Cybersecurity skill development through degree programme relative to labor market

Solomon Luoma

2021 Laurea

Laurea University of Applied Sciences

Cybersecurity skill development through degree programme relative to labor market

Solomon Luoma

Security management

Bachelor's Thesis

December 2021

Laurea University of Applied Sciences **Abstract**

Security management

Bachelor's degree

Solomon Luoma

Cybersecurity skill development through degree programme relative to labor market

Year 2021 Number of pages 33

In recent years cybersecurity has become global concern for all citizens. Importance of this research should not be underestimated considering the growth technological fields and cyber threats, that comes with it. Finland as part of the global world and member of the European Union must contribute to the global safety through its institutions. The objective of this thesis is to analyze how cybersecurity skills gained from degree program relates into Finnish labor market. The assignment for this research came through ECHO. This thesis is part of the ECHO project where Laurea university of applied science is partner institution.

Research was completely done by using qualitative method. Since this was not developmental project secondary data and thematic analyze were used. Firstly, knowledge based was gathered about the topic. Secondly the two components degree programmes and labor market were analyzed. First component was analyzed by searching the existing cyber security degree programmes and skills derived from the curriculums. Focus group was university and university of applied science. Second component the labor market was analyzed by using four popular recruitment channels Linkedin, Duunitori,Oikeotie and Monster. Screening for the search engine was done by Cybersecurity as keyword, definition of recently graduated as requirement and country of Finland as region. Thirdly the results were presented. Research question was used in order to guide and help to navigate the research. Finally, the conclusion and recommendations were given.

The results answered the research question by showing that there is the skill gap between skills gained from degree programme and skills demanded by the labor market. This thesis also argues that in most parts there is no equivalency between degree programmes and current labor market.

Keywords: Cybersecurity, cyber skill, labor market, degree programme

Table of contents

1 Introduction

In this fast-moving world where we are consuming information and products via online or where services are being automated more than ever before, it becomes more difficult for the industries to identify and mitigate all the possible risks. Organizations in the public and private sectors are depended on information technology and information systems to successfully carry out their missions and business functions (NIST 2012). Isaca (Information System Audit and Control Association) run the state of the cyber security 2020 survey and it stated that 53% believe that they will face a cyber-attack within 12month. Cyber-attacks were the most common threat actors with 22%. 62% said that their cyber security teams were understaffed. Which is significant because understaffed teams showed less confidence in their ability to responds to cyber threats according to same survey. Organizations that took more than six months to fill cyber security positions were exposed to 38% of cyber-attacks and organizations that took less than two weeks was 28% (ISACA 2020). Report made by European commission stated, that "The cyber security skill gap for cybersecurity professionals working in the industry in Europe is predicted to be 350000 and globally 1.8 million by 2022" (The European Commission 2017). Cyber criminals find new ways to hack into different infrastructures. For this reason, it is very important for the organizations to try to stay ahead of cyber criminals.

This research will be part of ECHO (The European network of cybersecurity centers and competence hub for innovation and operation) collaboration with Laurea university of applied science. The main objective of ECHO is to strengthen the proactive cyber defense of the European Union by enhancing Europe's technological sovereignty through effective and efficient multi-sector and multi-domain collaboration. The project will develop a European Cybersecurity ecosystem to support secure cooperation and development of the European market as well as to protect the citizens of the European Union against cyber threats and incidents (ECHO 2019). Laurea university of applied science is one of the 30 partners in this project. This research will contribute to the objective of the ECHO project by having deeper understanding of the cyber skill development in educational system in one of the EU member state countries and the current state of its cyber labor market. As a result of this thesis Echo project takes one step closer of identifying possible reasons for skill gaps.

One of the key concepts of Finland's cybersecurity strategy 2014 was strengthening of research and educational programs (Turvallisuuskomitea 2014). The objective was to improve the standards of curriculum requirements for cybersecurity in educational institutions. This research will target the skills gained from Finnish degree programmes that has cybersecurity

as part of the curriculum. For conclusion we should be more aware of skills gained from Finnish cyber education and skills demanded by cyber labor market.

This research will assess thoroughly the following components: The educational institution and Labor market. Thesis is divided in five chapters. The first is introduction. The second chapter is literature. In this chapter the two components will be analyzed through exciting literature such as thesis, reviews, curriculums, reports and books. The purpose is to understand current landscape of Cyber security education in Finland and cybersecurity labor market. Degree programme in this research refers to both bachelors and master's degree programmes provided by higher educational institutions. The third chapter is methodology. In this chapter the qualitative research method is used for data collection and to answer the research question which is" Does post graduate cyber security skills meet the demands of labor market"?

2 Cybersecurity skill development through degree programme and labor market

With the birth of www (World Wide Web) also came the threat of network crime (Cybersecurity 2020). If the idea back then was that network security should be the key priority, the one would think that by 2021 cyber security should be the most common and well-understood security fields. However particularly in Finland, where new technology skills, intelligence skills, cryptography, a broad understanding and management of the entire cyber field have come to the fore when discussing the cybersecurity skills shortage (Niemelä 2019).

2.1 Cybersecurity

When trying to define cyber security, there are lot of different and broad definitions. The word cyber is a prefix. Just like "un" it is a letter or group of letters added to the beginning of the word in order to give it new meaning (Cambridge dictionary 2021). The word cyber derives from the Greek word "cybereo" (Turvallisuuskomitea 2018). In colloquial language the word cybersecurity is associated with any crime that happens through electronical device. Here are few different definitions for cyber security: Cyber security is the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation (National initiative for cyber security studies and careers 2021). The Finnish security committee defines the cyber security as: a target state in which the cyber environment can be trusted and secured (Turvallisuuskomitea 2018). Cybersecurity can be defined as measures to protect against cyberattacks and their effects and take the necessary countermeasures (Lehto & Kähkönen 2015).

As the examples show that the definitions are not too specific. Few conclusions can be taken from these different definitions. First, they are describing an ongoing process not an end state. Second, they are describing protection of information. Third, they describe an action within a cyber space. Lehto and Kähkönen (2015) in their research paper “Kyberturvallisuuden Kansallinen Osaaminen” referred to Martin C. Libicki’s OSI (Open system Interconnection Reference Model) as foundation of cyberworld. OSI consists of five layers. First the physical layer includes the physical parts of the communication network, such as network devices, switches, routers, and both wired and wireless connections. Second the syntactic layer consists of various system control and management programs as well as functions with which devices connected to the network interact with each other such as network protocols, debugging, handshake, etc. Third the semantic layer is the core of the entire cyber world. It includes information and data contents on the user's terminals, as well as various user-controlled functions such as printer control. Fourth the service layer includes all public and private digital network services. Fifth the cognitive layer describes the world of understanding user information, the world in which information is interpreted and personal understanding and perception is formed. OSI model defines how two computers can transfer data to each other, thus creating computer network (Lehto & Kähkönen 2015).

