Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen nykytila ja kehittämistarpeet

Integratiivinen kirjallisuuskatsaus

Tanja Bhaskar

Opinnäytetyö, ylempi AMK
Toukokuu 2025
Projektijohtamisen tutkinto-ohjelma YAMK, Sosiaali- ja terveysala

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Bhaskar Tanja

Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen nykytila ja kehittämistarpeet. Integratiivinen kirjallisuuskatsaus

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2025, 69 sivua

Projektijohtamisen tutkinto-ohjelma YAMK, Sosiaali- ja terveysala. Opinnäytetyö ylempi AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Teknologian vauhdikas kehitys ja digitalisaatio ovat muokanneet sosiaali- ja terveydenhuollon palveluita merkittävästi viime vuosikymmeninä. Työelämän muutoksen myötä digitaalinen osaaminen ja kyberturvallisuuden hallinta ovat nousseet keskeiseen rooliin toimialan henkilöstön päivittäisessä toiminnassa. Opinnäytetyön tarkoituksena oli tutkia sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamista käsittelevän kirjallisuuden avulla.

Kyberrikollisuuden kohdistuessa aikaisempaa enemmän terveyspalveluihin, on kyberturvallisuuden edistäminen ajankohtainen aihe sosiaali- ja terveydenhuollon organisaatioissa. Huoltovarmuuskeskuksen rahoittaman Digitaalinen turvallisuus 2030- ohjelmaan kuuluvan KyberSoTe-kehittämisprojektin avulla pyritään edistämään toimialan varautumista, palveluiden jatkuvuutta ja potilasturvallisuutta vahvistamalla kyberturvallista sosiaali- ja terveydenhuollon arkea. Opinnäytetyön tavoitteena oli tuottaa tietoa KyberSoTe-projektille sosiaali- ja terveydenhuollon henkilökunnan kyberturvallisuusosaamisen nykytilasta ja sen mahdollisista muutos- ja kehitystarpeista. Opinnäytetyön tuloksia voidaan hyödyntää projektin tulevassa kehittämistoiminnassa.

Opinnäytetyö toteutettiin integratiivisena kirjallisuuskatsauksena. Aineistoa haettiin CINAHL-, PubMed, ProQuest-, Sage Journal- ja Sience Direct-tietokannoista sekä hakua täydennettiin manuaalisella haulla. Aineistoon valittiin haun kautta 15 tutkimusta ja manuaalisen haun kautta kolme tutkimusta. Haun aikarajauksena oli vuodet 2020–2024. Aineisto analysoitiin induktiivisena sisällönanalyysinä.

Katsauksen tulokset kuvaavat sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen olevan vaihtelevaa. Tutkimuksessa todettiin niin hyvää ja keskimääräistä, kuin välttävää ja heikkoa kyberturvallisuusosaamista. Lisäksi tutkimuksessa havaittiin kyberturvallisuusosaamisen eri osa-alueita tarkasteltaessa merkittävää vaihteluväliä työntekijöiden osaamisen välillä. Tutkimustuloksista nousi runsaasti kyberturvallisuusosaamisen kehittämistarpeita, joita voidaan hyödyntää tulevassa KyberSoTe-projektin kehittämistyössä sekä muussa toimialan tutkimuksessa ja kehittämistoiminnassa. Kyberrikollisuuden yleistyessä sosiaali- ja terveydenhuollon organisaatioiden on erityisen tärkeää panostaa henkilöstön kyberturvallisuusosaamisen jatkuvaan ylläpitämiseen ja systemaattiseen kehittämiseen.

Avainsanat (asiasanat)

Kyberturvallisuus, kyberturvallisuusosaaminen, terveysala, kirjallisuuskatsaukset

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Bhaskar Tanja

Social and healthcare personnels cybersecurity competence and development needs. Integrative literature review.

Jyväskylä: JAMK University of Applied Sciences, May 2025, 69 pages.

Master´s degree Programme in Project management. Health and Welfare. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The rapid advancement of technology and digitalization has significantly transformed social and healthcare services in recent decades. As working environments evolve, digital competence and cybersecurity management have become essential to the daily work life of healthcare professionals. This thesis aimed to investigate the cybersecurity competence of social and healthcare personnel through a literature-based analysis.

As cybercrime increasingly targets healthcare services, the promotion of cybersecurity has become a timely and critical issue in social and healthcare organizations. The KyberSoTe-development project, which is part of “digital security 2030” program funded by Finland’s National Emergency Supply Agency, seeks to enhance preparedness, ensure service continuity, and strengthen patient safety by promoting a cyber-secure operational environment in the sector. The goal of the thesis was to produce information for the KyberSote-project about the current state of cybersecurity competence among social and health care personnel and to identify areas in need of development. The findings are intended to support future cyber security development within the project.

The study was conducted as an integrative literature review. Data were collected from the CINAHL, PubMed, ProQuest, Sage Journals, and Science Direct databases, supplemented with manual searches. A total of 18 studies published between 2020 and 2024 were included in the review. 15 of the studies were found among the reviews and three of them were searched manually. The material was analyzed by using inductive content analysis.

The results of the thesis indicate that cybersecurity competence among social and health care professionals varies considerably. The studies reported a range of competencies, from good and average to weak and insufficient. Significant variation was also observed across different areas of cybersecurity knowledge between individual professionals. The findings highlighted also numerous development needs which may guide future actions in the KyberSoTe-project. The findings also may contribute to broader sector-wide research and development efforts. As cybercrime becomes more and more widespread, it is especially important for social and healthcare organizations to invest in the regular maintenance and development of their staff's cybersecurity competence.

Keywords/tags (subjects)

Cybersecurity, Cybersecurity competence, Healthcare sector, literature review

Miscellaneous (Confidential information)

--

Sisältö

Kuviot

Taulukot

1 Johdanto

Teknologian vauhdikas kehitys ja digitalisaatio ovat muokanneet työelämää merkittävästi viime vuosikymmeninä. Digitalisaatio on tuonut työelämän tueksi lukuisia eri tieto- ja viestintäteknologioihin perustuvia palveluita, joiden käytön tarkoituksena on tuottaa asiakkaille uudenlainen automatisoidumpi palvelukokemus (Järvinen & Rousku 2017, 12). Kehityksen myötä myös sosiaali- ja terveydenhuollon palveluissa on otettu käyttöön uutta teknologiaa ja digitaalisia palveluita asiakkaiden hyvän hoidon, palvelun laadun ja tehokkuuden edistämiseksi. (Kyberturvallisuus- ohje sosiaali- ja terveysalan toimijoille 2019, 13–14). Laadukkaan ja häiriöttömän palvelun tuottaminen asiakkaalle edellyttää monipuolisen infrastruktuurin, teknologisten laitteiden toimintakyvyn ja tukitoimintojen lisäksi terveydenhuollon henkilöstön kattavaa digitaalista osaamista (Terveydenhuolto nd.).

Työelämän digitalisoitumisen myötä henkilöstön digitaalisen osaamisen ja kyberturvallisuustaitojen hallinnan tulisi olla keskeinen osa organisaation kyberturvallisuusajattelua ja -strategiaa. Kyberturvallisen toimintaympäristön luominen organisaatioon edellyttää, että jokainen työntekijä osaa toimia asianmukaisesti sekä arjen tilanteissa että mahdollisissa häiriötilanteissa (Limnéll, Majewski & Salminen 2014, 44). Hyvän kyberturvallisuusosaamisen avulla sosiaali- ja terveydenhuollon ammattilaiset turvaavat palveluiden ja toimintojen jatkuvuutta, toimivuutta sekä asiakasturvallisuutta. (Blek, Lahdenperä & Lehosmaa 2024).

Tänä päivänä työelämän nojautuessa yhä enemmän erilaisiin teknologisiin palveluihin, on kyberrikollisuus noussut työelämän merkittäväksi uhkatekijäksi. Verkossa kohdattavat riskit ja uhkat voivat toteutuessaan pahimmillaan vaarantaa Suomen huoltovarmuutta eli kansallista kriittistä infrastruktuuria, yhteiskunnan elintärkeitä toimintoja tai yksilön turvallisuutta. (Kyberturvallisuuden sanasto 2018, 25.) Viime vuosina kyberrikollisuus on moninkertaistunut sosiaali- ja terveydenhuollon palveluiden piirissä. Toimialan viimeaikaisista kyberturvallisuushaasteista kertovat erinäiset julkisuuteenkin nousseet tietojärjestelmien murrot, kuten Terapiakeskus Vastaamon tietomurto vuonna 2020 ja Helsingin Kaupungin tietomurto vuonna 2024. Näissä tietomurroissa vietiin satojen tuhansien yksityishenkilöiden arkaluonteisia terveys- ja henkilötietoja. (Kantola & Grönholm 2020; Loula 2024.) Kyberrikolliset ovat tänä päivänä kiinnostuneita yksityisistä henkilötiedoista, koska näiden arvo on rikollisilla markkinoilla voi olla jopa kymmenkertainen luottotietoihin nähden (Cartwright 2023, 1124–1125).

Sosiaali- ja terveydenhuollon organisaatioiden kyberturvallisuuden yhdeksi haavoittuvuudeksi on tunnistettu ihmiseen liittyvät tekijät ja inhimilliset virheet. Tämän haavoittuvuuden paikkaamiseksi organisaatioiden turvallisuustoiminnan tulisi keskittyä henkilöstön kyberturvallisuusosaamiseen ja sen edistämisen. (Cartwright 2023, 1125.) Sosiaali- ja terveydenhuollon palveluissa kyberturvallisuutta pyritään edistämään oikeanlaisella riskienhallinnalla sekä erilaisilla kyberturvallisuuskoulutuksilla ja harjoittelulla (Kyberturvallisuus- ohje sosiaali- ja terveysalan toimijoille 2019, 13–14, 22–24).

Tässä opinnäytetyössä tutkittiin sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamista. Aiheen tarkastelu toteutettiin henkilöstön kyberturvallisuusosaamisen nykytilanteen ja kehittämiskohteiden kautta. Opinnäytetyö toteutettiin integratiivisena kirjallisuuskatsauksena. Tämä opinnäytetyö on työelämälähtöinen ja se toteutetaan osana Huoltovarmuuskeskuksen rahoittamaa digitaalinen turvallisuus 2030 ohjelmaa ja KyberSoTe-projektia. Tämän opinnäytetyön tarkoituksena on tuottaa KyberSoTe-projektille ajankohtaista ja tutkimukseen perustuvaa tietoa sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen nykytilasta sekä siihen liittyvistä muutos- ja kehittämistarpeista. Tuotettua tietoa voidaan hyödyntää KyberSoTe-projektin tulevassa kehittämistoiminnassa kyberturvallisuuden vahvistamiseksi sosiaali- ja terveydenhuollon kontekstissa.

2 Opinnäytetyön tausta

Tämä opinnäytetyö on työelämälähtöinen ja se toteutetaan osana KyberSote-projektia. KyberSoTe-projektin tarkoituksena on edistää sosiaali- ja terveydenhuollon organisaatioiden kykyä varautua kyberuhkiin sekä tukea palveluiden jatkuvuutta ja potilasturvallisuutta vahvistamalla kyberturvallista sosiaali- ja terveydenhuollon arkea. KyberSoTe-projektin päätavoitteina on edistää kyberturvallista sosiaali- ja terveydenhuollon arkea kahdesta näkökulmasta. Ensimmäiseksi lisäämällä terveydenhuollon henkilöstön kyberturvallisuusosaamista ja kyberturvallisten toimintamallien hyödyntämistä, sekä toiseksi vahvistamalla sote-ammattilaisten ja tietohallinnon välistä yhteistyötä kyberturvallisuusasioiden osalta. (KyberSoTe- Kyberturvallisuutta sote-arkeen nd.).

KyberSoTe-projektin tarkoituksena on tuottaa sosiaali- ja terveydenhuollon organisaatioille käyttöön kyberturvallisuutta edistäviä työkaluja ja toimintamalleja, kuten osaamiskartoituskysely, samaistuttavia opastusvideoita sekä sote-ammattilaisten ja tietohallinnon vuorovaikutusta tukevia

havainnekuvia. (KyberSoTe- Kyberturvallisuutta sote-arkeen nd.). Tämän opinnäytetyön tarkoituksena on tuottaa tietoa sosiaali- ja terveydenhuollon kyberturvallisuusosaamisen nykytilasta ja sen mahdollisista kehitys- ja muutostarpeista. Opinnäytetyön tulokset luovutetaan KyberSoTe-projektin käyttöön, jossa niitä voidaan hyödyntää tulevan kehittämistyön tukena sosiaali- ja terveydenhuollon kyberturvallisuuden edistämisessä.

KyberSoTe- projekti on osa Huoltovarmuuskeskuksen rahoittamaa Digitaalinen turvallisuus 2030-ohjelmaa. Projekti toteutetaan vuosina 2024–2026. Projektin ensimmäisessä vaiheessa vuosina 2024–2025 tutkitaan sosiaali- ja terveydenhuollon kyberturvallisuusosaamisen tilaa, kehitetään toimintamalleja- ja työkaluja sekä pilotoidaan näitä Keski-Suomen hyvinvointialueella. Projektin toisen vaiheen tavoitteena on juurruttaa projektin tuloksia käytäntöön sekä jakaa näitä myös muiden hyvinvointialueiden hyödynnettäväksi. Projektin päätoteuttajana on Jyväskylän ammattikorkeakoulun terveysala, IT-instituutti ja liiketoimintayksikkö sekä osatoteuttajina Laurea, Turun ammattikorkeakoulu ja Tampereen ammattikorkeakoulu. Yhteistyökumppanina projektissa on Keski-Suomen hyvinvointialue ja huoltovarmuuskeskus. (KyberSoTe- Kyberturvallisuutta sote-arkeen nd.; KyberSoTe nd..)

3 Kyberturvallisuus sosiaali- ja terveydenhuollon palveluissa

3.1 Digitalisaation eteneminen ja kehittyminen

Digitalisaatiolla tarkoitetaan tehtävien ja toimintatapojen muutosta teknologian avulla. Digitalisaatio työelämässä ei ole pelkästään teknologinen ilmiö, vaan siihen liittyy myös merkittäviä sosioekonomisia muutoksia, minkä vuoksi työntekijöiden sopeutuminen muutosprosessiin on keskeistä huomioida. (Digitalisaatio ja työ, nd.) Digitaaliset palvelut ja kyberturvallisuusajattelu ovat alun perin tulleet osaksi sosiaali- ja terveydenhuoltoa sähköisten potilastietojärjestelmien sekä elektronisten lääkintälaitteiden kehittämisen ja niiden turvallisuuden tarkastelun myötä. Vauhdikkaan kehityksen myötä teknologiset laitteet ovat nopeasti nousseet keskeiseksi osaksi sosiaali- ja terveydenhuollon palveluketjua. Tänä päivänä teknologia ohjaa sosiaali- ja terveyspalveluiden tuottamista ja johtamista sekä mahdollistaa palveluiden tehokkuuden ja tuloksellisuuden. Lisäksi teknologian avulla seurataan pitkällä aikavälillä toteutuneita terveys- ja hoitokäytäntöjä sekä niiden vaikutuksia ihmisten terveyteen. (Nifakos, Chandramouli, Papachristou, Koch, Nikolaou, Panaousis & Bonacina 2021, 2). Sosiaali- ja terveydenhuollon palveluissa digitalisaation keskeisenä

tavoitteena on laadukkaan, tehokkaan ja turvallisen palvelun tuottaminen asiakkaalle uusien menetelmien avulla. (Kyberturvallisuus- ohje sosiaali- ja terveysalan toimijoille 2019, 13–14).

Viime vuosina tekoälyn ja pilvipalveluiden kehittyminen on muokannut sosiaali- ja terveydenhuollon palveluita. Tekoälystä, erityisesti generatiivisestä tekoälystä, on kaavailtu ratkaisua sosiaali- ja terveydenhuollon pitkään jatkuneeseen resurssipulaan. Generatiivisesta tekoälystä puhuttaessa viitataan tekoälyyn, joka pystyy tuottamaan uutta materiaalia kuten tekstiä, kuvia, koodeja ja ääntä (Sanmark & Sanmark 2024). Tulevaisuudessa generatiivisen tekoälyn on kaavailtu tukevan sosiaali- ja terveydenhuollon palveluita muun muassa tiedonhaussa ja sen tiivistämisessä, lausuntojen kirjaamisessa ja tallentamisessa, asiointipalveluissa, yksilöllisessä neuvonnassa sekä hyvinvointia tukevien laitteiden perustana. (Heinäsenaho, Äyräs-Blumberg & Lähesmaa 2023.)

Tekoälyjärjestelmien hyödyntämisessä on keskeistä huomioida järjestelmien turvallisuus sekä niihin liittyvät mahdolliset uhkat ja riskit. Tekoälyyn pohjautuvien ratkaisujen käyttö voi altistaa järjestelmät tieto- ja kyberturvariskeille, jotka liittyvät käytettävän opetusdatan ja tekoälymallin luottamuksellisuuteen, eheyteen ja saatavuuteen. Lisäksi tekoälyjärjestelmien monimutkaisuuden ja laajemman hyökkäyspinnan on tunnistettu lisäävän turvallisuusriskejä. (Lintulahti 2024.)

Pilvipalveluiden avulla sosiaali- ja terveydenhuollossa on puolestaan perinteisesti turvattu kriittistä dataa kuten potilastietoja. Tänä päivänä pilvipalvelut ovat kuitenkin kehittyneet pelkästä tietojen säilytyspaikasta uudenlaiseksi yhteydenpitopalveluksi, jonka avulla organisaatiot voivat tarjoavat uudenlaisia ja monipuolisia palveluita asiakkailleen. (Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen 2017, 17–18.) Pilvipalveluita hyödynnettäessä on keskeistä varmistaa potilastietojen luotettava ja eriytetty suojaus siten, että vain valtuutetut henkilöt voivat käsitellä tai tarkastella näitä. (Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille 2019) Pilvipalveluiden sisältämä sensitiivinen ja kriittinen data on kyberturvallisuuden näkökulmasta tärkeää suojata potilasturvallisuuden ja toiminnan jatkuvuuden turvaamiseksi.

3.2 Kyber- ja tietoturvallisuus

Kyberturvallisuudella tarkoitetaan digitaalisen ja verkottuneen maailman turvallisuutta ja niiden vaikutusta erinäisiin toimintoihin (Kyberturvallisuuden sanasto 2018, 22). Kyberturvallisuudessa vallitsee käytännön toiminnan ja ymmärryksen kautta tuotettu luottamus hallita ja sietää erinäisiä

kyberuhkia (Limnéll ym. 2014, 39). Kyberturvallisuusajattelu kattaa teknologiset laitteet sekä erilaiset olemassa olevat prosessit ja käytännöt, joilla suojellaan käytössä olevia verkkoja, dataa, ohjelmia ja laitteita ei-toivotulta käytöltä ja vahingoilta (Lehto, Pöyhönen & Lehto 2019, 14). Sosiaali- ja terveydenhuollossa kyberturvallisuudella varmistetaan toimialan palveluiden tuottaminen ja niiden kokonaisturvallisuus (Kyberturvallisuus- ohje sosiaali- ja terveysalan toimijoille 2019, 11).

Kyberturvallisen toimintaympäristön luominen organisaatioon vaatii usean toiminnan ajantasaisuutta, ennakointia sekä keskeisenä henkilöstön kykyä toimia asianmukaisesti arjessa ja mahdollisessa häiriötilanteessa (Limnéll ym. 2014, 44). Sosiaali- ja terveydenhuollon kontekstissa kyberturvallisuus käsittää laajan repertuaarin potilastyössä käytettäviä teknologisia laitteita, henkilöstön asian- ja roolinmukaisen digitaalisen osaamisen sekä lukuisia tukipalveluita, joiden kaikkien tulee toimia yhdessä ajantasaisesti. (Kyberturvallisuus- ohje sosiaali- ja terveysalan toimijoille 2019, 14–17.)

Sosiaali- ja terveydenhuollon palveluiden kyberturvallisuutta ylläpidettäessä ja kehitettäessä tulee huomioida toimialan laajan työskentelykenttä. Sosiaali- ja terveydenhuollon palveluita tuotetaan tänä päivänä lukuisissa erilaisissa toimintaympäristöissä kuten sairaaloissa, terveysasemilla, poliklinikoilla, asiakkaiden omissa koti- ja arkiympäristöissä sekä etävastaanottoina. Digitalisaatiokehityksen myötä näitä toimintaympäristöjä ja niiden kyberturvallisuutta tulee tarkastella aikaisempaa laajemmin. Kyberturvallisuus kattaa tänä päivänä sähköiset potilastietojärjestelmät, kyberfyysiset järjestelmät sekä esineiden internetin (IoT). Kyberfyysisiin järjestelmiin voi kuulua esimerkiksi lääkinnälliset tietojärjestelmät, terveydenhoitolaitteet, kirurgiset laitteet ja leikkausrobotit. Esineiden internet voi sisältää esimerkiksi hyvinvointilaitteet ja -applikaatiot sekä kuntoilulaitteet. (Pöyhönen ym. 2019, 8.) Teknologisten laitteiden käyttö ja digitaalisten palveluiden tuottaminen vaihtelevissa ympäristöissä on tuonut uudenlaista haastetta palveluiden kyberturvallisuudelle. (Kyberturvallisuus – Ohje sosiaali- ja terveydenhuollon toimijoille 2019, 14–17, 20.)

Viime vuosina perinteisten työskentelymallien rinnalle on noussut etätyömahdollisuus sekä henkilökohtaisten mobiililaitteiden hyödyntäminen työtehtävissä, mitkä ovat osaltaan lisänneet kyberuhkien todennäköisyyttä ja hämärtäneet henkilökohtaisen ja ammatillisen toiminnan välisiä rajoja. (Clarke & Martin 2024, 17; Kioskli 2023, 7.) Mobiililaitteiden käyttöön liittyviä tunnistettuja

haasteita ovat laitteiden käyttö vaihtelevissa, ei välttämättä rakenteellisesti suojatuissa ympäristöissä sekä laitteiden huomiotta jättäminen ja altistuminen varkaudelle. Mobiililaitteiden kyberturvallisuuden on lisäksi tunnistettu olevan heikompaa kuin perinteisten työasemien. Mobiililaitteiden käyttöä kriittisessä potilastyössä tai muussa toimintakriittisessä tehtävässä tulee harkita tarkasti, sillä järjestelmien toiminta on riippuvainen matkapuhelinverkkojen toiminnasta. Turvallisuuden takaamiseksi kaikkien sairaalajärjestelmiin yhdistettyjen mobiililaitteiden tulisi kuulua organisaation tietohallinnon hallinnoimaan kokonaisuuteen. (Pöyhönen ym. 2019, 17.)

Organisaation kyberturvallisuuden ylläpitäminen ja edistäminen on jatkuvaa työtä. Kansallisesti kyberturvallisuutta pyritään edistämään erilaisten organisaatioiden toiminnalla, tutkitulla tiedolla, erilaisilla standardeilla ja viitekehyksillä sekä EU:ssa unionin asettamalla yhteisellä kyberturvallisuusdirektiivillä, NIS-2 direktiivillä. Kyberturvallisuusdirektiivin tavoitteena on vahvistaa kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisten toimialojen, kuten sosiaali- ja terveydenhuollon osalta. (Kyberturvallisuuslaki on hyväksytty eduskunnassa - NIS2-direktiivin mukaiset velvoitteet astuvat voimaan 8.4.2025, 2025.) Valtakunnallisesti puolestaan kyberturvallisuuskeskus, puolustusvoimat ja poliisi tekevät yhteistyötä kyberuhkien, -rikkeiden ja -rikollisuuden ehkäisemiseksi, tunnistamiseksi ja pysäyttämiseksi. Viranomaisten lisäksi kyberuhkia torjuvat organisaatioiden ja yrityksien tietoturva-ammattilaiset sekä muu henkilöstö päivittäisessä toiminnassaan. (Kyberturvallisuus vaatii jatkuvaa työtä 2022.) Sosiaali- ja terveydenhuollon organisaatioiden kyberturvallisuuteen on viime vuosina kohdistettu yhä enemmän tutkimusta ja resursseja, mikä on seurausta toimialaan kohdistuneiden kyberhyökkäysten lisääntymisestä sekä näiden aiheuttamista merkittävistä turvallisuusriskeistä ja kasvavista taloudellisista kustannuksista. (Cartwright 2023, 1123–1126).

Kyberturvallisuuteen liittyy vahvasti käsite tietoturvallisuus, jolla tarkoitetaan organisaation järjestelyitä, joilla varmistetaan tarvittavan tiedon saatavuus, eheys ja luottamuksellisuus. Tiedon saatavuudella tarkoitetaan sitä, että tarvittava tieto on aina käytettävissä, kun sitä tarvitaan. Tiedon eheydellä tarkoitetaan tiedon paikkaansa pitävyyttä ja luotettavuutta. Tiedon luottamuksellisuudella puolestaan tarkoitetaan tietojen olevan vain sen käyttöön oikeutettujen henkilöiden käytössä. (Kyberturvallisuuden sanasto 2018, 15.)

Tietoturvallisuuteen liittyy keskeisesti kaksi käsitettä: tietoturva ja tietosuoja. Tietoturvalla tarkoitetaan organisaation omien tietojen suojaamista ja sen toiminnan turvaamista, kun taas tietosuojalla tarkoitetaan henkilötietojen ja yksityisyyden suojaamista. (Järvinen 2022, 25–27.) Tietoturvallisuus eroaa kyberturvallisuudesta siten, että se käsittää digitaalisen toimintaympäristön lisäksi reaalimaailman, toisin kuin kyberturvallisuus. Tietoturvallisuuden ylläpitämiseksi organisaatiossa tarvitaan kyberturvallisuutta. (Mitä on tietoturva? nd.)

Tietoturvan erilaisia toimenpiteitä ovat kulunvalvonta ja tilojen lukitseminen, salattujen tiedostojen turvallinen säilyttäminen, sensitiivistä tietoa sisältävien tiedostojen hävittäminen, tietojen varmuuskopiointi ja salaaminen sekä erilaisten teknisten tietoturva järjestelyiden kuten virustorjuntaohjelmien, palomuurin ja varmenteiden käyttö. Lisäksi tietoturvaan kuuluu laitteistojen, ohjelmistojen, tietoaineistojen, tietoliikenteen ja yleisen toiminnan varmistaminen ja turvaaminen. (Kyberturvallisuuden sanasto 2018, 15.) Sosiaali- ja terveydenhuollon palveluissa henkilöstön tietoturvallisuusosaaminen korostuu erityisesti asiakastietoja käsiteltäessä. Tietojenkäsittelyn tulee aina olla luottamuksellista asiakkaiden yksityisyyden takaamiseksi ja hoidon turvaamiseksi. (Kyberturvallisuus- ohje sosiaali- ja terveysalan toimijoille 2019, 13–14.) ’

Sosiaali- ja terveydenhuollon palveluiden tietoturvallisuuden ylläpitämisen tulee pohjautua tietoturvasuunnitelmaan, missä kuvataan sosiaali- ja terveyspalvelujen tuottajan tietoturva- ja tietosuojakäytäntöjä ja niiden järjestämistä. Tietoturvasuunnitelman avulla edistetään asiakastietojen turvallista käsittelyä, yhdenmukaistetaan ja kehitetään alan toimijoiden tietoturvaa ja -suojaa, vahvistetaan tietoturvallisuuden ja -suojan käytäntöjä sekä autetaan hallitsemaan digitalisuuteen liittyviä riskejä. Tietoturvasuunnitelman noudattamista valvotaan organisaatioiden omavalvontana sekä valvontaviranomaisten mahdollisin tarkastuksin. (Tietoturvasuunnitelma 2024.)

3.3 Kyber- ja tietoturvauhkat

Kyberuhkalla tarkoitetaan kyberympäristössä toteutuvaa pakottavaa toimintaa, jonka oletetaan aiheuttavan negatiivisen vaikutuksen kyseessä olevaan toimintaan tai sen intresseihin. Kyberuhkia voidaan tarkastella riskin, uhkan ja haavoittuvuuden kautta. Riskillä tarkoitetaan normaalia olemassaolon ehtoa eli negatiivisen tapahtuman mahdollisuutta kaikessa toiminnassa. Uhkalla tarkoitetaan vaaraa, jonka toteutuminen organisaatiossa pyritään välttämään tai torjumaan erilaisilla ennakoivilla toimilla sen haitallisuuden vuoksi. Haavoittuvuus puolestaan tarkoittaa organisaation

heikkoutta, joka avaa mahdollisuuden heikentää palvelun tieto- tai toimintavarmuutta. Kyberuhkien tarkastelulla ja oikeanlaisilla toimilla pyritään estämään kyberuhkien toteutuminen. (Limnéll ym. 2014, 105–111.) Kyberuhkien uhriksi voi joutua suoraan tai välillisesti yksittäinen kansalainen, yhteiskunnan elintärkeä toiminto tai kriittinen infrastruktuuri, kuten sosiaali- ja terveydenhuolto (Kyberturvallisuuden sanasto 2018, 25).

Tietoturvauhka puolestaan tarkoittaa tietojärjestelmän toimintaa uhkaava ja toteutuessaan vaarantavaa tekoa tai tapahtumaa (Peltomäki & Norppa, 2015, 172). Kyber- ja tietoturvauhkien takana voi olla useita erilaisia tekijöitä ja motivaatioita. Tekijöinä voivat toimia rikolliset, aktivistit, terroristit, yritykset tai valtiot. Motivaatio kyberrikollisuudelle puolestaan voi olla muutoksen edistäminen, tiedon varastaminen, taloudellinen hyötyminen, poliittinen tai sotilaallinen vaikuttaminen tai pelon lietsominen. (Limnéll ym. 2014, 111–113.)

3.3.1 Kyber- ja tietoturvauhkat sosiaali- ja terveydenhuollon palveluissa

Digitalisaation myötä sosiaali- ja terveydenhuollon palvelut ovat kohdanneet uudenlaisia haasteita erilaisten turvallisuusriskien ja -uhkien muodossa. (Kyberturvallisuus- ohje sosiaali- ja terveysalan toimijoille 2019, 13–14). Viime vuosina kyberrikolliset ovat kohdistaneet hyökkäyksiä entistä enemmän sosiaali- ja terveydenhuollon palveluita kohtaan, koska rikolliset ovat tunnistaneet henkilökohtaisten terveys- ja henkilötietojen arvon rikollisilla markkinoilla. Anastetuilla tiedoilla rikolliset voivat aiheuttaa uhreille niin henkistä kuin taloudellista kärsimystä ja haittaa. (Cartwright 2023, 1124–1125.)

Sosiaali- ja terveysalan organisaatioihin kohdistuneita tunnistettuja kyber- ja tietoturvauhkia ovat erilaiset tietoturvaloukkaukset, tietojenkalasteluyritykset, palvelunestohyökkäykset sekä kiristyshaittaohjelmat. Tietoturvallisuuteen liittyviä yleisiä loukkauksia ovat salasanojen ja käyttäjätunnusten väärinkäyttö, tietomurrot ja tiedon varastaminen. Tietojenkalasteluyrityksillä rikolliset pyrkivät saamaan henkilön lataamaan tietokoneelle ei-toivottuja ohjelmia tai paljastamaan salattuja tietoja. Palvelunestohyökkäysten tavoitteena on puolestaan kuormittaa tai pysäyttää tietojärjestelmän toiminta ja aiheuttaa täten haasteita organisaation toiminnalle. Kiristyshaittaohjelmilla puolestaan väärennetään tai salataan laitteella olevia tietoja, ja vaaditaan lunnaita tietojen palauttamiseksi tai salausten purkamiseksi. (Blek & Solankallio- Vahteri 2022, 354.)

Sosiaali- ja terveydenhuollon organisaatioihin kohdistuvilla kyberhyökkäyksillä voidaan aiheuttaa uhkaa potilaiden hoidolle ja turvallisuudelle (Blek & Solankallio- Vahteri 2022, 354). Kyberhyökkäyksen avulla rikolliset voivat aiheuttaa haittaa potilaiden hoidolle antamalla vääriä lääkemääräyksiä, häiritsemällä kriittisten lääkinnällisten laitteiden toimintaa tai viivyttämällä sairaalan yleistä toimintaa. (Rajamäki, Rathod & Kioskli 2023, 713.) Lisäksi hyökkäyksillä voidaan aiheuttaa haittaa potilaiden yksityisyydensuojalle ja yleisesti terveydenhuollon palveluiden tuottamiselle (Blek & Solankallio- Vahteri 2022, 354). Kyberturvallisuuden haasteet aiheuttavat merkittävää haittaa sosiaali- ja terveydenhuollon palveluiden taloudelle ja maineelle (Pöyhönen ym. 2019, 15).

Tulevaisuudessa sosiaali- ja terveydenhuollon palveluiden pohjautuessa entistä enemmän tekoälyn varaan on tärkeää huomioida kyberturvallisuuden näkökulma. Generatiivisen tekoälyn käyttöön liittyviksi riskeiksi on tunnistettu puutteellinen tietosuoja, tekoälyn tuottamat epätodet vastaukset sekä terveydenhuollon henkilöstön liiallinen luotto tekoälyn tekemiin päätöksiin (Sanmark & Sanmark 2024). Tunnistettujen riskien lisäksi kyberrikolliset ovat myös alkaneet hyödyntää tekoälyä rikollisessa toiminnassaan. Tekoälyä on hyödynnetty esimerkiksi haavoittuvuuksien etsinnässä sekä aikaisempaa automatisoidumpien ja kohdennetumpien kyberhyökkäyksien toteutuksessa. Tekoälyteknologian kehittyessä ja sen saatavuuden laajentuessa yhä laajemmalle, on esitetty huolta siitä, että rikolliset toimijat voivat ryhtyä hyödyntämään tekoälyä myös osana kyberhyökkäyksiä. (Tekoäly tulee muuttamaan myös kyberhyökkäyksiä 2022.)

3.4 Kyberturvallisuuden edistäminen

Kyberturvallisuuden jatkuva ylläpitäminen ja edistäminen on keskeistä organisaation kokonaisvaltaisen kyberturvallisuuden varmistamiseksi. Organisaatiot voivat hyödyntää kyberturvallisuuden kehittämistyön tukena Kybertuvallisuuden viitekehystä (Cybersecurity Framework 2.0). Viitekehyksen avulla tunnistetaan ja priorisoidaan toimenpiteitä kyberturvallisuusriskien hallitsemiseksi luomalla organisaation käyttöön yhteinen toimintamalli. Viitekehys koostuu kuudesta avaintoiminnosta, jotka jakautuvat useampaan alakategoriaan. (The NIST Cybersecurity Framework (CSF) 2.0, 2024.)

Viitekehyksen avaintoiminnot ovat hallinnointi, tunnistaminen, suojaaminen, havainnointi, reagointi ja palautuminen. Hallinnoinnilla tarkoitetaan organisaation digitaaliseen turvallisuuteen liittyvien strategioiden, käytäntöjen ja ohjeiden linjassa oloa organisaation toimintojen kanssa sekä

digitaalisen turvallisuuden asianmukaista johtamista. Tunnistaminen tarkoittaa organisaation kykyä tunnistaa toiminnan kannalta kriittiset suojattavat kohteet ja omistukset sekä näihin liittyvät riskit ja uhkat. Suojaamisella tarkoitetaan organisaation kykyä suojata tärkeät järjestelmät, tiedot ja tietovarannot. Havainnointi tarkoittaa organisaation taitoa kehittää häiriöiden havainnointikykyä ja -prosesseja digitaalisen turvallisuuden ylläpitämiseksi. Reagointi tarkoittaa organisaation kykyä reagoida turvallisuuden poikkeamiin nopeasti ja suunnitellusti, kun taas palautuminen tarkoittaa organisaation kykyä toipua digitaalisesta häiriöstä ja jatkaa toimintaansa normaaliin tapaan. (The NIST Cybersecurity Framework (CSF) 2.0, 2024.)

Kyberturvallisuuden viitekehystä hyödyntämällä sosiaali- ja terveydenhuollon palveluissa voidaan siirtyä kohti ennakoivaa toimintamallia kyberturvallisuuden ylläpitämisessä ja edistämisessä. Tutkimuksen perusteella monien organisaatioiden ja toimialojen, kuten myös terveydenhuollon, toimintaa leimaa toimintatapa, jossa reagoidaan vasta häiriötilanteessa. Reagoiva toimintatapa tarkoittaa sitä, että vika- tai uhkatilanne on käsillä, ja siihen reagoidaan nopeilla päätelmillä sekä kiireellisillä toimenpiteillä (Pöyhönen ym. 2019, 23.) Nämä eivät useinkaan tuota parasta lopputulosta.

4 Digitaalinen osaaminen

Termillä osaaminen, joka usein kääntyy myös termiksi kompetenssi, tarkoitetaan kykyä muuttaa tieto ja taito halutunlaiseksi toiminnaksi. Osaaminen on aina suorittavan yksilön ominaisuus, ja se on moninaista. (Kajander-Unkuri 2015, 16–17.) Yksilön osaaminen koostuu tietojen ja älyllisten taitojen lisäksi motivaatiosta, tahdosta, tunteista ja temperamentista. Osaaminen sisältää aina mahdollisuuden jatkuvaan oppimiseen ja kehittymiseen, ja sitä tulee tarkastella tilanne- ja tehtäväkohtaisesti tietyssä kontekstissa. (Hanhinen 2010, 71–74.)

Digitaalisella osaamisella puolestaan tarkoitetaan yksilön taitoa hyödyntää tieto- ja viestintätekniikkaa monipuolisesti ja tehokkaasti elämän kaikilla osa-alueilla (Digitaitotasot nd.). Yksi digitaalisten osaamisen jaottelutapa on Vuorikarin, Kluzerin ja Punien (2022) luoma Kansalaisten digitaalisen osaamisen viitekehys DigComp. DigComp viitekehys jaottelee digitaalisen osaamisen viiteen eri osa-alueeseen; informaatio- ja digilukutaitoon, vuorovaikutukseen ja yhteistyöhön, digitaalisen sisällön luomiseen, turvallisuuteen ja ongelmanratkaisuun, joita tarkastellaan tiedon, taidon ja asenteen yhdistelmänä. (Vuorikari ym. 2022, 3 & 7.)

Kansalaisen digitaalisen osaamisen viitekehyksessä Informaatio- ja digilukutaito tarkoittaa yksilön moninaista tiedonhankintataitoa eri verkkoympäristöissä sekä sen kriittistä tarkastelua ja turhan tiedon suodattamista. Tällöin yksilö kykenee käsittelemään lukemaansa tietoa asiallisesti ja säilyttämään sitä oikein. Vuorovaikutus ja yhteistyö tarkoittaa mediataitojen hallintaa eli nettietikettiä. Nettietiketti tarkoittaa yksilön asiallista verkossa vuorovaikuttamista, verkkoyhteisöissä toimimista, tiedon jakamista sekä oman digitaalisen identiteetin hallintaa. Digitaalisen sisällön luomisella tarkoitetaan yksilön kykyä tuottaa uutta sisältöä pohjautuen jo olemassa olevaan tietoon. Tällöin yksilö kykenee muokkaamaan tietoa, hallitsee prosessien erinäiset lisenssi- ja lupa-asiat sekä omaa ohjelmoinnin taidon. Turvallisuudella tarkoitetaan erilaisten käytettävien laitteiden, henkilökohtaisten tietojen, oman ja muiden terveyden- ja hyvinvoinnin sekä ympäristön suojaamisen hallintaa. Ongelmanratkaisu taas tarkoittaa sitä, että yksilö tunnistaa oman digitaalisen osaamisensa, havaitsee tekniset ongelmat ja osaa ratkaista ne oikeilla välineillä. (Vuorikari ym. 2022, 7.) Digitaalisesti taitava henkilö hallitsee edellä mainitut osa-alueet hyvin ja näitä noudattamalla edistää kyberturvallisuutta toiminnassaan.

5 Kyberturvallisuusosaaminen sosiaali- ja terveysalalla

Kyberturvallisuuden tarkastelu on muuttunut viime vuosina yhä enemmän teknologisten toimenpiteiden tarkastelusta ihmisen toiminnan tarkasteluun. Tänä päivänä kyberturvallisuuden ylläpitämisen keskeisenä tekijänä pidetään henkilöstöä ja heidän kykyään toimia kyberturvallisesti niin arjessa kuin uhkatilanteissa. (Kioskli, Fotis, Nifakos & Mouratidis 2023, 7.)
Kyberturvallisuusosaaminen on aina monimuotoista, ja siksi sen tarkempi tarkastelu on tärkeää.

5.1 Kyberturvallisuusosaamisen määritelmä

Kyberturvallisuusosaaminen termillä on kirjallisuudessa useita hieman toisistaan poikkeavia määritelmiä. Tässä opinnäytetyössä kyberturvallisuusosaaminen määritellään yhdistelmäksi yksilön asennetta, tietoisuutta, taitoja ja käyttäytymistä, joilla varmistetaan kyberturvallisuutta. Asenne tarkoittaa käyttäytymiseen vaikuttavaa negatiivista tai positiivista tunnetta, aikomusta tai uskomusta. (Tieteen termipankki nd.) Tietoisuudella tarkoitetaan yksilön kullakin hetkellä kokemien ajatuksien, tunteiden, aistimuksien, elämyksien ja aikaisempien muistikuvien kokonaisuutta (Finto – suomalainen asiasanasto ja ontologiapalvelu nd.). Taito puolestaan on yksilön kykyä ratkoa ongelmia ja suoriutua erinäisistä tehtävistä (Defining ‘Skill’ and ‘Competence’, nd.). Käyttäytymisellä

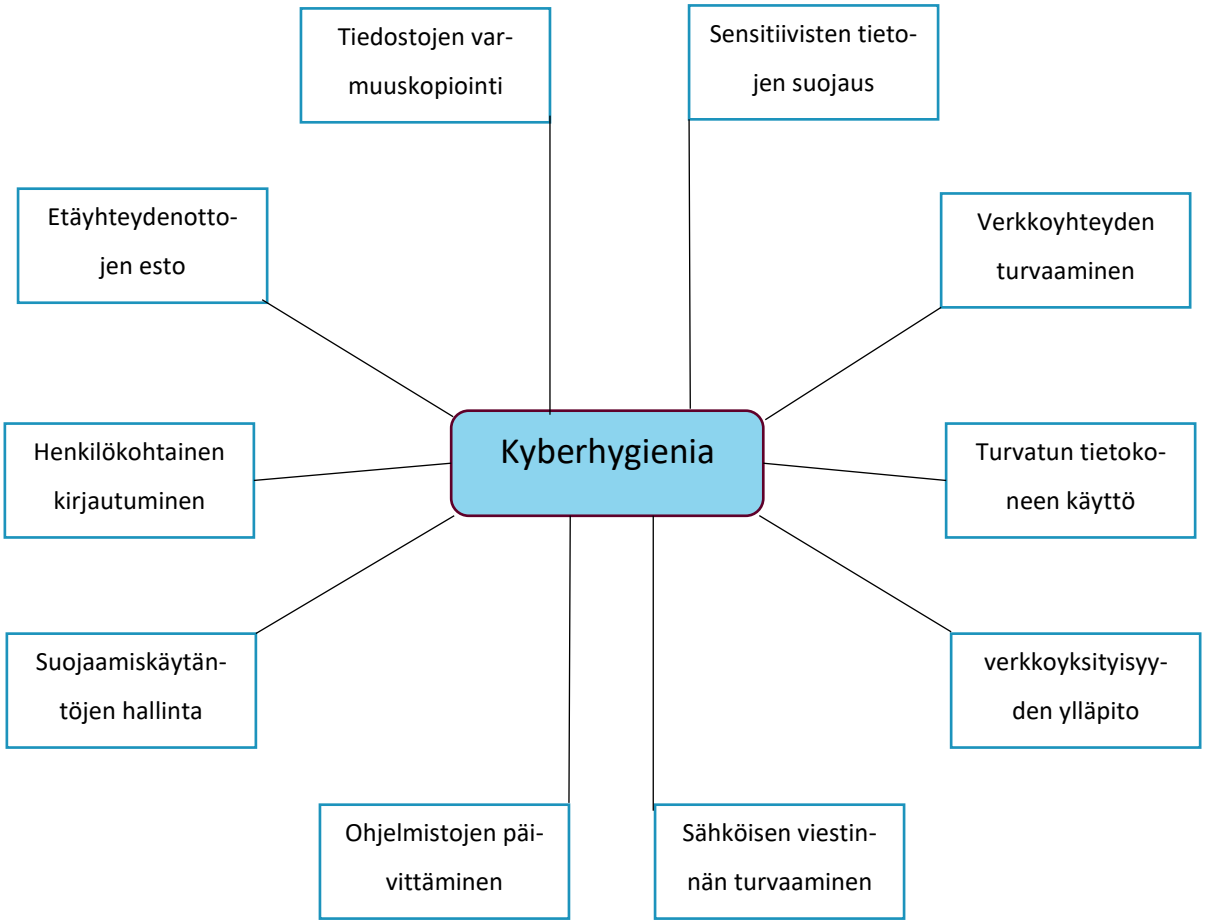
tarkoitetaan yksilön tapaa toimia tietyssä tilanteessa tiettyjen vaatimuksien alaisena (Cambridge Dictionary nd.). Kyberturvallisuusosaaminen on aina yksilöllisiä ja usein altista erilaisille vaikutteille, minkä vuoksi ihmiskeskeinen näkökulma on tärkeä kyberturvallisuudessa. Kyberturvallisuuden edistämisen keskiössä tulisi olla henkilöstön tietoisuuden lisääminen sekä heidän osallistamisensa ja sitouttamisensa organisaation kyberturvalliseen toimintaan. (Kioskli ym. 2023, 7, 13.)

5.2 Työntekijän kyberturvallisuusosaaminen

5.2.1 Kyberhygienia

Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen tarkastelussa voidaan hyödyntää useita eri välineitä, joista yksi on kyberhygienia. Kyberhygienialla tarkoitetaan erilaisia asetettuja käytäntöjä ja protokollia, joiden avulla ylläpidetään organisaatioiden digitaalista turvallisuutta ja ehkäistään kyberuhkien toteutumista. Sosiaali- ja terveydenhuollon organisaatioissa hyvään kyberhygieniaan kuuluu useita keskeisiä käytäntöjä, joilla pyritään turvaamaan tietojärjestelmien ja potilastietojen suoja ja yksityisyys. Näihin käytäntöihin sisältyy esimerkiksi tiedostojen säännöllinen varmuuskopiointi ja sensitiivisten tietojen suojaaminen. Lisäksi on tärkeää käyttää suojattua ja turvallista verkkoyhteyttä sekä ajantasaisin ohjelmistoin varustettua tietokonetta. Verkkoyksityisyyden ylläpitäminen ja sähköpostiliikenteen turvaaminen ovat keskeisiä osia turvallista työskentelyä. Ohjelmistojen ja sovellusten säännöllinen päivittäminen vähentää tietoturva-aukkoja. Työntekijöiden tulee hallita suojautumiskäytännöt ja käyttää aina henkilökohtaisia kirjautumistietoja kirjautuessaan terveydenhuollon laitteisiin tai järjestelmiin. Lisäksi omalle työpisteelle kohdistuvat ei-toivotut etäyhteydenotot on estettävä. (Kioskli ym. 2023, 10.) Sosiaali- ja terveydenhuollon hyvät kyberhygieniset käytännöt havainnollistettuna kuviossa 1.

5.2.2 Kyberhygieniset käytännöt



Kuvio 1. Sosiaali- ja terveydenhuollon hyvät kyberhygieniset käytännöt

Kyberhygienisten käytäntöjen tulisi olla osa jokaisen sosiaali- ja terveydenhuollon ammattilaisen osaamista ja päivittäistä toimintaa. Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisiin toimenpiteisiin kuuluu keskeisesti vahvojen salasanakäytäntöjen hallitseminen. Tällä tarkoitetaan yksilöllisen, riittävän haastavan ja uniikin salasanan asettamista, sen turvallista säilyttämistä, säännöllistä päivittämistä sekä eri salasanojen käyttöä eri alustoilla. Salasanasuojaus on jokaisen yksilön henkilökohtaista tietoa, eikä sitä tule jakaa muille. Terveydenhuollonjärjestelmiin kirjautumisessa suositellaan käytettävän kaksivaiheista tunnistautumista. (Kioskli ym. 5, 10, 11; Nifakos ym. 2021, 18, 14.)

Turvallisten salasanakäytäntöjen lisäksi henkilöstön käytössä olevien älylaitteiden kuten tietokoneiden, älypuhelimien ja tablettien ohjelmistot tulee päivittää säännöllisesti. Ohjelmistojen uusimmat versiot ja suojauspäivitykset takaavat laitteiden kyberturvallisuutta ja turvallista työkäyttöä.

Työhön liittyvät tiedostot, erityisesti potilastiedot ja sairaskertomukset, tulee varmuuskopioida säännöllisesti tietojen säilömiseksi mahdollisessa kyberhyökkäystilanteessa tai teknisten laitteiden kaatuessa. Varmuuskopioidut tiedot takaavat uhkatilanteissa potilaiden hoidon jatkuvuuden ja turvallisuuden. (Kioskli ym. 2023, 6 & 11)

Työkäytössä olevia teknologisia laitteita yhdistettäessä verkkoon, tulee aina varmistaa verkkoyhteyden turvallisuus. Sairaalaympäristössä on turvallista käyttää työpaikan omaa verkkoyhteyttä tai turvattua VPN-yhteyttä. Julkisten ja turvaamattomien verkkoyhteyksien käyttöä ei suositella sosiaali- ja terveydenhuollon palveluissa kyberuhkien ehkäisemiseksi. Työlaitteilla internetiä käytettäessä on tärkeää kiinnittää huomiota käytettyjen verkkosivustojen luotettavuuteen ja turvallisuuteen sekä välttää tuntemattomien tiedostojen lataamista laitteelle (Kioskli ym. 2023, 6, 11)

Kyberturvallisessa ajattelussa ja toiminnassa on keskeistä tietoturvallisuuden ylläpitäminen. Sosiaali- ja terveydenhuollossa potilastietojen luottamuksellinen käsittely, tietojen oikeaoppinen suojaaminen sekä sensitiivisten tietojen salassapito ovat tärkeä osa palveluketjua. Erityisesti potilastietoja viestiessä on tärkeää huomioida tiedonjaon turvallisuus. Viestintävälineeksi tulee aina valita turvallinen väylä kuten tähän tarkoitettu sovellus tai järjestelmä, esimerkiksi potilastietojärjestelmä. Turvaamattomien viestintäväylien kuten tekstiviestien, henkilökohtaisessa käytössä olevien sähköpostien tai erinäisten sovelluksien käyttöä ei suositella käytettäväksi potilasviestinnässä. (Kioskli ym. 2023, 11.)

Tänä päivänä sosiaali- ja terveydenhuollon henkilöstö hyödyntää työvälineenä yhä enemmän henkilökohtaisia mobiililaitteita kuten puhelimia, tabletteja tai tietokoneita. Erityisesti älypuhelimen käyttö on kasvanut työntekijöiden keskuudessa. Henkilökohtaisen älypuhelimen työkäytössä on tärkeää varmistaa, että työhön liittyvät tiedot ja henkilökohtaiset tiedot säilytetään asianmukaisesti omissa erillisissä kansioissaan. Potilastietojen suojaamiseksi henkilökohtainen puhelin on tärkeää turvata vahvojen salasanojen avulla ja varmuuskopioida säännöllisesti. (Cartwright 2023, 1127.)

Henkilökohtaisten älylaitteiden käytön myötä sosiaalinen media on tullut osaksi arkipäiväämme. Nykyään ihmiset jakavat sosiaalisessa mediassa tietoa itsestään, perheestään ja läheisistään sekä

vapaa-ajan tekemisistään ja työstään. Kyberrikolliset voivat hyödyntää näitä jaettuja tietoja esimerkiksi käyttäjän manipuloinnissa (social engineering). Käyttäjän manipuloinnissa rikollinen pyrkii hyödyntämään keräämiään tietoja niin, että uhri tekisi jotain, mitä tämä ei normaalisti tekisi. (Lehto ym. 2017, 15.) Kyberuhkien ehkäisemiseksi on tärkeää pohtia, mitä tietoja sosiaalisessa mediassa on turvallista jakaa.

Tänä päivänä käyttäjien manipulointi on kyberrikollisten yksi keskeinen rikollisuuden muoto. Käyttäjien manipulointi toteutetaan usein kalasteluviestejä, kuten sähköposteja tai tekstiviestejä, lähettämällä. Nämä lähetetyt viestit sisältävät usein linkin, jota uhria houkutellaan klikkaamaan. Henkilöstön tapoja ylläpitää organisaation kyberturvallisuutta on kalasteluyritysten tunnistaminen ja oikeanlainen reagointi niihin. Tunnistamalla manipulointiyritykset työntekijä toimii portinvartijana salaisille tiedoille ja estää näin rikollisten pääsyn järjestelmiin. (Kioskli ym. 2023, 6, 11.)

Kyberturvallisuuden ylläpitämiseksi ja edistämiseksi organisaatioiden on tärkeää sisällyttää kyberturvallisuus osaksi yrityksen strategista toimintaa. Henkilöstön kyberturvallista käyttäytymistä tukevat selkeät ohjeet, toimintamallit sekä jatkuva tuki teknologisten palveluiden käyttöön. (Peltomäki & Norppa, 2015, 99.) Kyberturvallisuuden tukena sosiaali- ja terveydenhuollon palveluissa toimii osaava IT-tuki, joka ylläpitää verkkojen ja järjestelmien turvallisuutta sekä tukee henkilöstöä näiden käytössä (Kioskli ym. 2023, 11).

Henkilöstön kyberturvallisuusosaamisen edistämisessä on tärkeää osaamisen säännöllinen tarkastelu ja kouluttaminen (Kioskli ym. 2023, 11). Sosiaali- ja terveydenhuollon organisaatioiden tulee tunnistaa työntekijöidensä kyberturvallisuusosaamisen taso ja tarpeet sekä tarjota näiden mukaisia koulutuksia. Kyberturvallisuuskoulutukset voivat sisältää uhka-arvioihin, riskeihin ja haavoittuvuuksiin perustuvia kohdistettuja harjoituksia. Uusien toimintamallien jalkauttamiseksi osaksi päivittäistä toimintaa on tärkeää toteuttaa harjoitukset yhdessä sosiaali- ja terveydenhuollon henkilöstön sekä muiden todellisessa häiriötilanteessa tarpeellisten tahojen kanssa. (Kyberturvallisuus – Ohje sosiaali- ja terveydenhuollon toimijoille 2019, 22–24; Clarke & Martin 2024, 18.) Kyberturvallisuuden edistäminen vaatii vankkaa tietoturvallisuuden ja terveydenhuollon toimintatapojen ymmärrystä. (Pöyhönen, Lehto & Lehto 2019, 16.)

5.2.3 Työtehtävien vaikutus kyberturvallisuusosaamisen vaatimuksiin

Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamista tarkasteltaessa on tärkeää huomioida työntekijän työnkuva, ja suhteuttaa kyberturvallisuusosaamisen vaatimukset tähän. Sairaalaympäristössä työskentelevän ammattilaisen tulee hallita potilastietojen ja potilastietojärjestelmien asianmukaisen käsittelyn ja käytön lisäksi etähoitojärjestelmien, verkottuneiden lääkintälaitteiden, potilaiden tunnistamiseen käytettävien järjestelmien, erilaisten verkko- ja mobiilipäälaitteiden sekä sairaalarakennuksen kiinteistöautomatisaation turvallinen käyttö. Sosiaalihuollon palveluissa kyberturvallisuusosaaminen puolestaan näyttäytyy tavanomaisten ja arkaluonteisten asiakastietojen käsittelynä, päätöksien tekona sekä erilaisen toimistotekniikan ja tietojärjestelmien käyttönä. Lisäksi tänä päivänä sosiaali- ja terveydenhuollon palveluita tuotetaan yhä enemmän asiakkaiden omissa koti- ja arkiympäristöissä tai etäyhteyksillä työntekijän omista ympäristöistä. Digitaalisten laitteiden etäkäyttö vaihtelevissa ympäristöissä vaatii työntekijöiltä uudenlaista ymmärrystä kyberturvallisuudesta, erityisesti etäyhteyksien ja tietosuojan turvallisuudesta. (Kyberturvallisuus – Ohje sosiaali- ja terveydenhuollon toimijoille 2019, 14–17, 20.)

6 Toteutus

6.1 Tutkimuskysymys ja tavoite

Tämän integratiivisen kirjallisuuskatsauksen tarkoituksena on tutkia sosiaali- ja terveydenhuollon henkilökunnan kyberturvallisuusosaamista käsittelevän kirjallisuuden avulla. Tutkimuksessa tarkastellaan henkilöstön kyberturvallisuusosaamisen nykytilaa ja kehittämistarpeita. Tutkimuksessa pyritään vastaamaan tutkimuskysymykseen:

Minkälainen on sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen nykytila ja mitkä ovat sen kehittämistarpeet?

Kirjallisuuskatsauksen tavoitteena on tuottaa tietoa sosiaali- ja terveydenhuollon henkilökunnan kyberturvallisuusosaamisen nykytilasta ja sen mahdollisista kehitys- ja muutostarpeista työn toimeksiantajalle KyberSoTe- projektille.

6.2 Tutkimussuunnitelma ja -menetelmät

Tämä opinnäytetyö toteutettiin integratiivisena kirjallisuuskatsauksena. Integratiivinen katsaus on monipuolinen menetelmä, joka tarjoaa kattavan kuvan tutkimusaihetta käsittelevästä kirjallisuudesta. Integratiivinen kirjallisuuskatsaus sallii analyysin pohjaksi niin laadullisin kuin määrällisin menetelmin tehdyt tutkimukset, seulomatta aineistoa liian tiukasti. (Vilkka 2023, 25.) Kirjallisuuskatsauksen avulla tunnistetaan, arvioidaan ja tiivistetään olemassa olevan tutkimuksen aineistoa, joka toimii perustana uusille tutkimustuloksille. (Salminen 2011, 5–6). Integratiivisen kirjallisuuskatsauksen keskeisiä tunnusmerkkejä ovat kriittinen ja järjestelmällinen ote aineiston kokoamisessa ja tarkastelussa sekä ennalta toteutettu aiheen käsitteellinen taustoitus (Vilkka 2023, 25). Tämän kirjallisuuskatsauksen tutkimusmenetelmäksi valittiin integratiivinen kirjallisuuskatsaus, sillä se mahdollistaa kyberturvallisuusosaamisen tarkastelun laaja-alaisesti eri näkökulmista ja menetelmillä tuotetun tutkimustiedon pohjalta. Integratiivinen lähestymistapa mahdollistaa monipuolisen ja selkeän synteesin muodostamisen, jota opinnäytetyön toimeksiantaja voi hyödyntää käytännön kehittämistoiminnassaan.

Tämän kirjallisuuskatsauksen pohjana käytettiin Cooperin ja integroivan kirjallisuuskatsauksen mallia, jota Whittemoren ja Knafln ovat muokanneet. Salmisen mukaan Cooper (1989) on tiivistänyt integroivan kirjallisuuskatsauksen vaiheet seuraavasti: tutkimusongelman asetus, aineiston hankinta, arviointi, analyysi sekä tulkinta ja tulosten esittäminen. Tutkimuskirjallisuuteen nojaava integratiivinen kirjallisuuskatsaus on aina täsmällinen, systemaattinen ja toistettavissa oleva tutkimusmenetelmä. (Salminen 2011, 5–6 & 8.) Integratiivisen kirjallisuuskatsauksen malli kuviossa 2.

Kuvio 2. Integratiivisen kirjallisuuskatsauksen vaiheet Cooperin (1989) ja Whittemoren ja Knafln (2005) mukaisesti

6.3 Tiedonhaku

Integratiivisen kirjallisuuskatsauksen keskeinen prosessi on tiedonhaku. Tiedonhakuprosessi tulee suunnitella ja toteuttaa huolellisesti ja systemaattisesti. Tiedonhaku tulee toteuttaa ennalta määritellyin kriteerein siten, että hakuprosessi on tarvittaessa toistettavissa ja tuottaa samat tulokset (Tiedonhaun opas nd.) Tämä kirjallisuuskatsaus toteutettiin Cooperin (1989) sekä Whittemoren ja Knafln (2005) tiivistämän viisi vaiheisen mallin mukaisesti. (Sulosaari & Kajander- Unkuri 2015, 113.) Kirjallisuuskatsauksen teon tukena hyödynnettiin alan kirjallisuutta ja oppaita sekä Jyväskylän ammattikorkeakoulun (JAMK) kirjaston informaatikon ohjausta.

Kirjallisuuskatsauksen ensimmäisessä vaiheessa asetetaan tutkimusongelma, joka ohjaa tutkimusmenetelmän valintaa ja tutkimusprosessin etenemistä. Tässä kirjallisuuskatsauksessa tutkittavan aiheen yläraamit on asettanut työelämän toimeksiantaja eli KyberSoTe-projekti. Tutkimusongelman määrittämiseksi suoritettiin alustavia tiedonhakuja sekä käytiin ohjauskeskusteluja opinnäytetyönohjaajan ja työelämäyhteistyökumppanin kanssa. Aineiston tuottamista varten tutkimusongelmasta johdettiin tutkimuskysymys, jonka perusteella laadittiin tiedonhakustrategia (Kananen 2015, 41–42 & 55–59). Tiedonhaun suunnitteluvaiheessa määritettiin aiheeseen liittyvät keskeiset käsitteet, joista muodostettiin haussa käytettävät hakusanat ja -lausekkeet (Niela-Vilén & Hamari 2016, 25–27). Hakusanojen ja -lausekkeiden toimivuutta testattiin erilaisilla hakukokeiluilla ennen virallista tiedonhakua (Lehtiö & Johansson 2016, 36–42).

Tutkimuksen toinen vaihe eli aineiston hankinta toteutettiin sähköisistä tietokannoista joulukuun 2024 aikana. Tiedonhaku toteutettiin seuraavissa tietokannoista: CINAHL, ProQuest, PubMed, Sage Journals ja Sience Direct. Tiedonhakua tehtiin useilla eri hakusanoilla- ja lausekkeilla, jonka pohjalta tutkimukseen valittiin toimivimmat hakulausekkeet. Tiedonhakua muokattiin tietokanta kohtaisesti huomioiden tietokantojen omat asiasanastot ja asetetut kelpoisuusehdot. Tutkimukseen päätyneet hakusanat ja lausekkeet sekä tulokset liitteessä 1.

Tiedonhakustrategian yksi keskeinen osa on kelpoisuusehtojen asettaminen. Aineiston rajaus on tärkeää, jotta saatu aineisto on käsiteltävissä ja se vastaa asetettuun tutkimuskysymykseen. Yleisinä rajauksina tiedonhaussa hyödynnetään kelpoisuuskriteereitä sekä mukaanotto- ja poissulkukriteereitä. (Lehtiö & Johansson 2016, 57.) Mukaanotto- ja poissulkukriteerit taulukossa 1. Tämän

kirjallisuuskatsauksen kelpoisuuskriteereiksi on asetettu: vertaisarvioitu tieteellinen artikkeli, alkuperäistutkimus, koko julkaisu, aikarajaus 2020–2024, julkaisukieli englanti tai suomi, hakusana mainittu otsikossa tai abstraktissa sekä poissulku kirjallisuuskatsauksille. Vertaisarvioitu tieteellinen artikkeli, alkuperäistutkimus ja koko julkaisun saatavuus valittiin aineiston rajauskriteereiksi tutkimuksen luotettavuuden lisäämiseksi. Lisäksi hakusanan esiintyminen artikkelin otsikossa tai abstraktissa helpottaa aineiston hallintaa ja käsittelyä. Aikarajauksella 2020–2024 ja kirjallisuuskatsauksien rajaamisella pyritään varmistamaan nopeasti kehittyvän tutkimusaiheen uusin ja päivittynein tieto.

Kelpoisuuskriteerien lisäksi tutkimuksen aineistoa rajaa kirjallisuuskatsaukselle asetetut mukaanotto- ja poissulkukriteerit. Mukaanotto- ja poissulkukriteerit ohjaavat tiedonhakuprosessia ja tarkentuvat mahdollisesti hakuprosessin edetessä. (Valkeapää 2017, 57–60.) Potentiaalisen aineiston keräämisen jälkeen arvioidaan vastaako löytynyt aineisto asetettuun tutkimuskysymykseen ja määritettyihin kriteereihin (Sulosaari & Kajander-Unkuri 2016, 111–112). Mukaanottokriteerien perusteella tämän tutkimuksen aineiston tuli vastata siihen minkälaisena näyttäytyy sosiaali- ja terveydenhuollon valmistuneiden työntekijöiden kyberturvallisuusosaamisen nykytila ja mitkä ovat sen kehittämistarpeet. Poissulkukriteereiksi asetettiin muiden kuin sosiaali- ja terveydenhuollon alojen henkilöstön sekä sosiaali- ja terveysalan opiskelijoiden kyberturvallisuusosaamisen nykytilaa ja kehittämistarpeita kuvaavat tutkimukset. Mukaanotto- ja poissulkukriteerit taulukossa 1.

Taulukko 1. Aineiston mukaanotto- ja poissulkukriteerit

Mukaanottokriteerit (artikkeli vastaa tutkimuskysymykseen)	**Poissulkukriteerit (artikkeli ei vastaa tutkimuskysymykseen)**
Artikkeli kohdistuu sosiaali- tai terveydenhuollon palveluissa työskenteleviin henkilöihin	Artikkeli ei kohdistu sosiaali- tai terveydenhuollon palveluissa työskenteleviin henkilöihin
Artikkeli käsittelee sosiaali- tai terveydenhuollon palveluissa työskentelevien kyberturvallisuusosaamisen nykytilaa	Artikkeli käsittelee muiden ammattiryhmien kyberturvallisuusosaamisen nykytilaa
Artikkeli käsittelee sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen kehittämistarpeita	Artikkeli käsittelee muiden ammattiryhmien kyberturvallisuusosaamisen kehittämistarpeita
Artikkeli käsittelee sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamiseen vaikuttavia tekijöitä	Artikkeli käsittelee muiden ammattiryhmien kyberturvallisuusosaamisen vaikuttavia tekijöitä
Artikkeli kohdistuu ammattiin valmistuneisiin sosiaali- ja terveydenhuollon henkilöihin	Artikkeli kohdistuu sosiaali- tai terveydenhuollon opiskelijoihin

Toteutettu sähköinen tiedonhaku tuotti yhteensä 507 viitettä. Otsikkoseulan läpäisi 110 viitettä ja Abstraktiseulan 56 viitettä. Maksumuurien takana oli 4 artikkelia. Koko tekstin lukemisen ja laadun arvioinnin jälkeen artikkeleista kirjallisuuskatsaukseen valikoitui 15 artikkelia.

Sähköinen tiedonhaku ei suunnitelmallisuudestaan huolimatta tavoita aina kaikkea kirjallisuuskatsaukseen soveltuvaa tietoa. Tiedonhakua tulee siis täydentää manuaalisella haulla. (Niela-Vilén & Hamari 2016, 25.) Tässä kirjallisuuskatsauksessa manuaalista hakua toteutettiin käymällä läpi kerätyn aineiston viitteitä ja lähdeluetteloja sekä toteuttamalla vapaasanahakua Google Scholar- verkkopalvelussa. Lähdeluettelojen läpi käynnin, manuaalisen haun ja vapaasanahaun perusteella kirjallisuuskatsaukseen lisättiin 3 artikkelia.

Objektiivisuuden varmistamiseksi kirjallisuuskatsauksen tiedonhaku ja lähteiden luotettavuuden arviointi suositellaan toteutettavaksi ensisijaisesti kahden tutkijan toimesta itsenäisesti. Tämän jälkeen tulokset yhdistetään ja yhdenmukaistetaan yhteisen keskustelun ja arvioinnin perusteella. (Systemaattinen tiedonhaku opas nd). Koska kyseessä oli yksilöllinen opinnäytetyö, kirjallisuuskatsaus on toteutettu yhden tutkijan toimesta. Kirjallisuuskatsauksen luotettavuuden varmistamiseksi tutkija dokumentoi huolellisesti kaikki tutkimusprosessin vaiheet ja teki tarkat muistiinpanot eri vaiheista. Tiedonhakuprosessi on kuvattu auki kuviossa 3. Kirjallisuuskatsauksen luotettavuutta on käsitelty tarkemmin luvussa 8.2.

Kuvio 3. Tiedonhaun PRISMA-kaavio (PRISMA flow diagram)

6.4 Laadunarviointi integratiivisessa kirjallisuuskatsauksessa

Integratiivisen kirjallisuuskatsauksen kolmannessa vaiheessa kerätyn lähdeaineiston laatu eli luotettavuus ja käyttökelpoisuus arvioidaan huolellisesti ennen sen käyttöä (Sulosaari & Kajander-Unkuri 2016, 111–112). Laadunarvioinnissa tarkastellaan valittujen tutkimusten toteutusta sekä niiden soveltuvuutta kirjallisuuskatsauksen tarkoitukseen ja asetettuun tutkimuskysymykseen. Yksityiskohtainen laadunarviointi tulee toteuttaa niille valikoidulle tutkimukselle, jotka ovat keskeisiä omalle kirjallisuuskatsaukselle. Tutkimuksien laatua arvioidaan luotettavuuden, pätevyyden, sovellettavuuden, siirrettävyyden ja yleistettävyyden käsitteiden kautta. (Vilkka 2023, 92–94.)

Tähän kirjallisuuskatsaukseen valikoitui eri tutkimusmenetelmin tehtyjä tutkimuksia. Aineisto sisälsi määrällisiä tutkimuksia 8kpl, monimenetelmällisiä tutkimuksia 7 kpl, tapaustutkimuksia 2kpl ja tilastotutkimuksia 1kpl. Kaikki tutkimukseen valikoituneet artikkelit olivat vertaisarvioituja tieteellisiä artikkeleita. Kirjallisuuskatsaukseen valikoitujen tutkimuksien laadun arvioimiseksi aineisto jäsenneltiin taulukkoon, johon kerättiin tiedot tekijöistä, julkaisuvuosi, maa, kuvaus tutkimuksen tarkoituksesta, menetelmästä ja otannasta sekä itse laadunarviointikriteerit. Laadunarvioinnin työkaluna käytettiin Kangasniemen, Pakkasen ja Korhosen (2015) luomaa kriteeristöä, joka havainnoi tutkimuksen tarkoitusta ja tavoitteita, tutkimusasetelmaa, teoreettista viitekehystä, tutkimuksen rajoituksia sekä keskustelua ja johtopäätöksiä. Arviointi toteutettiin kolmiportaisella asteikolla ”kyllä”, ”huono” tai ”ei raportoitu”. Kangasniemen ja kollegoiden luoma malli pohjautuu Bowlingin (2002) ja Gazarian (2013) tietoon arvioinnista. (Kangasniemi ym. 2015, 3, 5–7.) Laadunarvioinnin perusteella kaikki valikoidut tutkimukset otettiin mukaan kirjallisuuskatsaukseen. Laadunarvioinnin taulukko liitteessä 2.

6.5 Tutkimusaineiston analysointi

Kirjallisuuskatsauksen neljännessä vaiheessa kerätty aineisto analysoidaan. Analysointivaiheen tarkoituksena on tuloksien tasavertainen ja huolellinen tarkastelu sekä yksittäisten tutkimusten tulosten synteesi (Sulosaari & Kajander-Unkuri 2016, 112–114). Tämän kirjallisuuskatsauksen tulosten analyysi on toteutettu induktiivisena eli laadullisena sisällönanalyysinä, jonka tarkoituksena on järjestää hajallaan oleva aineisto selkeäksi tiiviiksi sanalliseksi kuvaukseksi tutkittavasta ilmiöstä. Aineiston analysoinnilla lisätään tutkittavan aiheen informaatioarvoa. (Tuomi & Sarajärvi 2018, 121–

122.) Elo & Kyngäs (2008) mukaan aineiston analyysi sisältää valmisteluvaiheen, analyysin ja raportointivaiheen. Valmisteluvaiheessa perehdytään aineistoon ja valitaan analyysiyksikkö. Sisällönanalyysivaiheessa aineistosta poimitaan tutkimuskysymykseen vastaavat alkuperäisilmaisut, aineisto pelkistetään ja koodataan sekä luokitellaan ja ryhmitellään. Raportointivaiheessa tulokset jaotellaan luokkiin, kategorioihin, malliin tai käsitejärjestelmään. (Elo, Kajula, Tohmola & Kääriäinen 2022, 2018–224.)

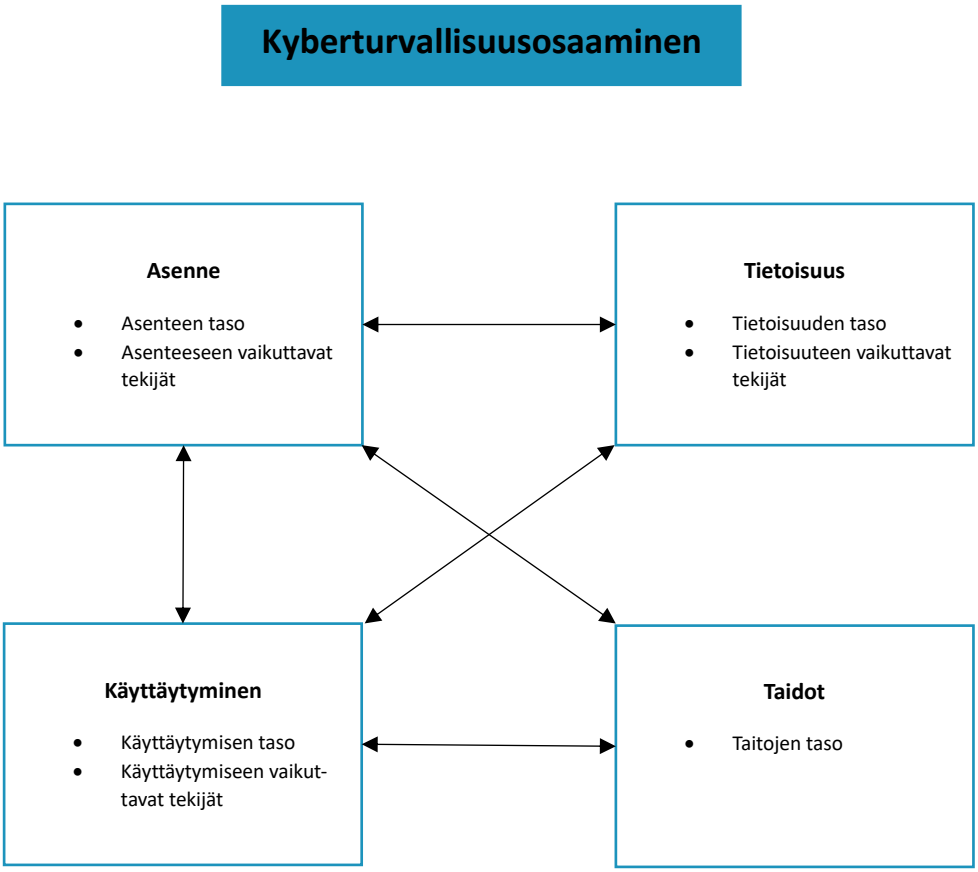
Tässä kirjallisuuskatsauksessa aineisto analysoitiin lukemalla tutkimusaineisto huolellisesti läpi useaan kertaan. Tutkimusaineistosta kerättiin aihetta käsittelevät alkuperäisilmaisukset, jotka pelkistettiin, ja joille muodostettiin alaluokka, yläluokka, pääluokka ja kokoava luokka. Analyysin loogista etenemistä alkuperäisilmauksesta yleiseen luokitteluun varmistettiin analyysipoluilla useamman kerran. Analyysista muodostuneita yläluokkia ja kokoavia luokkia hyödynnettiin tutkimuksen tuloksien raportoinnissa teemoina ja otsikoina. Esimerkki sisällönanalyysistä ja teema jaottelusta taulukossa 2.

Taulukko 2. Esimerkki sisällönanalyysistä

Alkuperäinen ilmaus	Pelkistys	Alaluokka	Yläluokka	Pääluokka	Kokoava luokka
77 % would decline the request (Share password)	77 % ei jaa kirjautumistietojaan kollegalle	Ei jaeta salasanaa ulkopuolisille	Salasanan turvallisuudesta huolehtiminen	Salasana käyttäytyminen	Kyberturvallisuus käyttäytyminen
They are not allowed to share passwords with colleagues	He eivät saa jaksaa salasanoja kollegoille				
Staff forgetting their passwords leads to selection of more predictable passwords	Sanasanojen unohtaminen, johtaa helppojen arvattavissa olevien salasanojen käyttöön	Salasanojen unohtaminen johtaa helppojen salasanojen käyttöön	Riittävän turvallisen salasanan käyttö		
31 % uses unique password	31 % käyttää uniikkia salasanaa	Uniikin salasanan käyttö			
Physicians.. demonstrated the lowest cybersecurity scores compared with nurses and administrators	Lääkäreillä alemmat pisteet kyberturvallisuus tietoisuudessa kuin hoitajilla tai johdolla	Lääkäreiden kyberturvallisuustietoisuus heikompaa kuin muilla ammattilaisilla	Ammatin vaikutus kyberturvallisuus tietoisuuteen	Kyberturvallisuus tietoisuuteen vaikuttavat tekijät	Kyberturvallisuus tietoisuus
Nurses performed better than doctors in the HAIS-Q, suggesting greater levels of cybersecurity awareness	Hoitajat suoriutuivat lääkäreitä paremmin HAISQ:sta, mikä viittaa hoitajien parempaan kyberturvallisuustietoisuuteen	Hoitajilla parempi kyberturvallisuus tietoisuus kuin lääkäreillä			

7 Tutkimustulokset

Integratiivisen kirjallisuuskatsauksen viidennessä eli viimeisessä vaiheessa tulokset tulkitaan ja esitetään. Tämä kappale käsittelee toteutetun kirjallisuuskatsauksen tuloksia, eli sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen nykytilaa ja sen kehittämistarpeita. Tulokset on jaoteltu analyysissä nousseiden kokoavien luokkien eli asenteen, tietoisuuden, taitojen ja käyttäytymisen osa-alueisiin sekä näiden yhteyden tarkasteluun. Viimeiseen alalukuun on koottu tutkimuksessa havaitut kyberturvallisuusosaamisen kehittämistarpeen. Kirjallisuuskatsauksen tuloksien jaottelu havainnollistettu kuviossa 4.



Kuvio 4. Kyberturvallisuusosaaminen kirjallisuuskatsauksen tuloksien pohjalta

7.1 Henkilöstön kyberturvallisuusasenne

Tässä kappaleessa tarkastellaan sosiaali- ja terveydenhuollon kyberturvallisuusasennetta ja siihen vaikuttavia tekijöitä. Tulokset on kuvattu taulukossa 3.

7.1.1 Asenteen taso

Tutkimuksien mukaan sosiaali- ja terveydenhuollon henkilöstön asenne teknologisia laitteita, digitaalisia palveluita ja näiden kyberturvallisuutta kohtaan on keskimääräistä. Tutkimukset osoittavat, että työntekijöillä on innostusta ja myönteinen asenne uudenlaisten teknologisten palveluiden käyttöönottoa kohtaan, mutta samanaikaisesti esiintyy epävarmuutta ja pelkoa näiden käyttöön liittyen. (Morris, Brusco, Jones, Taylor, East, Semciw, Edvardsson, Thwaites, Bourke, Khan, