		is familiar with the basic structure of the Internet and the home and small business network (1551)	
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).		illustrates cyber threats and related risks (1322)	
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0004	Knowledge of cybersecurity and privacy principles.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0005	Knowledge of cyber threats and vulnerabilities.	confirms system vulnerabilities (1325)		
K0006	Knowledge of specific operational impacts of cybersecurity lapses.		illustrates cyber threats and related risks (1322)	
K0053	Knowledge of measures or indicators of system performance and availability.		uses system management tools (1363)	
K0088	Knowledge of systems administration concepts.	configures and manages the system (1364)		
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	diagnose and resolve hardware, driver, network, and printing problems (1478)		
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices,	diagnose and resolve hardware, driver, network, and printing problems (1478)		

	telephones, copiers, facsimile machines, etc.).			
K0116	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).			**No mention**
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.			**No mention**
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.		supports the use of workplace applications and operating systems (1479)	
K0237	Knowledge of industry best practices for service desk.	operates and documents its work in accordance with the organization's support service processes (1481)	5	
K0242	Knowledge of organizational security policies.	follows information security instructions in their work (1321)		
K0247	Knowledge of remote access processes, tools, and capabilities related to customer support.	supports and guides the customer and manages the device remotely if necessary (1475)		
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0262	Knowledge of Personal Health Information (PHI) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	follows information security instructions in their work (1321)		
K0292	Knowledge of the operations and processes for incident, problem, and event management.	operates and documents its work in accordance with the organization's support service processes (1481)		

K0294	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.	configures and manages the system (1364)		
K0302	Knowledge of the basic operation of computers.	diagnose and resolve hardware, driver, network, and printing problems (1478)		
K0317	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.	operates and documents its work in accordance with the organization's support service processes (1481)		
K0330	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.	manages system emergency states and coping with them (1362)		
		18	5	2
Skills				
S0039	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	manages system emergency states and coping with them (1362)		
S0058	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.	diagnose and resolve hardware, driver, network, and printing problems (1478)		
S0142	Skill in conducting research for troubleshooting novel client-level problems.	manages system emergency states and coping with them (1362)		
S0159	Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.	selects the appropriate serial installation method (1357)		
S0365	Skill to design incident response for cloud service models.			**No mention**
		4	0	1
Abilities				
A0025	Ability to accurately define incidents, problems, and events in the trouble ticketing system.	operates and documents its work in accordance with the organization's support service processes (1481)		
A0034	Ability to develop, update, and/or maintain standard operating procedures (SOPs).	operates and documents its work in accordance with the organization's support service processes (1481)		
A0122	Ability to design capabilities to find solutions to less common and more complex system problems.	manages system emergency states and coping with them (1362)		
		3		

Network Operations Specialist (OM-NET-001): Plans, implements, and operates network services/systems, to include hardware and virtual environments.	Network installers are able to install the cabling for data networks according to the customer's requirements and instructions. They pay attention to the structures of the data networks and the materials used and carry out the measurements and tests required to ensure the operation of the system.

Knowledge		YES	PARTIAL	NO
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)		
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).		illustrates cyber threats and related risks (1322)	
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0004	Knowledge of cybersecurity and privacy principles.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0005	Knowledge of cyber threats and vulnerabilities.	confirms system vulnerabilities (1325)		
K0006	Knowledge of specific operational impacts of cybersecurity lapses.		illustrates cyber threats and related risks (1322)	
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)		
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	selects the appropriate devices and takes into account the characteristics of the network equipment (1378)		

K0029	Knowledge of organization's Local and Wide Area Network connections.	is familiar with the basic structure of the Internet and the home and small business network (1551)		
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.			**No mention**
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).		understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)	
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.		understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)	
K0053	Knowledge of measures or indicators of system performance and availability.	use management software to monitor the telecommunications network and active devices (1370)		
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).		knows the structure and protocols of a data network (1377)	
K0071	Knowledge of remote access technology concepts.		compares different encryption methods and selects the appropriate encryption method (1328)	
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.			**No mention**
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).	understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)		
K0104	Knowledge of Virtual Private Network (VPN) security.		compares different encryption methods and selects the appropriate encryption method (1328)	

K0108	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).	understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)		
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	tests the functionality of the active device (1371)		
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)		
K0135	Knowledge of web filtering technologies.			**No mention**
K0136	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).		knows the structure and protocols of a data network (1377)	
K0137	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	knows the structure and protocols of a data network (1377)		
K0138	Knowledge of Wi-Fi.	knows the structure and protocols of a data network (1377)		
K0159	Knowledge of Voice over IP (VoIP).	knows the structure and protocols of a data network (1377)		
K0160	Knowledge of the common attack vectors on the network layer.		scan for vulnerabilities in the agreed network under review (1326)	
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).		illustrates cyber threats and related risks (1322)	
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	use management software to monitor the telecommunications network and active devices (1370)		

K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).		installs network equipments in accordance with applicable regulations, standards, manufacturer's instructions and customer environment requirements (1374)	
K0201	Knowledge of symmetric key rotation techniques and concepts.		compares different encryption methods and selects the appropriate encryption method (1328)	
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).		follows information security instructions in their work (1321)	
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0262	Knowledge of Personal Health Information (PHI) data security standards.	is familiar with laws, regulations and other official directions related to information security and privacy protection (1323)		
K0274	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	understands the structures, interfaces, topologies and communication technologies of telecommunication networks (1011)		
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	follows information security instructions in their work (1321)		
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	knows the structure and protocols of a data network (1377)		
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.			**No mention**

		22	13	4
Skills				
S0004	Skill in analyzing network traffic capacity and performance characteristics.		use management software to monitor the telecommunications network and active devices (1370)	
S0035	Skill in establishing a routing schema.	configures the active device to be secure and ready for use (1372)		
S0040	Skill in implementing, maintaining, and improving established network security practices.	makes development proposals to improve cyber security (1324)		
S0041	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.	configures the active device to be secure and ready for use (1372)		
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).		use management software to monitor the telecommunications network and active devices (1370)	
S0077	Skill in securing network communications.		compares different encryption methods and selects the appropriate encryption method (1328)	
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).		makes development proposals to improve cyber security (1324)	
S0084	Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).		configures the active device to be secure and ready for use (1372)	
S0150	Skill in implementing and testing network infrastructure contingency and recovery plans.			**No mention**
S0162	Skill in applying various subnet techniques (e.g., CIDR)	knows the structure and protocols of a data network (1377)		
S0170	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	configures the active device to be secure and ready for use (1372)		
		5	5	1
Abilities				
A0052	Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	configures the active device to be secure and ready for use (1372)		

A0055	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	use management software to monitor the telecommunications network and active devices (1370)		
A0058	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	use management software to monitor the telecommunications network and active devices (1370)		
A0059	Ability to operate the organization's LAN/WAN pathways.	manages and protects home and small business network equipments and peripherals (1550)		
A0062	Ability to monitor measures or indicators of system performance and availability.	monitor the data network using a variety of analysis tools (1327)		
A0063	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	uses workplace communication channels and softwares (1557)		
A0065	Ability to monitor traffic flows across the network.	monitor the data network using a variety of analysis tools (1327)		
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	monitor the data network using a variety of analysis tools (1327)		
		8	0	0

Appendix 2. Survey

Master's Thesis survey Janne Jaurimaa

Tämä kysely on osa opinnäytetyötäni Jyväskylän ammattikorkeakoulun kyberturvallisuuden YAMK-koulutusohjelmassa. Kyselyn tarkoituksena on selvittää suomalaisen kyberkoulutuksen soveltuvuutta eri toimialoille. Tutkimuksen pääpaino on toisen asteen koulutuksessa.

Kysely sisältää 12 kysymystä, joihin vastaamiseen menee noin 15-20 minuuttia.

Kyselyn vastaukset käsitellään anonyymisti, eikä yksilöiviä henkilö- tai organisaatiotietoja kerätä.