The www became an internet system for connecting different files to each other across the internet network. This gave access for millions of people to explore vast amount of information. These files and people who used them created an online world. The world of interdependent network of different information technologies such as telecommunications networks, computer systems, and embedded processors and controllers. This world is called cyber space (NICCS 2021). It is a cyberspace that differentiates cybersecurity from information security. Information security is about different methodologies and processes that are design to protect the data (NIST 2012). The data can be form of print, electronic or any other form which possesses sensitive information, that only authorized people should have access to (Fruhlinger 2020). The key difference is that in information security, sometimes referred to as data security or InfoSec the purpose is to protect any form of important information, this includes information in physical form. Whereas in cyber security, the information in physical form is not included, only the data that exists within cyber space. Cybersecurity specifically is concerned with protecting digital data by controlling, managing and preventing data from outside threats, that coexist within a cyberspace (National institute of Standards and Technology 2012). Distinction between cybersecurity and information security is very important to make, in order to be clear about state of cybersecurity education and labor market. With regard previously mentioned, to talk about cybersecurity in vacuum, without any overlap with information security, makes it a challenge.

The growth of digital industries, where increasing number of private or public companies and their services only operates in online. The increasing number of online stores and other digital

services creates attractive environment for cyber criminals. For this reason, companies must make sure that cyber security is design to be integral part of the whole product lifecycle (Liikenne & viestintä ministeriö 2016). Companies such as Instagram and YouTube, who are offering a platform, where private citizens and corporations can create and promote their businesses. These companies that provide these platforms are extremely depended on the fact that they are safe from cybercrimes. It is not just the business aspect of it, but also social. Big part of the modern social life is done in this kind of platforms such as dating, meeting and creating friends, networking and simple conversations with friends from different parts of the world. Apps such as Facebook, Instagram and Snapchat allows people to connect by using their own name or avatar. This creates a threat for different cybercrimes such identity theft and cyber bullying.

The growing digitalization in different types of businesses also increases the demand for human capital with the knowledge of different branches such as artificial intelligence, robotization and the Internet of Things. Also, in the public sector cybersecurity is becoming increasingly important in securing vital societal functions in a national and international environment (Turvallisuuskomitea 2014). This coexistence between information, brand and the product where all are in digital form, changes the landscape of security and makes it more complex and difficult to adapt. Cyber-attacks on private sector can create chain of events that will have an impact on local and global community.

Cyber security also plays a role in purchasing decisions. According to ETLA (Elinkeinoelämän tutkimuslaitos) “in 2015 39% of Europeans and 50% of Finns did not use some digital products or services due to related security concerns” (Mattila, Ali-Yrkkö & Timo 2020). Also 11% of small businesses in the EU-28 countries had cyber security problems, in Finland the figure was 16% (Mattila et al. 2020). Based on this we could argue that cybersecurity has become an intangible asset for companies, that operates mainly in internet. In order to stay competitive small, medium and large-scale companies, that operates in online must think cyber security critically. The same level of cyber security urgency applies for public and NGOs (Non-government organization). Best examples of this would be the large-scale leakage and blackmail of personal data by autumn 2020. This at the latest raised the importance of information security for the general public (Mattila et al. 2020). In this incident psychotherapy center Vastaamo was a victim of two hacks. The hackers successfully broke into customer database and had access to personal data of tens of thousands of customers. This led to a multiple blackmail attempt (Yle 2020). In USA (United State of The America) attackers have demanded more from victims, with the average ransom demand rising to over 1,000 USD in 2016, up from approximately 300 USD a year earlier (Sanou 2017). In general, the larger the company or organization is, the more common the cybersecurity problems are (Mattila et al. 2020).

These types of continuous global cyber-attacks, which are causing major disruptions to companies and hospitals are prompting a call for greater cooperation around the world (Sanou 2017). Cyber space has made a world a smaller and borderless place. Globalization and digitalization have forced Finland's security environment to change rapidly, in order to answer to increasing number of threats to national security, espionage, terrorism-related phenomena and projects, which are increasingly occurring on information networks (Turvallisuuskomitea 2014). In order to keep local and global communities safe, countries must be able to produce capable workforce for private and public sectors.

2.2 Skill development

In this subchapter we are going to analyze skill development in Finland. The purpose is to have better understanding about skill development in educational institutions in Finland as it relates to cyber security. Finland as EU member state has adapted the idea of Lifelong Learning (LLL). According to UNESCO (The United Nations Educational, Scientific and Cultural Organization) the definition of LLL is: All purposeful learning activity undertaken on an ongoing basis with the aim of improving knowledge, skills and competence (UNESCO 2021). The aim of LLL is to advance society's participation in labor market, social activities and to improve the know-how on sustainable and productive lifestyle (Opetushallitus 2021). For this initiative they have also build a LLL framework which introduces eight key competences which are: literacy, multilingual skills, mathematical, digital skills, social skills, civic skills, entrepreneurial skills and cultural skills (Opetushallitus 2021). For Digital skills the emphasis is on: Information and media literacy, communication and co-operation, digital content creation, safety and copyrights. One of the key functions of LLL is to reduce inequalities in Finnish society (Aarnio & Pulkkinen 2015). It offers an educational roadmap for young children from basic education (grades 1-9) to move on vocational education, higher education and adult education. The emphasis of this thesis is on degree from higher education. One of the implementations of LLL between member states is European qualification frameworks (Opetus & Kulttuuriministeriö 2021). The Finnish version of this is called Finnish National Framework for Qualification and other Competence modules (FiNQF). This framework describes the key competencies required (Opetus & Kulttuuriministeriö 2021). These qualifications are covering every step of the educational roadmap. There are eight levels of these qualifications. The levels 6 and 7 describes the degree graduates, but not doctoral which would be level 8 (Opetushallitus 2021). The description of these qualifications shows very clearly that one of the key elements is work oriented approach (Miettinen et al. 2021). Which is very much in line with LLL. If work-oriented approach is one of the key functions of LLL, then it creates working life and educational equivalency relationship between the labor market and educational institution (Aarnio & Pulkkinen 2015). These two components are then in strong interaction with each other, in a way that educational institutions are shaping their

curriculums more adaptable for labor market and labor market then tries to interact with educational institutions through recruiting, internships and trainee programs.

Just like cyber the word skill has very broad definition. Often in academia or in working environment the word skill and competence are being used loosely and sometimes they get mixed-up (Mclean, Jagannathan & Sarvi 2012). Skills are the measurements of how employees can perform defined tasks (Marquardson & Noshokaty 2019). Competence, which also has many definitions is more of blend of different multidisciplinary skills, such as social skills, management, communication and programming (Shahara 2017). This thesis accepts that both skills and competence in certain sense can be synonyms to each other and both can be used as a measurement. However, as it relates to this thesis "skill" is used because it answers the question "What can you do" more directly (Anumala 2019). Cybersecurity employees might have skills in a particular programming language, applying certain security certificates (such as ISO 27000) a database platform or another knowledge domain. Developing a skill is a major contributor for everyone's career. Differences in skills plays a huge role in how income differences are created in societies (Anumala 2019). Individuals with less skill are more likely to face unemployment due to their inability to be attractive in labor market (Musset 2015). Since the employer expects a person to perform defined skills with expertise (Anumala 2019), so the employer then goes and seeks the individual with the most suitable skills. A skill personally improves the efficiency or productivity of a person. It's no surprise that income differences between skilled and unskilled workers are huge in any economy around the world (Musset 2015).

