

This is an electronic reprint of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version: Frisk, I. ; Ruoslahti, H. & Tikanmäki, I. (2023) Cybersecurity Through Thesis in Laurea University of Applied Sciences . Proceedings of the 22nd European Conference on Cyber Warfare and Security. Vol. 22 No. 1., 484-492.

doi: 10.34190/eccws.22.1.1447

Available at: <https://doi.org/10.34190/eccws.22.1.1447>

[CC BY-NC-ND 4.0](#)

Cybersecurity Through Thesis in Laurea University of Applied Sciences

Ilona Frisk¹, Harri Ruoslahti¹ ¹ and Ilkka Tikanmäki^{1, 2} ²

¹*Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland*

²*Department of Warfare, National Defence University, Helsinki, Finland*

Ilona.frisk@laurea.fi

Harri.ruoslahti@laurea.fi

Ilkka.tikanmaki@laurea.fi


Abstract: Information technology and its applications surround us and those have become crucial to our lives. However, the understanding of the digital world is not as strong. Successful and functional cybersecurity is a vital component for the defence of a civilised society. This study looks at how cybersecurity has been handled in theses written at one University of Applied Sciences and what kind of topics have been chosen by thesis writers, and what is written about cybersecurity in them to understand how cybersecurity is seen in higher education. The goal of this paper was to find out how cybersecurity has been handled in theses and what kind of topics have been chosen by thesis writers. The two research questions are: what theses have been published that handle cybersecurity; and how does cybersecurity in them? As typical of a case study, attention is paid to a small number of cases (n = 15) attempting to describe the phenomenon they represent. Of the fifteen theses, two were master's and thirteen bachelor's theses, and mostly completed in Safety, Security and Risk Management, Security Management, and Business information technology programmes. Based on the results in this case, cyber security is being examined or developed from several, different points of view and in multidisciplinary ways.


Keywords: Cybersecurity, comprehensive security, cybercrime, resilience

1. Introduction

Information technology and its applications surround us in today's world. These have become very important for our work and civilian lives, and we have become increasingly dependent on them (Shoemaker and Conklin, 2011). However, this does not mean that our understanding of the digital world is strong, but quite the opposite there is a recognized gap in understanding what cybersecurity is and what affects it, despite efforts to increase overall security. Functional and successful cybersecurity is a vital component in the defence of civil society and its organizations, and each individual is part of a community and of society, and part of this defence which is why it is important to understand what cybersecurity is (Bowden, 2010, p. 16; Burgess, 2010; Limnéll, Majewski and Salminen, 2014).

Project Dynamic Resilience Assessment Method including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO) builds on the work of European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) to understand the role of e-skills in society within the societal impacts of project outcomes and cyber security.

¹  <https://orcid.org/0000-0001-9726-7956>

²  <https://orcid.org/0000-0001-8950-5221>

To understand how cybersecurity is visible in the context of higher education, as seen by soon to graduate future work life experts this study looks at how cybersecurity has been investigated in theses written at Laurea University of Applied Sciences (UAS), and what topics the authors of these theses have chosen. Laurea graduated some 800 bachelor's and master's students in 2021, from 43 degree programs fields ranging from social services and nursing to business and administration, security and risk management, and business information technology, which are most likely to choose cyber security topics (Laurea University of Applied Sciences, 2022). All Laurea graduates can select an interesting and relevant topic of study or development on which they are, as part of their degree, publish a thesis report. This study examines the theses published in 2021 and beginning of 2022 to understand how cybersecurity is seen in higher education, by looking at how they write about cybersecurity.

The research questions (RQ) of this study are:

RQ1: What published theses are on cybersecurity?

RQ2: How does cybersecurity appear in them?

2. Cybersecurity

The importance of the cyberworld makes cybersecurity a topical issue it is, however, not clear to everyone what cybersecurity stands for. Based on the literature examined, it appears that little research has been done on what topics are studied at higher education institutions (HEI). This section provides an overview on the literature on cybersecurity.