Toivon, että välitätte kyselylinkkiä organisaationne sisällä sopivaksi tuntemillenne tahoille, varsinkin heille, jotka toimivat tai ovat toimineet kyberpainotteisten tehtävien rekrytointiprosessien parissa.

Mikäli haluatte lisätietoja kyselystä, niin ottakaa ihmeessä yhteyttä m1270@student.jamk.fi

Kysely on avoinna 26.7.2020 saakka.

Kiitokset vastauksesta jo etukäteen
-Janne Jaurimaa

Seuraava

1. Mikä on toimialanne? Valitkaa parhaiten kuvaava.

- ◯ AV/Media
- ◯ Kemia
- ◯ Puolustus
- ◯ Digitaaliset palvelut ja alustat
- ◯ Energia
- ◯ Finanssi
- ◯ Elintarvike
- ◯ Julkishallinto
- ◯ Terveydenhuolto
- ◯ Tuotantoteollisuus
- ◯ Ydinvoima
- ◯ Turvallisuus
- ◯ Avaruus
- ◯ Tietoliikenne
- ◯ Logistiikka

2. Yrityksenne henkilöstömäärä

- ◯ <10
- ◯ 10-50
- ◯ 50-250
- ◯ >250

3. Suomen kyberturvastrategiassa 2019 on määritelty strategisia toimenpiteitä kyberturvallisuuden osaamisen edistämiseksi. Kuinka merkityksellisinä pidätte alla näkyviä toimenpidelinjauksia oman organisaationne kannalta?

	Ei lainkaan merkitystä	Vain vähän merkitystä	Melko tärkeä	Tärkeä	Erittäin tärkeä
Ammatillisen koulutuksen, ammattikorkeakoulujen ja yliopistojen kyber- ja tietoturvallisuuteen, ohjelmisto- ja sovelluskehitykseen sekä tietoverkkoihin ja tietoliikenteeseen liittyviä koulutusohjelmia vahvistetaan.	○	○	○	○	○
Kansallisesti kriittisten kyberosaamisalueiden edellyttämä korkeatasoinen koulutus varmistetaan. Tätä tuetaan sekä kansallisella että kansainvälisellä koulutuksella ja harjoitustoiminnalla.	○	○	○	○	○
Kansallista kyberturvallisuuden tutkimus-, kehitys- ja testaustoimintaa vahvistetaan.	○	○	○	○	○
Valtakunnallista digiturvallisuuden koulutus- ja harjoitusjärjestelmää vahvistetaan osana julkisen hallinnon digitaalisen turvallisuuden koulutusta. Sillä kehitetään julkishallinnon, yritysten ja muiden sidosryhmien työntekijöiden sekä kansalaisten osaamista.	○	○	○	○	○
Julkisen hallinnon, elinkeinoelämän ja yksityisten ihmisten tietoisuutta lisätään uusien palveluiden ja tuotteiden tietoturvasta. Kyberturvallisuus on datatalouden ja tekoälyyn perustuvien sovellusten ehdoton edellytys. Tämä edellyttää valmistajien ja palveluntarjoajien luottamusta toisiinsa sekä kansalaisten luottamusta heille tarjottuihin palveluihin ja tuotteisiin.	○	○	○	○	○

4. Ammattikoulujen tieto- ja viestintätekniikan perustutkinnon osa "Kyberturvallisuuden ylläpitäminen" koostuu alla olevista ammattitaitovaatimuksista. Kuinka merkityksellisinä pidätte alla näkyviä vaatimuksia oman organisaationne kannalta?

	Ei lainkaan merkitystä	Vain vähän merkitystä	Melko tärkeä	Tärkeä	Erittäin tärkeä
Opiskelija käyttää kyberuhkien hallinta- ja suojautumiskeinoja:					
suojaa laitteen päivityksillä ja ohjelmistoilla	○	○	○	○	○
hallitsee laitetta hallintatyökaluilla	○	○	○	○	○
vertailee eri salausmenetelmiä ja valitsee tarkoituksenmukaisen salausmenetelmän	○	○	○	○	○
Opiskelija hallitsee kyberturvariskejä:					
valvoa tietoverkkoa hyödyntämällä erilaisia analysointityökaluja	○	○	○	○	○
skannata haavoittuvuuksia tarkastelun kohteena olevasta sovitusta verkosta	○	○	○	○	○
varmentaa järjestelmien haavoittuvuuksia	○	○	○	○	○
tekee kehittämisehdotuksia kyberturvan parantamiseksi	○	○	○	○	○
Opiskelija edistää kyberturvallisuusratkaisuja					
tuntee tietoturvaan- ja tietosuojaan liittyvät lait, asetukset sekä muut viranomaismääräykset	○	○	○	○	○
havainnollistaa kyberuhkia ja niitä vastaavia riskejä	○	○	○	○	○
noudattaa työtehtävissään tietoturvaohjeita	○	○	○	○	○
opastaa kyberturva- tai tietosuoja-asioissa	○	○	○	○	○

5. Jyväskylän ammattikorkeakoulun tieto- ja viestintätekniikka, insinööri (AMK) - tutkinnossa on valittavana seuraavat kyberturvallisuusmoduulit. Kuinka merkityksellisinä pidätte alla näkyviä kokonaisuuksia oman organisaationne kannalta?

	Ei lainkaan merkitystä	Vain vähän merkitystä	Melko tärkeä	Tärkeä	Erittäin tärkeä
Kyberpuolustus: Tietoturvakontrollit Kyberturvallisuuden hallinta Kyberuhkatieto ja data-analytiikka Hyökkäykset ja puolustusmenetelmät sekä suojaaminen Koventaminen Poikkeamien hallinta ja kyberturvakeskukset	○	○	○	○	○
Eettinen hakkerointi: Web -sovellusten turvallisuus Takaisinmallintaminen Ohjelmistohaavoittuvuudet ja niiden hyväksikäyttö CTF -haaste Salaustekniikat ja -järjestelmät Auditointi, Penetraatiotestaus ja Red Team -toiminta	○	○	○	○	○
Forensiikka ja analysointi: Haittaohjelmien analysointi Digitaalinen forensiikka Uhkien metsästys Edistynyt Digitaalinen forensiikka Digitaalinen forensiikka ja poikkeamienhallinta Kyberuhkatieto ja data-analytiikka	○	○	○	○	○
Kyberturvallisuusharjoitus: Kyberturvallisuusharjoitusten perusteet Kyberturvallisuusharjoituksen suunnittelu Kyberturvallisuusharjoitus Poikkeamien hallinta ja kyberturvakeskukset Kyberuhkatieto ja data-analytiikka Auditointi, Penetraatiotestaus ja Red Team -toiminta	○	○	○	○	○

6. Hakiessanne kyberturvallisuustehtäviin painottuvaa henkilöstöä, mihin luokkaan asettaisitte tavoitteellisen kokemustason?

- ○ Entry-level (Remember, Undestand)
- ○ Intermediate (Apply, Analyze)
- ○ Expert (Evaluate, Create)

7. Suomalaisen tieto- ja viestintätekniikan perustutkinnon tutkintonimikkeitä ovat mm. IT-tukihenkilö, tietoverkkoasentaja sekä ohjelmistokehittäjä. Peilaten opinto-ohjelmien sisältöä NIST:n NICE 800-181 viitekehyksen työrooleihin, saadaan tutkintoihin kohdistettua melko sopivat viitekehyksen roolit niiden sisältämien tietojen, taitojen ja kykyjen (knowledge, skills and abilities) perusteella.

Technical Support Specialist - Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components.

Network Operations Specialist - Plans, implements, and operates network services/systems, to include hardware and virtual environments.

Software Developer - Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Kuinka pitkä kokemus alalta työntekijällä täytyy mielestänne olla, jotta häntä voidaan pitää ammattilaisena yllä kuvatuissa tehtävissä? Expert-level (Evaluate, Create). Antakaa vastaus täysinä vuosina.

Technical Support Specialist	
Network Operations Specialist	
Software Developer	

8. Onko organisaatiossanne tunnistettu avointen tehtävien täyttämisen yhteydessä tarvetta kyseisille työrooleille toisen asteen koulutuksen kokemustasolla? (Apply-level)

	Ei	Jossain määrin	Kyllä
Viimeisen kahden vuoden aikana			
Technical Support Specialist	○	○	○
Network Operations Specialist	○	○	○
Software Developer	○	○	○
Lähitulevaisuudessa			
Technical Support Specialist	○	○	○
Network Operations Specialist	○	○	○
Software Developer	○	○	○

9.
Hakiessanne kyberturvallisuustehtäviin painottuvaa henkilöstöä, mihin asettaisitte tavoitteellisen koulutustason? Voitte valita useamman koulutusasteen.

- ☐ EQF 4 Ylioppilastutkinnot - Ammattitutkinnot ja Ammatilliset perustutkinnot
- ☐ EQF 5 Erikoisammattitutkinnot
- ☐ EQF6 Alemmat korkeakoulututkinnot - Ammattikorkeakoulututkinnot
- ☐ EQF 7 Ylemmät korkeakoulututkinnot - Ylemmät AMK-tutkinnot
- ☐ EQF 8 Tohtoritutkinnot - Lisensiaatin tutkinnot
- ☐ Sertifioinneilla osoitettu osaaminen

10. Oletteko onnistuneet rekrytoimaan tavoitteellisen osaamis- ja koulutustason henkilöstöä avoimina olleisiin kyberturvallisuustehtäviin viimeisen kahden vuoden aikana? Voitte halutessanne kuvailla mahdollisesti kohtaamianne haasteita rekrytoinneissa.

- ◯ Kyllä
- ◯ Ei

11. NIST:n NICE 800-181 viitekehyksessä määritellään kyberturvallisuuteen liittyvät työtehtävät kategorioittain seitsemään luokkaan. Miten arvioisitte yrityksenne työvoiman tarpeiden jakautumista niiden perusteella lähitulevaisuudessa?

	Ei tarpeellinen	Tarpeellinen	Erittäin tarpeellinen
Securely Provision (SP) - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	◯	◯	◯
Operate and Maintain (OM) - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	◯	◯	◯
Oversee and Govern (OV) - Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	◯	◯	◯
Protect and Defend (PR) - Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	◯	◯	◯
Analyze (AN) - Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	◯	◯	◯
Collect and Operate (CO) - Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	◯	◯	◯
Investigate (IN) - Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	◯	◯	◯

12. Kuvailkaa omin sanoin mikä olisi paras tapa kehittää kyberturvallisuuskoulutusta Suomessa vastaamaan juuri teidän organisaationne tarpeita?

Appendix 3. Free text field answers

Development of technical expertise	Integration of basic level cyber education for all sectors of education	Practical work and essential knowledge of the basics	Educational cooperation and general networking	Development of curriculums and learning paths	Others
Tietoturvahyökkäysten ja menetelmien parempi tekninen ymmärtäminen.	Kyberturvallisuuden perustason laaja-alainen mutta ei välttämättä kovin syvällinen on tärkeää lähes kaikissa toimenkuvissa yrityksessämme. Kyberturva-asiantuntijoiden osalta kaipaamme erityisesti SOC osaamista.	Olemme kohtuu suuri (1k+) IT talo ja vaikka meillä on oma kyberturvallisuusyksikkö, näkisin, että suurin hyöty meille olisi kuitenkin sen, että meille mihin tahansa roolii rekrytoitavilla henkilöillä olisi kädet-saveen tason ymmärrys siitä mitä kyberturvallisuus on ja mitä sillät tarkoitetaan (sen sijaan että se tunnetaan vain hype-sanana).	Pyritään lisäämään oppilaitosten ja yritysten kanssakäymistä ja yritettäisiin availla suorempia tiedonvaihtokanavia työelämän tarpeiden välittämiseen.	Enemmän koulutustarjontaa eri kouluissa.	Markkinoida alaa, jotta pystytään löytämään potentiaaliset koulutettavat eri koulutusohjelmiin ja sitä kautta työelämään oikeille paikoille.
Etsitään uusia ratkaisuja ja testataan jatkuvasti	Sanoisin, että kyberturvan osalta olisi syytä aloittaa asioiden läpikäynti jo hyvin varhaisessa vaiheessa julkisia koulutuspalveluita. Koutulutusasteiden kasvaessa tietämystä tulisi viedä tarkemmalle tasolle ja aloituspaikkoja kyberturvaan keskittyville koulutuslinjoille tulisikin olla riittävästi. Koulutuksessa voisi pistää vielä enemmän paukkuja turvalliseen ohjelmistojen kehittämiseen.	Ihmiset oppivat parhaiten käsien kautta, eli pitää harjoitella harjoitella harjoitella. Powerpointi-johtaminen ei auta yhtään.	Alan yritysten ja koulutusta tarjoavien organisaatioiden yhteistyön lisääminen.	En tiedä mitkä painotukset koulutusohjelmissa on, mutta toivoisin, että opiskelija voisi valita haluaako syventyä tekniseen vai hallinnolliseen puoleen. Tekniselle puolelle painottaisin hands-on-hacking tyyppistä toimintaa, koska jotta voi ymmärtää tietojärjestelmiin kohdistuvat riskit, pitää ensin tietää miten niitä hyväksikäytetään. Toisaalta sitten ne ketkä ei niin välitä teknisestä puolesta, niin GRC:n puolelle syventymistä. Joskin kumpaakin pitää ymmärtää riippumatta siitä mihin syventyi. Joka tapauksessa kumpiakin osaajia tarvitaan laajasti.	Minun mielestäni on aivan sama kyberkoulutuksella, jos ei yksilöllä löydy mielenkiintoa myös ylläpitää osaamista, esimerkiksi harrastaen. Olemalla 'vain päivätöissä' saadaan diipadaapailijoita ihan tarpeeksi. Vaikeaa on löytää ne henkilöt jotka oikeasti ja aidosti ovat kiinnostuneet, ne jotka ovat mukana muotoilemassa alaa.
	Kyberturvallisuus itsessään erillisenä koulutusohjelmana ei yleensä tuo yritysten kannalta toivottuja tuloksia. Turvallisuus on osa kaikkea toimintaa ja yrityksen muuta operointia ja kyberturvallisuus on osa laajempaa turvallisuuden kokonaisuutta. Vaikka toimimme hyvin spesifisesti kyberturvallisuuden parissa, kun kehitämme ja ylläpidämme erinäisiä sekä omia, että asiakkaidemme järjestelmiä, ei meillä käytännössä ole suurta tarvetta varsinaisille "cyber security specialisteille". Sensijaan kyberturvallisuuden kokonaisuuksien tulisi olla konsepteina, menetelminä sekä nykyisin käytettävissä olevina teknologioina tuttuja itse siinä substanssissa, jota henkilö varsinaisesti tekee ja opiskelee.	Käytännön harjoiteet ja osittainen koulutus oppisopimuksella alan yrityksissä toisivat opiskelijoille tukitärkeää käytännön osaamista. Lisäksi ymmärrys tietoverkoista (verkko-osaaminen) kokonaisuuden ymmärtämiseksi tulisi olla kiitettävällä tasolla.	Kyberklusterin sekä huoltovarmuuskriittisten yritysten ja Yliopistojen/AMK välinen koulutuksellinen yhteistyö, jotta yritysten erityistarpeet tulevat ainakin kuulluksi ja toivottavasti myös koulutuksellisesti huomioitua.	Kyberturvallisuuskoulutus täytyisi lisätä jo peruskoulujen opetussuunnitelmaan. Suurin uhka on human factor, joten koko henkilöstön kyberturvallisuuskoulutus selkokielellä jonkun (kalliin) konsulttifirman toimesta palvelisi jokaista organisaatiota. Teknisen kyberturvallisuuskoulutuksen tarjonta tuntuu lisääntyvän koko ajan, haasteena onkin löytää koulutustarjonnasta laadukasta ja relevanttia koulutusta tarjoavat yritykset/konsultit/oppilaitokset.	
	Kyberturvallisuus ei ole asia, jota voi liimata ohjelmistoon, järjestlemään tai tekniseen ympäristöön "päälle", vaan sen tulee olla mukana aivan kaikessa tekemisessä itse kokonaisuuden suunnittelusta lähtien. Kyberturvallisuutta on myös huono opettaa irrallisena kokonaisuutena koska sen todellinen ymmärrys vaatii aina myös huomattavan syvällisen ymmärryksen itse suojattavasta kohteesta sekä kokonaisuudesta, jonka osa kyseinen kohde on. "Expert" tasolla toiminen tietoturvassa käytännössä vaatii "Expert" -tason tiedot ja ymmärryksen myös itse ympäristön toiminnasta ja siinä käytetyistä teknologioista. Muussa tapauksessa kyberturvallisuus jää lähes poikkeuksetta vain "filosofian" tasolle, eikä tiedot ja taidot ole sovellettavissa reaalimaailmassa.	Työharjoittelu, opiskelijoiden sijoittaminen määräaikaisesti yrityksiin käytännön tehtäviin, esim. SOC-tehtäviin. Käytännön työtä, kädet "savessa". Tulisi luoda menettely jossa yritykset sitoutuvat sijoittamaan opiskelijoita säännöllisesti em. tehtäviin. Tästä hyötyisivät myös yritykset, sillä alan suurimpia ongelmia on osaavan henkilökunnan puute.	Oppilaitosyhteistyö, jossa kyetään selkeästi kertomaan mitä juuri meidän yrityksessääme tarvitaan riittävän kyber-suojauksen aikaansaamiskesi ja ylläpitämiseksi	Perus IT-asiantuntijan kyberturvallisuustietoisuus ja perustaidot pitää saada kuntoo jo lähtien ammattikoulusta niin että perustaso on jo riittävä tunnistamaan riskejä ja tuottamaan palveluita turvallisesti Kyberturvallisuuteen erikoistuneet henkilöt tukevat erikoistumisellaan jäljelle jääviä puutteita.	

	Suomen kyberomavraisuus on kansalliseen turvallisuuteen liittyvä asia, matalan tason ymmärrystä lisättävänä. Vielä 10-15 edes yliopistotasolla ei opetettu järjrstelmiin murtautumista tai heikkouksien hyödyntämistä. Jos näitä asioita ei itse osaa tehdä niin uhkien tunnistaminen ja/tai torjunta on mahdotonta.	Tekemällä oppii hyvin, joten koulutusta voisi järjestää enemmän tekemisen suunnalta, joten oppilaat tekisivät puolustavia ja hyökkääviä toimenpiteitä, kävisivät läpi ja tekisivät niin sanotusti oikeita tapauksia oikeanlaisessa ympäristössä ja työkaluilla mitä on yrityksissä käytössä.	Yhteistyössä yritysten ja valtionlaitosten kanssa koulutusohjelmien määrittely ja tarvittavien teknologioiden käyttöönotto.	Vaikea määritellä lyhyesti. Ensinnäkin tarvitaan laadukasta perustason opetusta tietoliikenne- ja tietotekniikasta, jonka päälle voidaan rakentaa substanssiosaamista kyberturvallisuuden osa-alueilta. Meillä osaamista kehitetään ja hallitaan suomessa mutu-tuntumalla. Sille harvoin on muuta, kuin mielipideperusteluja. Esimerkiksi käyttämällä mainittua NIST'n 800-181 frameworkia pohjana, tästä mutusta päästäisiin eroon ja meillä olisi perusteltua koulutusta aihealueesta. Tällä hetkellä useissa paikoissa puhutaan ura-polusta ja sen rakentumisesta, kun pitäisi puhua osaamispoluista ja tunnistaa osaamisen rakentamisen tarvetta järkevästi ns. henkilöstöryhmä tai koulutustaustariippumattomasti. (Toki ne eri tasot kuten 2 aste sekä alempi ja ylempi korkea-aste tarvitaan, mutta siellä on myös erityisesti ns entry-level tasolla yhteneväisyyksiä, joita voidaan opettaa kaikille ryhmille ja tämän jälkeen eriyttää opetusta tunnistamalla osaamispolun tarpeet.) Eli, kun tunnistetaan tehtävässä tarvittava osaaminen 800-181 (NICE) mukaisesti --> tunnistetaan osaamispolku, jolla se rakentuu. Näin n määrään tehtävistä päästään rakentamaan yhteneväisiä osaamispolun osia, joista tarpeen tullen eri ryhmät ikäänkuin erkanevat omiksi haaroikseen. Tällä tavoin tehtävässä tarvittavaa osaamista tunnistamalla, päästään myös siihen, että ihan oikeasti rekrytointitilanteissa voidaan pyytää tarvittavaa osaamista. Tämän jälkeen voidaan tunnistaa myös osaamisen vaje siihen tehtävässä tarvittavaan ideaaliosaamiseen --> osaamisen kehitttämisen suunnitelma --> järkevää ja tarpeellista osaamisen kehittämistä. Ongelmana onkin ehkä pahiten se, kuinka tunnistaa ja tunnustaa luotettavasti rekrytoitavan työntekijäehdokkaan osaaminen ja siihen pitäisi päästä lisäämään vielä se abilities eli tunnistaa, onko henkilö kykenevä (vaikka osaaminen on muuten hallussa). Mikä muodostaa lopulta tämän ability:n? Esimerkki, jos haemme tier 3:n kaveria CSOCiin osaamiseltaan pätevä kaveri kaikin puolin ja päädymme rekrytointiin. Työssa havaitaan, että kaveri ei kykene tekemään työtä paineen alaisena. Ability petti? Tunnistettiinko sitä? Onko abilityn tunnistaminen tällä hetkellä rekrytoinnissa vain rekrytoijan mutu-tunne?	
	Varmistamalla määrällisesti ja laadullisesti riittävän korkeakoulutasoisen (alempi ja ylempi) koulutuksen. Lisäksi kaikkeen ICT-alan koulutukseen tulisi kuulua jossain määrin pakollisia kyberturvallisuuden opintoja.	Huolehtia ns perusasioiden riittävästä osaamisesta. Yleensä suomalaisessa koulutuksessa koulutukseen otetaan aivan liikaa erilaisia asioita suhteessa siihen, että ns perusasiat eivät ole opiskelijoilla kunnossa. Työhönotossa on mm törmätty lukuisia kertoja siihen, että työnhakijalla on ollut vaikka mitä tutkintoja suoritettuna, mutta kysyttäessä vaikka TCP/IP:stä tai jostain muusta vastaavasta asiasta aivan perusasioita eivät ne ole olleet hallussa. On työelämässä helpompaa kouluttaa "ylempiä asioita" tekijöille täydennyskoulutuksena kuin lähteä kouluttamaan paikkomalla aivan perusosaamisesta lähtien lähes kaikkea.	Yhteisölliset tapahtumat alan huippuammattilaisten vetämänä. Yritysten ja huippuammattilaisten yhteisöllisyys on paras tapa edistää proven and best practices osaamista. Koulutus on aina teoreettista ja konkreettiset opit saadaan oppimalla alan huippuammattilaisilta.		
	Osana koulutusta opiskelijoille tulisi opettaa yritysen ja muiden organisaatioiden yleisistä haasteista tietoturvan parissa. esim. Resurssit (aika, budjetti) sekä toimintamallit jotka voivat hidastaa tai jopa estää ketterän kehityksen, jonka seurauksena organisaatiot ovat jatkuvasti takamatkalla tietoturvan kanssa.		Riittävän pitkä roadmap joka koostetaan kansalliseen kyberturvallisuustoimintaan osallistuvien tahojen tarvekartoituksien pohjalta.Organisaatiot voivat kouluttaa myös toisiaan ja ulkoisen koulutuksen (oppilaitos tai kaupallinen kouluttaja) osalta vaatimustasoedellytykset (kokemus,puitteet yms.) käyttöön.		