Skill development is an integral part of any well-functioning society (Swedish International Development Cooperation Agency 2018). Its influence can be seen in production of goods, employability, private sector, economic growth and poverty reduction. Skills development is generally used to refer to individual's productive capabilities acquired through any educational settings (Swedish International Development Cooperation Agency 2018). As it relates to labor market the skills that needs to be developed are: Basic and foundational skills, transferable skills, Technical and vocational skills and professional and personal skills (Swedish International Development Cooperation Agency 2018). The combination of these skills can be called competency.

Basic and foundational skills are skills that are required in order to further your skill development (Swedish International Development Cooperation Agency 2018). Foundational skills usually are referred to literacy, basic quantitative reasoning and numerical understanding (Musset 2015). Since cybersecurity is a multidisciplinary field of study, having a strong foundational skill is very important factor for future skill-development. Finland according to OECD (Organization for Economic Co-operation and development) has in a recent history always scored high in literacy and numeracy and has also been successful in PISA

(Programme for International Student assessment) scores (Musset 2015). If skills improve efficiency and productivity, then having weak foundational skills will do the exact opposite (Musset 2015). In 2015 a study made in Finland showed that between ages of 16-65 600000 people can be subscribed to have low foundational skills.

The importance of the foundational skills can't be underestimate since internet is playing such an integral part of our daily life, even from a young age. For this reason, the basic education alone offered in elementary school should guarantee, that young people possess the skill required to operate in today's cyber world and that they understand the threats and know how to protect themselves (Lehto & Kähkönen 2015). This way students would already possess understanding of cyber world and cyber threats before entering in higher education (Zan & Franco 2019). Foundational skills are usually build-in during the basic education from 1st grade to 9th, where people usually move forward to seek more education in high school or VET (Vocational Education and training) and from there to directly employment or they seek higher education in order to build their core competences.

2.3 Degree programme

The degree program is a goal-oriented and comprehensive set of studies that focuses on a specific professional task area and its development (Jyväskylä university of applied science 2021). In Finland the education is free at all levels (Opetushallitus 2021). This allows students regardless of their ethnic or economic background to have access on every level of educational system. The Ministry of Education and Culture is responsible of all educational policies (Opetushallitus 2021). These policies set by the ministry of Education and Culture are then implemented by The Finnish National Agency for Education. Together these two institutions are set to develop educational objectives, content and methods for early childhood, pre-primary, basic, upper secondary and adult education (Opetushallitus 2021). Municipalities or joint municipal authorities are then responsible for the local administrative, in the areas where these schools are located (Opetushallitus 2021).

In Finland the higher education is divided between two branches: University and UAS (University of Applied Science). There is important distinction between how universities and universities of applied science are approaching the of subject cybersecurity. In Universities the emphasis is on Cybersecurity's scientific study, whereas in applied science the emphasis is on practicality in working life (Lehto and Kähkönen 2015).

Finnish universities mission is to promote free research and scientific and artistic education (Finlex 2021). Finnish universities are statutory corporations. This means that universities are independent corporations under the Finnish law (Opetushallitus 2021). Every three years universities together with Ministry of Education and Culture sets educational targets and determines the required resources. In Finland universities just like other schools are free for

Finnish students and students from EU, EEA and Switzerland. In Finnish universities degree programs are expected to last 3+2 years including bachelor's 180 study credits plus master's 120. In universities the education is more research driven (OECD 2020). Compare UAS students, university students are freer to choose their own study pace and subjects. In case of cyber security in all universities the degree programs are master's degrees, which means that student has received his/her bachelors on IT (information technology) or ICT (information and communication technology) or student has bachelor's degree in cyber security or ICT from UAS and go for the masters in university after the graduation.

Exactly like universities, the UAS enjoys extensive autonomy, which includes organizing their own administration, decide on student admission and design the contents of degree programmes (Opetushallitus 2021). The length of the studies depends on specific field. If student goes for Bachelor of arts studies such as Bachelor of business administration it is 180 ECT, but the bachelor's in science, which mostly includes engineering studies it is 240 ECT. In UAS the studies are only to bachelor's level (OECD 2020). In order to apply for the masters, the student must have at least of 2years of working experience. Unlike in Universities the general requirement for admission to universities of applied sciences is the completion of general upper secondary education or vocational education and training (Opetushallitus 2021). Student selection to universities of applied sciences is mainly based on entrance examinations, school achievement and work experience (OECD 2020). Universities of applied sciences may also admit applicants who are otherwise considered to have the necessary skills and knowledge to complete their studies successfully (Opetushallitus 2021).

2.4 Labor Market

From economic perspective labor market follows the very same free market principles, where rule of supply and demand applies. The labor market is the place where the supply and the demand for jobs meet, with the workers or labor providing the services that employers demand. Work can then be understood as a man-owned, desired input (Tilastokeskus 2021). The worker is then comparable to a seller while the employer is the buyer (Corporate finance institute 2015). This chapter is divided between three components: Labor market, the seller and the byer.

As it was mentioned previously word "cyber" is a prefix, it also makes it undefined term in labor market as well (Niemelä 2019). In the context of labor market, the closest definition can be found in ICT sector. ICT sector can be defined between production of goods and services (Tilastokeskus 2021). Cybersecurity is closer to field of services. In ICT the field of services includes Telecommunications, Software, consultancy and related activities, data processing, hosting and related services (Tilastokeskus 2021). The problem here is, that some

of the characteristics that are specific for the cybersecurity, such as security, national security, risk management and criminology are left out of ICT definition.

The Finnish labor market has shrunk by 10,000 people a year in recent years and the same expenditure continues as the population ages (Minna 2021). The aging population is usually the cause effect of low-birth rates (Lassila & Valkonen 2021). The low-birth rate will result smaller size households, which for start will release the parents to be part of the labor force, but eventually will culminate in smaller size labor force (Lassila & Valkonen 2021). If the age gap between new generation entering the labor force is too big, it will result for the increase of relative share of the labor force, who are entering to retirement (Kinnunen 2002). Just like any other industry the ICT market is forced to combat against this phenomenon. Small size of labor force causes private companies to invest less for expansion and overall production and use more capital in relation to labor force in production. Aging labor force will also diminish the innovation and production and it will also change the structure of consumer demand (Lassila & Valkonen 2021). One positive conclusion can be drawn from this, which is lot of companies are forced to invest money for new technologies in order to save money in labor cost. These investments will create jobs in technology department. One example of this would be robotization.

Overall population aging has a very negative influence particularly for cybersecurity field where new technology trends are introducing different types of threats that demands updated knowledge from cybersecurity specialist (Niemelä 2019). It is estimated that between 2018-2021 there will be 26500 people in retirement from technology industry (Teknologiateollisuus 2018) and 53000 new employees are needed between the same time period. There is prediction that the growth of technology field in Finland will demand 130 000 new jobs within next 10 years (Minna 2021). The added pressure also comes from the fac that private businesses and different government initiatives are expecting Finland to be part of global Cleantech competition and make cleantech one of the biggest Finnish export businesses (Kaitila & Kuusi 2021). This fight against global warming is forcing public and private businesses to continuously explore more low carbon solution through technology. It is estimated that cleantech export could be potentially valued as 30-billion-euro income for Finnish economy (Teknologiateollisuus 2020).

New technology creates new jobs that demands more people in the field of cybersecurity. In Finland the field of cybersecurity employed 6500-7000 in 2020 and is estimated to need 15000 cybersecurity specialists in 2025 (Sillanpää 2020).

2.4.1 The seller

Individual who has graduated among one year is considered as recently graduated in all official statistics (Tilastokeskus 2021). In the context of this research, the recently graduated

student is the seller, whose value is determined by the skills he or she possesses. It is for this reason why it is very important for educational institutions to provide the opportunity for wide range of skills in cyber field. This gives a student better opportunity to create stronger student portfolio, which then will be used for seeking employment.

Student portfolio becomes very important aspect, because it works as presentation of your competences. Exactly like in free market the seller is responsible to advocate his/her product when entering to market. From sellers' point of view the market can be divided between generalist field and profession field (Leinonen 2017). The difference between the two is that generalist such as Bachelor of Business Administration is knowledgeable about many topics such as accounting, math, business law and international business. This range of knowledge still lacks characteristics that are contributed to have profession such as code of ethics, professional autonomy to decide, degree as proof for body of knowledge and fulfillment of social function (Johnson 2001). Unlike Bachelor of Business Administration, a degree in Law would fulfill all the characteristics of profession. By this definition cybersecurity or any ICT field would not qualify as profession and recently graduated would still be classified as generalist in labor market.

For generalist the labor market is more challenging since there is no specific category, where they belong to. Regardless of if the employer sector is private or public the seller must make himself a target group (Leinonen 2017). This can be done with student portfolio which can be added to CV (Curriculum Vitae). In this CV the applicants' skills are highlighted. Employer can then make the decision if these skills match to the vacant that is open. It should be taken into consideration that roughly one third of the open vacancies are informed publicly in online, social media or newspapers (Leinonen 2017). These vacancies are usually put out by organization to have as many applicants as possible and through specific screening process they select the most fitting applicant. The rest of the two third are so called hidden vacancies, which means that these positions are filled privately. This creates one clearing disadvantage for recently graduate which is the lack of experience. Experience is one of the most valuable assets, when looking for employment in cybersecurity (Dawson & Thomson 2018). It should also be taking into consideration LLL also plays a huge role in competition among the sellers. Recently graduated should be consistently seek new information and new skills to add in portfolio. For the recent years cybersecurity professionals have believed that the following four areas every cybersecurity professional should be improving: threat intelligence, forensic, cloud computing and penetration testing. All this contributes to the fact that recently graduate is in the weakest position in labor market, which reflects the supply and demand nature of labor market (Leinonen 2017).

There is also regional component which the seller can't influence. Uusimaa is region in southern Finland which has a population of 1,6 million people. That makes around 30% of

Finnish population. The development of employment and business life in Uusimaa largely determines the development trend in Finland as a whole (Nieminen 2020). Employment around Uusimaa is mostly focused on service and sales (Nieminen 2020). The tense population attracts new businesses, which creates more competition and employment opportunities. According to Tilastokeskus (2020) overall employment for recently graduates has been increasing. The unemployment rate was highest at 14% among graduates from ICT field (Tilastokeskus 2021). It can be concluded that since ICT is closest to field of service, the recently graduated ICT student is in disadvantage by living less populated areas and not having working experience.

2.4.2 The buyer

The Buyer represents the employer sector either private or public. The buyer goes into the labor market with the intention to buy service of individual who can perform demanded tasks. This process is called recruitment (Neittaanmäk 2003). The target is to find best available candidate in terms of cost and benefit. Instead of viewing it as direct vacancies filling or cost and benefit ratio, it should be viewed as an optimization problem that maximizes the filling of an open job for a long time expected long-term benefits. The more productive a person is, the greater the benefit of lower opportunity costs of job vacancy and lower the immediate recruitment costs (Neittaanmäk 2003).

Recruitment is part of the personnel planning operation (Neittaanmäk 2003). Purpose of the personnel planning operation is to make sure that organization has right number of employees, working in the right positions (Valtioneuvosto & ministeriöt 2021). In order to personnel planning to be successful the organization needs to have clear understanding of the current market and future development of that market (Neittaanmäk 2003). When organization has a clear vision and know the direction of organization hiring the right personnel becomes much easier. One of the main career development challenges are unclear career opportunities, lack of organizational knowledge of their cyber security skills and training costs to prepare for a cybersecurity career (Lehto & Kähkönen 2015).

It is difficult for larger enterprises to describe the vision of a single organization covering several cyber functions to define cyber tasks. Many of these tasks at work are very different from each other (Niemelä 2019). Unambiguous description of the work is understandably problematic when trying to hire a right candidate for job. In some instances, organizations preferer to use popular frameworks such NCWF (National Cybersecurity Workforce Framework). These type of frameworks helps the organizations to identify different cybersecurity work tasks, which helps organizations to hire right individuals (Niemelä 2019). Importance of the right human capital can’t be underestimated because with the

organizational structure, culture and strategy they create the competence of the organization (Wagner 2012).

The recruitment process has three steps: to identify what type of vacancy is open and what is demanded in order to be successful, to identify right recruitment channels where the possible employee can be found, to have right screening process in order to hire best possible candidate. It is important to have efficient recruitment process, because organization doesn't want the expenses to be too high (Neittaanmäk 2003). According to Neittaanmäki (2003) the operational costs of recruitment process include communications costs (such as newspapers, social media etc.) people involved with the recruitment process usually Human resource and new employees training, mistakes and low input at the start of the new job.

Organizations that are looking for cybersecurity employees the recruitment is mostly done in two ways: direct search and indirect search (Niemelä 2019). Direct search includes headhunting and trainee programs etc. Indirect search includes career paths in organizations own websites or use of the social media etc. (Niemelä 2019). In areas where organizations suffer from labor shortages, instead of applying it may be sufficient for applicant to leave details (Duunitori 2021). The recruitment process can be very challenging for organizations that are looking for cybersecurity employee. The issue for these organizations is that the degree programs are relatively new and there needs to be clear understanding of core functions between cyberworld and the organizations (Niemelä 2019). As newly graduated generalist the cybersecurity candidates can be described as bit anomalous as where they fit in occupational structure (Dawson & Thomson 2018).

3 Methodology

The term research is related to seek out the information and knowledge on a particular topic or subject. In other words, research is an art of systematic investigation (Mishra & Alok 2017). Empirical research is research, where the outcomes of the study are strictly based on concretely empirical evidence (Patten 2000). It is process of following careful plans for making observations, engaging in a systematic, thoughtful process that deserves to be called research (Patten 2000). Empirical research can be conducted by using either qualitative or quantitative research methodology (Patten 2000).

Qualitative research is concerned with developing explanations of social phenomena. It aims to help us to understand the social world in which we live and why things are the way they are. It is concerned with the social aspects of our world (Beverly, Ockleford and Windridge 2009). Since the social phenomenon we are studying is Cybersecurity, that influence our life and requires to take more in-depth look at the phenomenon the qualitative research is the

right choice to conduct this research. Through qualitative research method this thesis is going to provide the acceptable empirical evidence about the outcome. Empirical evidence can be defined as data and information gathered by making presumptions about certain topic. Through this evidence it possible to prove or disprove a theory.

Research question plays a huge role in order to conduct any reliable research. Research questions are important because they help the writer to navigate through whole process (Beverly et al. 2009). When the writer can stay consistent with the content of the research, it also helps the reader to keep the focus on the topic. This way the research will be clearer for both parties. In both cases qualitative and quantitative research, the question must be selected in way that it links well with research method (Beverly et al. 2009). The research question is: Do degree graduate's cyber security skills meet the demands of labor market? This research question consists of two variables: Cybersecurity skills and labor market. First variable represents the supply, and second variable represents the demand. To deliver the answer to research question these variables must be analyzed and measured. This can be done by using sub questions. Sub questions are: What cyber skills does degree graduate possess and what type of cyber skills are demanded by labor market?

With the first sub question the idea is to understand the different cybers skills gained from different educational institution. This gives us the supply and better understanding of the pool choice that these organizations have. For example, student from University of Turku and student from University of Jyväskylä might possess different cybersecurity abilities since their curriculums might be different and student has then created different student portfolio with different skills and competences. Thereof their value in labor market might be different, because of the nature of supply and demand. With the second sub question we are trying to understand demand of the labor market. The idea is to find out the most common cybersecurity skills, that different organizations looking to hire a cybersecurity personnel? Screening the demand specifically for cybersecurity helps to distinguish the information security and ICT from cybersecurity skills. After answering to these two sub questions, we have studied the relationship between two main variables and the results should meet each other and give the answer for the main research question.

3.1 Content analysis

According to Klaus Krippendorff (2004) content analysis is method that systematically analyses and makes inferences from qualitative or quantitative data. As research tool the purpose of the content analysis is to enhance the researcher's knowledge about specific subject matter or phenomenon. The framework for the content analysis includes text, research question, context, analytical construct, inferences and validating evidence (Krippendorff 2004).

Content analysis will be applied for first variable, which is cyber skill. The text chosen for this are cybersecurity curriculums. Online certificates and other documents outside of finish degree program will not be part of this research. first sub question “What cyber skills does degree graduate possess” will be used. For the context cybersecurity skills within these curriculums works as acceptable data that is with the context of the cybersecurity skill. Other parts of the curriculum will not be accepted. For analytical construct the chosen data will be categorized for table. The next step is the process drawing inference based on gathered data. Last the validation of the data.

3.2 Thematic analysis

For the second variables the labor market thematic analysis is used as research method. Thematic analysis is used for analyzing qualitative data that entails searching across a data set to identify repeated patterns (Kiger & Varpio 2020). As it was stated in the second chapter the job description might be ambiguous. Most open vacancies are described more on competence based than skill based. It was also stated that competence have broader meaning than skill. This research is trying to find repeated patterns among labor market, in order to understand what the similarities among these different companies have when they are seeking to hire a cybersecurity employee. Since thematic analyze describes a iterative process, it most suitable research tool to answer the second sub question (Kiger & Varpio 2020). The process of thematic analysis includes familiarize yourself with the data, generate initial codes, search for themes, review the themes, defining and naming the themes (Kiger & Vapio).

For labor markets job search engines Oikotie, Duunitori, Linkedin and Monster were used. According to survey by Duunitori (2021) all the four recruiting channels were listed in top six most recruitment channels currently. Instagram and Facebook were not used for privacy reasons in order to not create account for privacy reason. Only the organizations that specifically fulfill cybersecurity related vacancies will be accepted for this research. This can be concluded based on if the heading of the job title or the work description includes cybersecurity,this gives us the codes. This way the possible overlap between ICT and information security can be avoided. Organizations that demanded more than one year of previous experience were also eliminated, based on the definition of recently graduated. Vacancies from all regions are accepted if work is within boarders of Finland. Key word for search engine will be Cybersecurity.

4 Results

There are only five schools that do offer full cybersecurity degree in Finland, University of Turku (Unversity of turku 2021), University of Jyväskylä (University of Jyväskylä 2021) Jyväskylä university of applied science (Jyväskylä university of applied science 2021) , South-Eastern Finland University of Applied Science (Xamk 2021).) Laurea University of applied science (Laurea University of Applied science 2021). Other educational institutions have integrated cyber security as part of the curriculum, which is important because education policy should ensure that there are enough cybersecurity experts from the various training programs (Mattila, Ali-yrkkö and Timo 2020). First there is literary explanation of the curriculums and then Table 1. Wraps up cybersecurity content in more compress form.

In University of Turku cyber security degree is of master's degree programme in faculty of Information and communication technology department. Student can specialize in three different tracks: Cyber security, Smart systems or Cryptography. Cybersecurity track focuses on researching cyber security technologies developed for networked systems and applications of the communication-intensive future. The technological topics covered include security of smart environments, system and network security, security of communication systems and applications, and designing secure systems (Unversity of turku, 2021).

Cybersecurity programme structure consists of: Advance level of studies in major subject (50 ECT), Thematic module or minor subject (20-25 ECT), Elective studies (15-20) and Master of Science in technology thesis (30 ECT). As applicant student is expected to have enough previous degree, which consists relevant studies in the field of information and technology. The relevant studies include Communication and network systems, software engineering, computer science, computer technology, information technology and other relevant fields of studies providing sufficient knowledge of computer network technology, programming and mathematics (Unversity of turku, 2021).

In University of Turku the focus is on information technology part. The technological topics covered include system and network security, security of communication systems and applications, and security in system design. They also have compulsory studies in cryptography and management aspects of cybersecurity. University has strong emphasis on hands-on modules with vendor systems from their partners. University of Turku states the high employment rate for their degree graduates based on students' knowledge in different topical areas in information security and benefits from co-operations with different companies within the region. In 2020 there were 159 mater degree graduates in the field of ICT.

In university of Jyväskylä Cybersecurity degree is master's degree programme in the faculty of Information Technology, which consists of 120 study credits. In order to be eligible to

enroll for this study programme, student must have bachelor's degree on relevant field, such as computer science, military science, security and management administration. (University of Jyväskylä 2021) The programme examines the cyber world and its security from an administrative and technological perspective. The subject content focuses on planning of cyber security, management of it, and management of information security risks from the point of a managerial as well as technological viewpoint. (University of Jyväskylä 2021).

In University of Jyväskylä the cybersecurity master's degree programme has two fields of studies: The field of cybersecurity and the field of general security and strategic intelligence. In the field of cyber security study emphasizes cyber security planning, management and information security risk management from both a management and technology perspective. The field of general security and strategic intelligence study direction of total security and strategic intelligence emphasizes the importance of information management in companies and organizations, as well as the possibilities of information acquisition and intelligence, especially as part of the activities of international organizations (University of Jyväskylä 2021).

Degree programme in Jyväskylä does not demand previous skills on programming. The student with no prior knowledge or skill on programming must take courses on basic knowledge of information technology which consists of 20credits. The field of cybersecurity consists of 20 credits of competence-based studies. These 20 credits are being divided between 10 credits from social deepening (such as cybersecurity psychology, ethic and information technology etc.) and 10 credits from technical deepening (such as secure system design, IOT/embedded security, introductory penetration testing and security assessment etc.) The field of general security and strategic intelligence consists only 10 credits of competence-based study. In this programme the cybersecurity related competence- based studies only include crises and societal change and history of crises and societal changes (University of Jyväskylä 2021) In 2020 University of Jyväskylä had an intake of 186 for master's degree programme in ICT, only 6 were counted as absent (Vipunen Opetushallinnon Tilastopalvelu 2021). Also, in 2020 there were 276 graduates from the same degree programme. In comparison to Turku university, for the field of cybersecurity Jyväskylä is more popular among students.

JAMK (Jyväskylä university of applied science) cybersecurity is bachelors and master's degree as part of ICT engineering studies. In Bachelors student must have 240 ECT at the end of the programme. JAMK ICT programme the student can specialize either in software engineering or in cybersecurity. At the end of the programme the student should be able to understand cyber security management, technical implementation, audit, standardization, and legislation (Jyväskylä university of applied science 2021).

Specialization in cybersecurity at bachelor's level includes 30 credits and each course is 5 credits. These courses are data security controls, cybersecurity management, cyber threat information and data analytics, attacks, defense and protection, hardening, incident management response and SOC. After completing the core competences in cybersecurity, the student should be able to understand the collection, processing and distribution of observational data required in cyber defense. The student knows the processes of cyber defense (Jyväskylän ammattikorkeakoulu 2021). In 2020 JAMK had 108 students graduating on bachelors in the field of ICT and they had student intake of 261.

At Masters level cybersecurity student must complete 60 ECT. The 60 ECT is divided in the core studies (20 credits) and master thesis (30 credits). The core studies or the professional studies includes the following courses: Security management in cyber domain, cybersecurity implementation in practice, Auditing and testing technical security and cyber security exercise. After completing the masters, the student should be able to know how to plan, develop, implement and control different technological solutions in realistic company environments. The student will also learn how to test and audit these solutions. Student has the knowledge and skills to defend cyber security attacks in a realistic environment (Jyväskylä university of applied science 2021)

South-Eastern Finland University of Applied Science (XAMK) also has the bachelors and master's degree programme in cybersecurity. The bachelor's degree is part of the faculty of engineering. Graduate student must complete 240 ECT. XAMK cybersecurity programme is very much a hands-on approach. After completing the studies, student should be familiar with cybersecurity frameworks, standards, security management and can classify the vulnerabilities and the principles of protection. After the studies, students can apply security solutions for discovering security threats and for protecting against them. You are also able to manage countermeasures against denial-of-service attacks.

The curriculum consists of programme-specific core studies 180 ECT, supplementary studies 60ECT. Internship is 30ECT and of bachelor's thesis is 15 ECT. (Kaakkoi- Suomen ammattikorkeakoulu 2021). The competence-based cybersecurity studies include. Applied cybersecurity, Advanced cybersecurity, Secure datacenter technology and Advanced Secure networking). XAMK has also integrated the use of cyberage as part of their educational learning environment. Virtual Lab is a virtual laboratory service running on the cyber lab datacenter. Virtual Lab is widely used in cybersecurity- and information networks education, as well as in RDI activities (Research, Development and Innovation).

XAMK's master's degree programme consist of 60ECT. The core competence studies consist of 25credits. Competence studies are divided into two separate categories, first being Strategic cybersecurity (introduction to cybersecurity, Cybersecurity auditing and cyber hygiene,

Networks and cybersecurity) and Functional cybersecurity (Defensive cybersecurity and offensive cybersecurity). The programme should take about 1,5 years and XAMK only has intake of 25 students. The masters programme also has cyberage as part of educational tool. After completing the master's degree, student should be able to you know the different frameworks for cyber security, standards, information security control and management, and you can classify vulnerabilities and protection principles and protect industrial Internet systems, manage intrusion detection systems, and implement network infrastructure security measures (Kaakkoi- Suomen ammattikorkeakoulu 2021).

Laurea University of applied science has cybersecurity as part of the BIT (Business information technology, Cybersecurity). In this programme you will deepen your expertise in Cybersecurity with business management perspective. Programme content is connected to cybersecurity frameworks provided by the most prominent associations including Comptia, ISC2 and ISACA. Cybersecurity technologies studies consists of 20ECT (Laurea university of applied science 2021).

School	Cybersecurity skills in curriculum
University of Turku	security of smart environments, system and network security, security of communication systems, applications, and designing secure systems
University of Jyväskylä	cybersecurity psychology, ethic and information technology, as secure system design, IOT/embedded security, introductory penetration testing and security assessment
Jyväskylä university of Applied science (Bachelors) (Masters)	cybersecurity psychology, ethic and information technology, as secure system design, IOT/embedded security, introductory penetration testing and security assessment. Security management in cyber domain, cybersecurity implementation in practice, Auditing and testing technical security and cyber security exercise

Southern-Eastern university of applied science (Bachelors) (Masters)	Applied cybersecurity, Advanced cybersecurity, Secure datacenter technology and Advanced Secure networking. Strategic cybersecurity (introduction to cybersecurity, Cybersecurity auditing and cyber hygiene, Networks and cybersecurity) and Functional cybersecurity (Defensive cybersecurity and offensive cybersecurity.
Laurea University of applied science	System security, Network and application security, enterprise security and practitioners and cybersecurity analyst

Table 1: Cybersecurity skills from curriculum

After the time span of 12.8- 13.11 only 21 jobs were found that fit the criteria of recently graduated. All the organizations were ICT companies or consultant companies that offered IT consultant among other services. Trainee programs were the most popular among open vacancies with four different organizations, that offered trainee position for students who were either recently graduated or in final stages in their studies. For these trainee programmes there were no specific skill demands, but student would be given around six-month training time. Some of the trainee programmes informed that salary is included. The experience rose as theme for recruitment search engine. It seemed to be one of the crucial factors in terms of employment. When search was conducted in September through linkedin the difference in cybersecurity jobs was 105 without any filtering, but when entry level filtering was put on search results drop to 32 and out of that 32 only 14 had cybersecurity as title.

Penetration testing was the most demanded skill with four different organizations requiring it. Next came Linux operating systems and Azure cloud computing, with three different organizations requiring from their applicants to know how to use them. Software development was asked twice and ISO security standards 27000 and 27001 were demanded once by two different organizations. The second sub-question has now been answered.

5 Conclusions

School and private institutions must be more actively engaging to one and other. This way the school and institutions, would have a better understanding about current cybersecurity

themes and trends. This would help schools to update their curriculum and possibly give a student a bit heads up about future labor demands. This way the equivalency between labor market and education could be created. Second the government needs to give more funding, so that cybersecurity programmes can have larger intake, but not only for that but for clearly for marketing.

The following conclusions can be derived from this thesis. There is skill gap between labor market skill demand and skills gained through educational institution. We can answer to our research question: Degree graduate's cyber skills do not meet the demand of the labor market. This research also suggests the idea, that regarding the field of cyber security labor market is not saturated. This research acknowledges the existence of cybersecurity skill gap. This presents qualitative or quantitative problem, in terms of does this saturation exist because Finnish educational programs inability to provide the skillful people or does the existing market demand too much, so educational system can't provide for the demand? This thesis argues that Finnish educational system does provide inadequate cybersecurity educatio. Based on these results the argument can be made that for existing cybersecurity curriculums there is no skill equivalency in labor market.

There is consensus in Finland, that the cybersecurity is ever growing field and demand for the cybersecurity experts only increases. With Finlands Greentech ambitions and Finnish government's ever-growing concern of safety of its citizens and its institutions through cybercrimes has demanded lot of governmental initiatives to tackle this. The issue that this thesis presents is that since Finnish educational institutions are almost completely under governments control, but most of the institutions that are seeking to employ these cybersecurity graduates are private. The fact that penetration testing was the single most demanded skill in this research and has been acknowledged in previous studies to be one the most important skill, but only University of Jyväskylä had it in their curriculum. Which now means that student who didn't go to Jyväskylä university has to learning it somewhere else or be trained by hiring institution. Since training is still counted as recruiting costs, it makes more sense for the company to hire a person with already experience or recruit person from competitor.

References

Printed

Aarnio, L. & Suvi, P. 2015. Mitä tarkoittaa "ammatillisen koulutuksen työelämävastaavuus. Helsinki. Opetushallitus

Hancock, B., Windridge, K. & Ockleford, E. 2007. An Introduction to Qualitative Research. East midlands. National institute for health research.

Duunitori. 2021. Kansallinen rekrytointitutkimus: Duunitori Oy. Accessed 10 December 2021

ISACA. 2020. State of cybersecurity survey part 2. Schaumburg: ISACA

Kiger, M. & Varpio, L. 2020. Thematic analysis of qualitative data. Journal of education in medical sciences, 131, 2-10. Accessed 3 December 2021

Krippendorff, K. 2004. Content analysis an introduction to its methodology. Third edition. Los Angeles: Sage

Kinnunen, H. 2002. Population ageing, labor markets and the outlook for public finances. Helsinki: Bank of Finland Economics department.

Lassila, J. & Tarmo, V. 2021. The economic effects of population ageing. Helsinki: Valtioneuvoston selvitys- ja julkaisusarja.

Lehto, M. & Kähkönen, A. 2015. Kyberturvallisuuden kansallinen osaaminen. Jyväskylä: Informaatioteknologian tiedekunnan julkaisuja. Accessed 10 October 2021

Leinonen, K. 2017. Lyhyt Johdatus työnhakuun. Joensuu: University of Eastern Finland.

Liikenne- & viestintä ministeriö & tietoturvallisen liiketoiminnan kehittämisryhmä. 2016. Maailman luotetuinta digitaalista liiketoiminta Suomen tietoturvallisuusstrategia. Helsinki: Liikenne- ja viestintäministeriö.

Mattila, J. Jyrki A. & Seppälä, T. 2020. Kyberuhat yleistyvät- Miten Suomen yritykset pärjäävät? Helsinki: Etla. Accessed 9 September 2021.

Miettinen, R., Lang, T., Leila P., & Kaisa, P. 2021. Euroopan Unionin elinikäisen oppimisen avaintaidot, Eurooppalainen tutkintoviitekehys ja oppilaitosten opetussuunnitelmien kehittäminen. Ammattikasvatuksen aikakauskirja, 23 (2).

Mishra S. & Shahsi, A. 2017. Research methodology handbook. New Delhi: Educreation.

Musset, P. 2015. Building skills for all: A Review of Finland Policy insights on literacy, numeracy and digital skills from the survey of adult skills. OECD.

National institute of Standards and Technology. 2012. Information security. Gaithersburg: Department of Commerce.

Neittaanmäki, M. 2003. Rekrytointipalvelut yritysten verkkosivuilla. Msc. Yhteisöviestintä. Jyväskylän yliopisto.

National institute of standards and technology. 2012. Guide for conducting risk assessment. Gaithersburg: National Institute of Standards and Technology. Accessed 14 September 2021

Niemelä, J. 2019. Kyberturvallisuusalan työvoiman kysyntä, saatavuus ja kehittäminen, vastaamaan työvoiman tarvetta. Msc. Informaatioteknologian tiedekunta Jyväskylän Yliopisto.

Opetushallitus. 2021. Tutkintojen ja viitekehysten osaamiskuvaukset. Accessed 9 September 2021

Patten, M. 2000. Proposing empirical research, a guide to fundamentals. 5th edition. New York: Pyrczak.

Sanou, B. 2017. Global cybersecurity index. Geneve: International Telecommunication Index.

Shahara, S. 2017. Competency-based curriculum. Department of Islamic religious studies.

Teknologiateollisuus. 2018. Teknologiateollisuuden koulutus ja osaaminen-linjaus. Accessed 9 September 2021.

The European Commission. 2017. Resilience, Deterrence and Defense: Building strong cybersecurity for the EU. Brussels: European union.

Turvallisuuskomitea. 2014. kyberturvallisuusstrategian toimeenpano-ohjelma. Helsinki. Accessed 1 December 2021

Turvallisuuskomitea. 2018. Vocabulary of cyber security. Helsinki: Accessed 1 December 202

Wagner, R. 2012. Organizational competence in project management new perspectives on assessing and developing organizations. Journal of Project Program & Portfolio Management, 45-57.

Electronic

Anumala, K. 2019. Skill-building process and strategies for development. Cham: Springer. Accessed 12 November 2021.
https://www.academia.edu/41218841/Skill-Building_Process_and_Strategies_for_Development

Corporate finance institute. 2015. Labor market. Accessed 12 October 2021.
https://corporatefinanceinstitute.com/resources/knowledge/economics/labor-market/

Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiatakis, D., Hernandez Ramos, J., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, S., Neisse, R., Nordvik, J., Papameletiou, D., Reina, V., Ruzzante, G., Sanchez Martin, J., Sportiello, L., Steri, G. and Tirendi, S., Cybersecurity, our digital anchor, Nai Fovino, I., Barry, G., Chaudron, S., Coisel, I., Dewar, M., Junklewitz, H., Kampourakis, G., Kounelis, I., Mortara, B., Nordvik, J. & Sanchez Martin, J. Cybersecurity, our digital anchor. 2020. Luxembourg: Publications Office of the European Union.
JRC Publications Repository - Cybersecurity, our digital anchor (europa.eu)

Dawson, J. Thomson, R. 2018. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Accessed 5 October 2021.
https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00744/full

Echo. 2019. Echo project summary. Accessed 30 August 2021.
Project summary – ECHO Network

Finland. 2009. Yliopistolaki 24.7.2009/558. Accessed 22 September 2021.
Yliopistolaki 558/2009 - Ajantasainen lainsäädäntö - FINLEX ®

Frhulinger, J. 2020. What is information security? Definition, principles, and jobs. Accessed 15 October 2021.
https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

Cambridge English dictionary. 2021. Meaning of prefix in English. Accessed 9 September 2021.
https://dictionary.cambridge.org/dictionary/english/prefix?q=prefix.

Jyväskylän ammattikorkeakoulu. 2021. Become ICT engineer for international tasks. Accessed 21 September 2021.
https://www.jamk.fi/en/Education/Technology-and-Transport/information-and-communication-technology-bachelor-of-engineering/

Kaitala, V. & Kuusi, T. 2021. Vihreistä tuotteista viennin uusi elämä: Elinkeinoelämän tutkimuslaitos. Accessed 21 October 2021.
https://www.etla.fi/ajankohtaista/vihreista-tuotteista-viennin-uusi-veturi/

Laurea University of Applied science. 2021. Degree Programme in Business Information Technology Cyber Security blended learning. Accessed 12. 9 2021.
https://ops.laurea.fi/index.php/en/212701/en/230740/NCA222SA/year/2022

Marquardson, J. & Noshokaty, A. 2019. Skills, Certifications or Degrees: What companies demand for entry level Cybersecurity jobs. Information systems educational journal. Article from ResearchGate. Accessed 20 September 2021.
https://www.researchgate.net/publication/338805856_Skills_Certifications_or_Degrees_What_Companies_Demand_for_Entry-level_Cybersecurity_Jobs

Mclean, R. Shanti, J. & Jouko, S. 2012. Skills development for inclusive and sustainable growth in Developing Asia-Pacific. Accessed 5 October.
https://books.google.fi/books/about/Skills_Development_for_Inclusive_and_Sus.html?id=VNtCDwAAQBAJ&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false

Minna, H. 2021. Maahanmuuttajat me tarvitsemme teitä. Posted 23 September Helsinki, Uusimaa, 23. September. Accessed 2 December 2021
https://teknologiateollisuus.fi/fi/ajankohtaista/maahanmuuttajat-me-tarvitsemme-teita

National initiative for cyber security studies and careers. 2021. Accessed 8 September 2021
https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

Nieminen, J. 2020. Työ- ja elinkeinoministeriön julkaisuja. Alueelliset kehitysnäkymät syksyllä 2020. Accessed 19 Novemeber 2021.
https://julkaisut.valtioneuvosto.fi/handle/10024/162491

Opetushallitus. 2021. Elinikäisen oppimisien avaintaidot. Accessed 9 September 2021
https://www.oph.fi/fi/koulutus-ja-tutkinnot/elinikaisen-oppimisen-avaintaidot

Opetushallitus. 2021. Finnish education in nutshell. Accessed 9 September 2021
https://www.oph.fi/sites/default/files/documents/finnish_education_in_a_nutshell.pdf

Opetus- ja Kulttuuriministeriö. 2021. Tutkintojen viitekehys. 10 September 2021
https://okm.fi/tutkintojen-viitekehys

Sillanpää, A. 2020. Kyberosaamistarpeet. Helsinki: Liikenne-ja Viestintäministeriö. Accessed 1 december 2021

https://api.hankeikkuna.fi/asiakirjat/164ec5f9-d5a8-4d1b-9bf6-05e6470daab5/a40f74fd-b8f3-4bb7-a829-242de5732fb0/RAPORTTI_20210204085928.pdf.

Swedish International development cooperation agency. 2018. Skills Development. Accessed 7 October 2021
https://cdn.sida.se/publications/files/sida62134en-skills-development.pdf

Teknologiateollisuus. 2020. Teknologiateollisuus pystyy vähentämään päästöjä. Accessed 9 September 2021.
https://teknologiateollisuus.fi/fi/ajankohtaista/tiedote/tiekartta-valmistui-teknologiateollisuus-pystyy-vahentamaan-paastoja

Tilastokeskus.2021. Käsitteet: Tilastokeskus. Accessed 24 October 2021
https://www.stat.fi/meta/kas/informaatiosekt.html#tab1

Tilastokoulu. 2021. accessed 14 October 2021
https://tilastokoulu.stat.fi/verkkokoulu_v2.xql?page_type=sisalto&course_id=tkoulu_tmt&lesson_id=1&subject_id=1

Tilastokeskus. 2021. Vastavalmistuneiden työllisyys parani edelleen. Accessed 21 October 2021
https://www.stat.fi/til/sijk/2018/sijk_2018_2020-01-23_tie_001_fi.html

UNESCO. 2021. European community's memorandum life learning issued. 9 September 2021
https://uil.unesco.org/document/european-communities-memorandum-lifelong-learning-issued-2000

University of Jyväskylä. 2021. Kyberturvallisuus. Accessed 21 September 2021
https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus

University of Turku. 2021. Master's degree programme in information and communication technology cybersecurity. Accessed 21 September 2021
https://www.utu.fi/en/study-at-utu/masters-degree-programme-in-information-and-communication-technology-cyber-security

Valtioneuvosto ja ministeriöt. 2021. Henkilöstösuunnittelu. Accessed 21 October 2021
https://vm.fi/valtio-tyonantajana/henkilostojohtamisen-tuki/henkilostosuunnittelu

Vipunen Opetushallinnon Tilastopalvelu. 2021. Opiskelijat ja tutkinnot. Accessed 10 October 2021
https://vipunen.fi/fi-fi/yliopisto/Sivut/Opiskelijat-ja-tutkinnot.aspx

Xamk. 2021. Opinto opas. Accessed 21 September 2021
https://opinto-opas.xamk.fi/index.php/en/28/en/188666

XAMk Kaakkois- Suomen ammattikorkeakoulu. 2021. Opinto-opas. Accessed 11 October 2021
https://opinto-opas.xamk.fi/index.php/en/28/en/188666

Appendices

Appendix 1: Recruitment results

	Company	Position	Skill demanded
17.9	ElfGroup	Penetration tester	penetration testing experience, know
	Loihde trust	Junior cyber security analysist	Linux,Windows, macos, IOS, Android
11.8	Innofactor	Konsultant	Cloudservice, ISO 27000, related stu
1.11	HoxHunt	Junior threat analyst	Growing intrest on cyber security
30.8	EY	Trainee	Vastaavan alan koulutus
5.1	Insta	Trainee	Vastaavan alan koulutus
5.1	Movial	Senior cyber security specialist	Software skill developer, with experie
3.11	Netum	Kyberturvallisuuskonsultti	Web sovellukset, penetration testing,
1.9	KPMG	Trainee techGURU	Vastaavan alan koulutus
14.8	Insta	trainee	Vastaavan alan koulutus
9.8	Accenture	Cyber security	Vastaavan alan koulutus
6.11	Ahlstrom-Munksjö	Cyber security specialist	
17.8	2ns	Cyber security	Iso 27001, Vahti,Katari,Pitukri,NIST ja
28.8	Deloitte	Cyber risk trainee	Vastaavan alan koulutus
1.11	Accenture	SOC analyser	Vastaavan alan koulutus, basic know
26.1	s4access	SAP-information security consult	Hyvä exel, IT alan koulutusohjelma
9.8	Innofactor	Cyber security consultant	Cloudservice, Azure, Azure, M365, Pe
11.11	Istekk	Consultant	Vastaava kolutus
27.1	ABB	IT and Cyber security specialist	Acronis, Veeam, Quest preferable, sc
7.1	Insta DefSec	Testing	Penetration testing, Linux, nettechnol
4.11	Elektrobit	Cyber security analyst	Cybersecurity standards and regulati

Appendix 2: The title of the second appendix