Several studies in scholarly literature find that cybersecurity is multidisciplinary and containing concepts from several fields (Craig, Diakun-Thibault and Purse, 2014) e.g., business management, behavioural studies, and technical and software engineering (Shoemaker and Conklin, 2011). The first part *cyber* is used as a prefix referring to the digital world of bytes (Limnell, Majewski and Salminen, 2014). It originates from the word *cybernetics*, which is the study of computers and automation systems communications, and simultaneously used with the concept *cyberspace*, a virtual and intangible space that exists by merging a variety of electronic communication systems and networks in an electronic space that is not part of the known and seen physical space; *cyberspace* is however, bound by physical elements and cannot exist without wires, cables or electromagnetic waves (Cavelty, 2010).

The dictionary defines the second part *security* as being safe and protected from danger and threats or measures used to accomplish that state (Lexico, 2022) One definition for cybersecurity is provided by (Craig, Diakun-Thibault and Purse, 2014, p. 17) as “organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign property rights”. Literature recognizes multiple definitions of cybersecurity, the definitions by e.g., (Cybersecurity and Infrastructure Security Agency (CISA), 2019), (Kaspersky, 2022), (National Cyber Security Centre, 2022) all look at cybersecurity being the protection of computers, devices, and services.

Cybersecurity is needed to make the virtual world secure and safe; cybersecurity can be seen as the use of technology and legislation to protect and manage information (Ruoslahti and Tikanmäki, 2022); or processes and measures to protect cyberspace and its systems and other physical aspects, devices and software from possible threats (Craig, Diakun-Thibault and Purse, 2014). There are similarities between information security and cybersecurity as both of their measures have three goals: to protect the confidentiality, integrity, and availability of information (Cavelty, 2010). It is not possible to separate between the physical and the virtual or digital elements of cybersecurity, as cyber events can have physical consequences and tangible effects even though cyberspace in itself is intangible (Shoemaker and Conklin, 2011; Limnell, Majewski and Salminen, 2014). Cybersecurity and security in general should be embedded as a solid part of all organizational processes so that security dimensions are considered in all actions and operations from the very beginning, not only when a new digital service is otherwise ready to be implemented (Limnell, Majewski and Salminen, 2014).

Cybersecurity needs to be consistent and continuous process because cyber threats and vulnerabilities are constantly new and emerging (Cavelty, 2010). Threats will continue to exist, and therefore cybersecurity measures are forever needed, as the goal of cybersecurity is to protect applications and cyberspace from various threats that could compromise its safety (Craig, Diakun-Thibault and Purse, 2014). Besides a technical issue, cybersecurity is mostly a strategic and political, with situational awareness, defined direction and guidelines in both organizations and society; making cybersecurity part of comprehensive security that belongs to all of us (Limnell, Majewski and Salminen, 2014). On a larger scale cybersecurity is close to national security, the differences are in the actors, scope, and funding, which both aim to create conditions that are free from either imagined or existing danger (Cavelty, 2010).

One internationally recognized threat to cybersecurity is cybercrime (Mohammed, 2015). The number of crimes and costs caused by cybercrime have been continuously increasing since their first appearance since personal computers became popular in the 1970's and 1980's. In the early stages, cybercrimes were divided in those threatening businesses and those affecting in national security (Cavelty, 2010), but modern definitions of cybercrime involve all illegal and criminal acts against computer data, systems, as well as unauthorized access, modification or impairment of digital or computer systems, which do not have geographical boundaries and only leave digital traces (Mohammed, 2015; Payne, 2020).

Besides its many risks and threats, the cyberworld provides organizations and businesses many new opportunities to grow and add value, so decision makers especially need updated knowledge and up-to-date situational information to build stability between threats and opportunities within this cyberspace all-around us (Limnell, Majewski and Salminen, 2014). Information and communications technology (ICT) is important in building organizational competitiveness (Mihalic and Buhalis, 2013) by promoting productivity and

competitiveness with the generation of knowledge, processing information, and organizational learning (Hortovanyi and Ferincz, 2015). Knowledge transfers can become promoted through ICT skills of the members of the organization (Salleh *et al.*, 2012), because knowledge flows and organizational learning can be enhanced with ICT (Škerlavaj, Dimovski and Desouza, 2010; Zhao and Kemp, 2013).

ICT skills can be upgraded to the use of the various Knowledge Management (KM) technologies and ICT tools needed to transfer and share information within and outside the organization by proper ICT trainings (Conkova, 2013; Isidro-Filho *et al.*, 2013). Building skills and competences are constructive processes that use and recognize previously adopted competences of learners, and aim at helping them better navigate the cyber domain (Aaltola and Taitto, 2019). When having appropriate ICT knowledge, workers can capture, store and share organizational knowledge that makes their expertise better available to the organization, its network and the surrounding society (Im, Porumbescu and Lee, 2013), and organizations can develop the skills needed to absorb state-of-the-art knowledge from external sources (Cupiał *et al.*, 2018).

3. Methodology

This paper presents a multiple case study. Case studies usually concentrate on one or some cases that are related to each other. This study considered cybersecurity themed theses published at Laurea University of Applied Sciences as cases (Hirsjärvi *et al.*, 2000) to understand how cybersecurity has been investigated in them, and what topics have been chosen by their authors. Laurea students may select an interesting topic of study or development that has work life relevance. This can be done based on their knowledge, taught courses, proposed by teachers, Laurea research and development projects, authority organizations, or private companies.

The first stage of purposeful sampling used in this case study (Merriam and Tisdell, 2015) was to search theses from Theseus, the common database of Finnish universities of applied sciences, where abstracts, bibliographic information, and full texts of the theses are publicly available. The search included theses written at Laurea during a set period of time in Finnish and English. The theses were searched from the database with search terms *cybersecurity* and its Finnish translation *kyberturvallisuus* appearing in either the main title, abstract or as a keyword.

Theses between 1.1.2021 and the day of the search 21.4.2022 were included, with an initial result of 52 theses that were organized according to their publication dates. Next, inclusion criteria that at least one search term or part of it be included in either the main title, abstract or keywords, were applied rendering 37 thesis reports that did not meet the criteria. Thus, fifteen thesis reports qualified for the final sample.

The qualitative analysis of the collected data included reading their full texts to examine how cybersecurity is investigated in each of these 15 theses. Common themes or categories that could be recognized were identified, as finding common themes or categories and building larger entities out of them to be able to describe the phenomenon of interest is typical to qualitative data-analysis (Merriam and Tisdell, 2015), which was deemed a suitable method to find answers to the research questions. The constructed themes are presented in the following Results section to explain how cybersecurity appears in the Laurea case theses.

4. Results

Out of the fifteen theses selected to the sample, two were master's theses and thirteen bachelor's theses. The 13 bachelor's degree programme theses include seven from Safety, Security and Risk Management or its former curricula Security Management, and six from Business Information Technology. The two master's programme theses are from the Business Administration and Innovative Digital Services of the Future programmes. The included thesis projects were all commissioned, by private organizations, Laurea research, development, and innovation (RDI) projects, or state authorities.

Three of the sample theses are in some aspect related to the develop resilience and business continuity aiming. Four of the examined reports had technical foci and aimed to develop case organizations' activities and abilities to respond to future developments. The sample theses became sorted into seven categories according to their themes as shown in Figure 1.

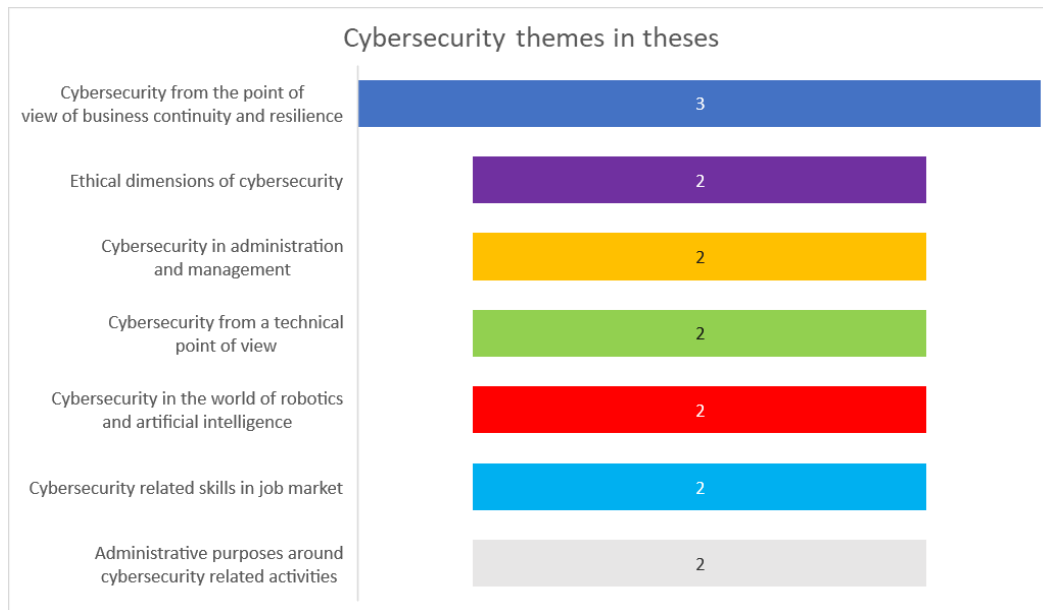


Figure 1. Seven themes identified from the theses.

These themes identified from these theses contain three theses in one category and two theses all the others. This Results section is structured according to these themes: Cybersecurity from the point of view of business continuity and resilience, Ethical dimensions of cybersecurity, Cybersecurity in administration and management, Cybersecurity from a technical point of view, Cybersecurity in the world of robotics and artificial intelligence, Cybersecurity related skills in job market, and administrative purposes around cybersecurity related activities.

4.1 Cybersecurity from the point of view of business continuity and resilience

The biggest category, with three theses, is on the theme of Cybersecurity from the point of view of business continuity and resilience, an IT security audit, a cybersecurity plan for the case company, and the protection of information assets.

(Reinikka, 2021) conducts an IT security audit on the office systems of a paper mill; a case study about an audit performed together with their partner organization following the framework provided by the Center of Internet Security (CIS) called CIS RAM (Risk Assessment Method). This framework is used to evaluate possibilities and impacts of vulnerabilities and threats identified in the risk assessment of the mill office systems.

(Gamoulos, 2021) executes a development project which creates a cybersecurity plan for the case company, a multimedia company that offers expertise and services that focus on website development, digital marketing, and video and film production. Interviews, a workshop, and risk assessment tools are used to collect data, and to put together a cybersecurity plan introducing e.g., the NIST framework, which is a voluntary framework of standards, guidelines, and best practices to manage cybersecurity risk.

(Koivuniemi, 2022) views in a research-based development project what cybersecurity is needed to protect the information assets of the commissioning organization. The main goal in the thesis is to increase resilience in the commissioning organization.

4.2 Ethical dimensions of cybersecurity

Two theses are on the theme exploring the ethical dimensions of cybersecurity. One thesis examines the contradictory values between biomedical and informational technology ethics, and the other offers guidelines for cybersecurity from the perspective of biomedical ethics.

(Kaukonen, 2021) as part of research, development, and innovation (RDI) activities of Laurea, generates enriched information for a project examining contradictory in values between biomedical ethics and informational technology, according to the principles of the project, by interviews of a sample limited to elderly people.

(Hämäläinen, 2021) provides guidelines from a cybersecurity and biomedical ethics perspective to his commissioning project SHAPES, as part of Laurea RDI activities, utilizing Hevner's Design Science Research model in his work and results with respond to ethical questions related to privacy, autonomy, consent, and beneficence where ethical decision-making is required.

4.3 Cybersecurity in administration and management

There are two theses that investigate cybersecurity in administration and management. One thesis looks at administrative level process description of cyber situational awareness (CSA), and the other how to design and implement convergence for cybersecurity and physical security in railway operations.

(Hedeman, 2022) explores cybersecurity situational awareness. The results of the thesis show a difference between situational awareness and situational understanding. The main goal is to put together an administrative level process description of cyber situational awareness (CSA) for the commissioner of the thesis.

(Pacelli Queiroz Felix and Yusuf, 2021) conclude that designing and implementing cybersecurity and physical security convergence in railway operations. Core areas such as people, process, and technology, must be seamlessly integrated, suggesting that converging the physical and cybersecurity departments can improve the risk management ability and enhance the security and safety of the railway operations of their commissioning organization and its members.

4.4 Cybersecurity from a technical point of view

Two theses look at cybersecurity from a technical point of view. One thesis examines Internet of Things (IoT), and the other investigates information security threats e.g., cyberattacks and cyberthreats.

(Laiso, 2021) examines the Internet of Things (IoT) by conducting a content analysis literature related to the cyber security of IoT devices, open interviews with manufacturers, and a review of the cyber security materials produced by these manufacturers, highlighting the differences in levels of cyber security between different device types and manufacturers, and also showing connections between low price and low level of cybersecurity, and company size and capability of cybersecurity documentation.

The thesis by (Syrjälä, 2021) approaches the cyberworld through information security using search words that address information security threats, such as cyberattacks and cyberthreats. The main goal of the thesis is to produce useful information about information security threats of IP cameras, and so its aims are technical in nature.

4.5 Cybersecurity in the world of robotics and artificial intelligence

Two theses fall under the category of cybersecurity in the world of robotics and artificial intelligence. These two theses investigate how artificial intelligence and robotics can assist leadership the financial sector, and the cybersecurity of care robots in the fields of physical and mental care. New future risks are to be expected.

(Anttila and Rantanen, 2021) concentrate on how artificial intelligence and robotics can assist leadership. The thesis views cybersecurity from the point of view of what skills are needed in future management and leadership in the financial sector by performing qualitative research with data collection through interviews and offering a model profile for leadership in the financial sector, with an overview of the effects of digitalization on Finland's financial sector.

(Järvinen, 2021) examines cybersecurity of care robots in the fields of physical and mental care. The study shows how cybersecurity threats are associated with the same risks and threats as the use of other IT devices and robots. The results, however, also address the underlying human factors behind cybercrime, and showing that potential threats are remote access of care robots, espionage, and eavesdropping through network connectivity; new risks by artificial intelligence and machine learning are expected in the future.

4.6 Cybersecurity related skills in job market

Two theses address cybersecurity related skills in the job market. One of these studies shows a possible gap between what skills are provided by Finnish higher education providers and what Finland's work life is looking for, while the other analyses what are the most desirable skills for cybersecurity on the Irish job market.

(Luoma, 2021) uses qualitative research to analyse how cybersecurity skills gained from degree programmes relate on the Finnish labour market. The thesis analyses job advertisements that are published in different forums and compares the skills found in them with different the learning objectives of Finnish higher education degree programmes. The results show that there is a possible gap between what the education provides and what the working life is looking for.

(Walsh, 2021) analyses what are the most desirable skills for cybersecurity on the Irish job market. Relevant cybersecurity skills are divided into four categories: technical, situational awareness, problem solving, and sector specific skills. Results indicate that technical skills are the most descriptive, while sector specific skills are the most infrequently asked. This case study enriches to the larger body of knowledge of the research project ECHO funded by the European commission.

4.7 Administrative purposes around cybersecurity related activities

Two studies examine cybersecurity from the perspective of administrative purposes around cybersecurity related activities. Both works enrichen the body of knowledge of the project ECHO as they look at Share Point portal models that could be used for data and information governance of the future ECHO network.

The study by (Lötjönen, 2021) promotes two possible models for a Share Point portal that could be used for data and information governance purposes for the ECHO network future organization. The aim to identify how to organize information governance in the cybersecurity network enriches the body of knowledge of the project ECHO project.

The thesis study by (Koskula, 2021) covers project administration related information systems and examines possible uses of SharePoint in that connection. The connection to cybersecurity is that it too enriches the body of knowledge of the project ECHO.

5. Conclusions

Based on the results of this case study cybersecurity is a topic that is being examined and/or developed in the theses written at Laurea University of Applied Sciences. The theme is discussed from several points of view and in multidisciplinary ways. The size of theme-based categories that can be recognized remains small during the sample period of this study. The theme-based categories show that the points of view that these thesis writers have taken towards cybersecurity vary significantly. The themes and their key features are presented in Table 1. This review mostly reflects interests of the students, but also the requirements of work life from industry, civil service, or Laurea RDI activities. This study helps understand what cybersecurity topics need to be addressed on in the classroom and to guide the selection of future thesis topics. This is a contribution to the scientific community and can be applied in other HEIs. The contribution to theory is a deeper understanding of how cybersecurity is seen in higher education.

Cybersecurity literature indicates that cybersecurity is everyone's concern and a topical issue, so it was expected to show in higher numbers of cybersecurity related thesis topics. However, after the search and looking into the theses found, it was somewhat surprising that not more theses would mention cybersecurity as a key concept or main field of interest.

Table 1. Cybersecurity themes and their key features

Cybersecurity theme	Key features
Cybersecurity from the point of view of business continuity and resilience	Risk management Continuity planning Asset protection
Cybersecurity in administration and management	Situational awareness Cybersecurity of processes
Ethical dimensions of cybersecurity	Ethically sustainable applications and cybersecurity solutions
Cybersecurity from a technical point of view	Internet of Things Network security Hardware and software security
Cybersecurity in the world of robotics and artificial intelligence	Artificial intelligence Robotics
Cybersecurity related skills in job market	Labour market requirements
Administrative purposes around cybersecurity related activities	Cybersecurity as a business or field of interest

It could be interesting to explore the theses that were excluded in this study to better understand why they appeared in the search. Reasons may vary and some of them may have appeared because they state that cybersecurity is excluded from the scope of their investigation. Many reports seem to have handled information security, and it would be especially interesting to see how they have defined the concept information security and what from their aspect is the role or definition of cybersecurity, and why it did not appear in their abstracts. This raises the question how well the concept cybersecurity is understood among higher education students.

Based on the findings, cybersecurity can be seen as a safe barrier around an organization's most valuable assets. When well organized and widely applied, cybersecurity measures may enhance business continuity. Figure 2 shows how cybersecurity could be seen as a circle around business continuity, which, according to literature, is a main target for every organization.

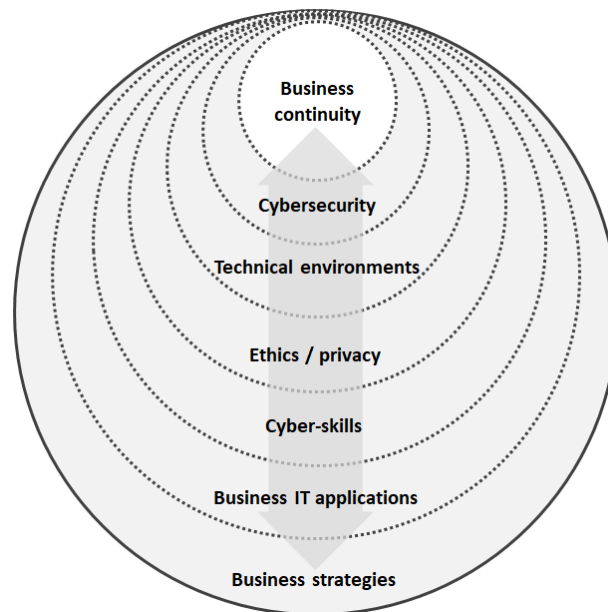


Figure 2. Model of the dimensions of cybersecurity.

As seen in Figure 2, the themes that were identified from the sample of this study recognize some dimensions of cybersecurity. Mainly, cybersecurity seems to be an essential support for business continuity. Secondly, comprehensive cybersecurity builds on appropriate cyber-skill levels and well working reliable technical environments. Neither of these alone provide security, they are needed together, and technical environments should be configured and used in ethical ways to ensure privacy when using business-IT applications. Cybersecurity becomes visible through business IT applications, which are cyber-physical in nature as they contain both digital and physical elements.

The model in Figure 2 also indicates that cybersecurity measures support business strategies by promoting business continuity, when applied throughout the entire organization and its processes. As some measures can increase the protection of some assets, they may at the same time cause harm to other assets or values, which need to be protected and the measures need to be in the right relation to the risks that they are planned to protect from.

It becomes essential to first expose any planned applications to the critical ethical discussion, before applying cybersecurity measures or solutions into the activities and processes of the organization. These ethical discussions should continue throughout organizational processes ongoingly also after the implementation of the applications and their cybersecurity measures.

Acknowledgements

This work was supported by the DYNAMO project, which has received funding from European Union's Horizon Europe research and innovation funding programme under the grant agreement no. 101069601.

References

- Aaltola, K. and Taitto, P. (2019) 'Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training', *Information & Security: An International Journal*, 43(2), pp. 123–133. doi: 10.11610/isij.4311.
- Anttila, A. and Rantanen, P. (2021) *Robotti digityön pomona : tekoäly ja robotiikka johtamisen apuna finanssialan työn murroksessa*. Available at: <http://www.theseus.fi/handle/10024/502387> (Accessed: 17 February 2023).
- Bowden, M. (2010) 'The Enemy Within', *The Atlantic*, 305(5), p. 14.
- Burgess, J. P. (2010) *Handbook of New Security Studies*. Routledge.
- Cavelty, M. D. (2010) 'Cyber-Security', in *The Routledge Handbook of New Security Studies*. 1st edn. London: Routledge, p. 328.
- Conkova, M. (2013) 'Analysis of Perceptions of Conventional and E-Learning Education in Corporate Training', *Journal of Competitiveness*, 5(4), pp. 73–97. doi: 10.7441/joc.2013.04.05.
- Craig, D., Diakun-Thibault, N. and Purse, R. (2014) 'Defining Cybersecurity', *Technology Innovation Management Review*, 4(10), pp. 13–21.
- Cupiał, M. et al. (2018) 'Information technology tools in corporate knowledge management', *Ekonomia i Prawo. Economics and Law*, 17(1), pp. 5–15.
- Cybersecurity and Infrastructure Security Agency (CISA) (2019) *What is Cybersecurity?* Available at: <https://www.cisa.gov/uscert/ncas/tips/ST04-001> (Accessed: 25 November 2022).
- Gamoulos, C. (2021) *Developing a cybersecurity plan for the websites of case company X*. Bachelor's Thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/512312> (Accessed: 17 February 2023).
- Hämäläinen, H. (2021) *Ethics of Cybersecurity and Biomedical Ethics – Providing Ethical Guidelines for the SHAPES Project*. Master's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/500513> (Accessed: 17 February 2023).
- Hedeman, E. (2022) *Kybertilannekuva valtioneuvoston kansliassa*. Bachelor's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/722709> (Accessed: 17 February 2023).
- Hirsjärvi, S. et al. (2000) *Tutki ja kirjoita*. 6. uud. laitos. Helsinki: Tammi.
- Hortovanyi, L. and Ferincz, A. (2015) 'The impact of ICT on learning on-the-job', *The Learning Organization*, 22(1), pp. 2–13. doi: 10.1108/TLO-06-2014-0032.
- Im, T., Porumbescu, G. and Lee, H. (2013) 'ICT as a Buffer to Change', *Public Performance & Management Review*, 36(3), pp. 436–455. doi: 10.2753/PMR1530-9576360303.
- Isidro-Filho, A. et al. (2013) 'Workplace learning strategies and professional competencies in innovation contexts in Brazilian hospitals', *BAR - Brazilian Administration Review*, 10(2), pp. 121–134. doi: 10.1590/S1807-76922013000200002.
- Järvinen, M. (2021) *Hoivarobottien kyberturvauhkien kartoitus hoivarobottiikan asiantuntijoiden näkökulmasta*. Bachelor's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/510631> (Accessed: 17 February 2023).
- Kaspersky (2022) *What is Cyber Security?*, www.kaspersky.com. Available at: <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security> (Accessed: 25 November 2022).
- Kaukonen, H. (2021) *Kyberturvallisuuden eettiset ulottuvuudet SHAPES-hankkeessa*. Bachelor's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/426748> (Accessed: 17 February 2023).
- Koivuniemi, M. (2022) *Jatkuvuudenhallinnan toimintamallin kehittäminen*. Bachelor's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/743772> (Accessed: 17 February 2023).
- Koskula, S. (2021) *ECHO hallinto- ja johtamisen tietojärjestelmän kehitys ja SharePointin käytön tutkinta*. Bachelor's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/511346> (Accessed: 17 February 2023).
- Laiso, M. (2021) *Toimintamalli turvateknisten IoT-laitteiden kyberturvallisuustason arviointiin laite- ja järjestelmäsentajille*. Master's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/500442> (Accessed: 17 February 2023).
- Laurea University of Applied Sciences (2022) 'Laurean strategiset mittarit', *Organisaation johtaminen ja kehittäminen*. Available at: https://laureaas.sharepoint.com/sites/staffFin_johtaminenjakehittaminen/SitePages/koulutuksen%20strategiset%20mittarit%20-%20osa%201.aspx (Accessed: 30 May 2022).
- Lexico (2022) *Definition of security*, www.dictionary.com. Available at: <https://www.dictionary.com/browse/security> (Accessed: 30 May 2022).
- Limnell, J., Majewski, K. and Salminen, M. (2014) *Kyberturvallisuus*. Jyväskylä: Docendo.
- Lötjönen, L. (2021) *SharePoint portaali tukemaan ECHO-verkoston strategisen suunnittelun prosessia*. Bachelor's Thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/503346> (Accessed: 17 February 2023).
- Luoma, S. (2021) *Cybersecurity skill development through degree programme relative to labor market*. Bachelor's thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/512744> (Accessed: 17 February 2023).
- Merriam, S. B. and Tisdell, E. J. (2015) *Qualitative Research: A Guide to Design and Implementation*. 4th edn. San Francisco: John Wiley & Sons.
- Mihalic, T. and Buhalis, D. (2013) 'ICT as a new competitive advantage factor – case of small transitional hotel sector', *Economic and Business Review*, 15(1), pp. 33–56.
- Mohammed, S. (2015) 'An Introduction to Digital Crimes', *International Journal in Foundations of Computer Science & Technology*, 5(3), pp. 13–24. doi: 10.5121/ijfcs.2015.5302.

- National Cyber Security Centre (2022) *cybersecurity - Glossary | CSRC, Cybersecurity*. Available at: <https://csrc.nist.gov/glossary/term/cybersecurity> (Accessed: 25 November 2022).
- Pacelli Queiroz Felix, W. and Yusuf, H. M. (2021) *Measures needed to integrate physical and cyber security in railways infrastructure : organization X case study*. Bachelor's Thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/510112> (Accessed: 17 February 2023).
- Payne, B. K. (2020) 'Defining Cybercrime', in Holt, T. J. and Bossler, A. M. (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham: Springer International Publishing, pp. 3–25. doi: 10.1007/978-3-319-78440-3_1.
- Reinikka, M. (2021) *An Information security audit for a Finnish paper mill*. Bachelor's Thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/496026> (Accessed: 17 February 2023).
- Ruoslahti, H. and Tikanmäki, I. (2022) 'Cybersecurity in Skills Development and Leadership', in *Future-proof Business - System Leadership Competences. 3UAS: Future-proof Business - System Leadership Competences*, Virtual conference.
- Salleh, K. et al. (2012) 'Learning and knowledge transfer performance among public sector accountants: an empirical survey', *Knowledge Management Research & Practice*, 10(2), pp. 164–174.
- Shoemaker, D. and Conklin, W. A. (2011) *Cybersecurity: The Essential Body of Knowledge*. Boston, MA: Cengage Learning.
- Škerlavaj, M., Dimovski, V. and Desouza, K. C. (2010) 'Patterns and structures of intra-organizational learning networks within a knowledge-intensive organization', *Journal of Information Technology*, 25(2), pp. 189–204. doi: 10.1057/jit.2010.3.
- Syrjälä, T. (2021) *IP-valvontakameroiden tietoturvallisuus*. Available at: <http://www.theseus.fi/handle/10024/466707> (Accessed: 17 February 2023).
- Walsh, B. (2021) *Cyber security skill requirements from the Irish job market*. Bachelor's Thesis. Laurea UAS. Available at: <http://www.theseus.fi/handle/10024/512741> (Accessed: 8 June 2022).
- Zhao, F. and Kemp, L. (2013) 'Exploring individual, social and organisational effects on Web 2.0-based workplace learning: a research agenda for a systematic approach', *Research in Learning Technology*, 21. doi: 10.3402/rlt.v21i0.19089.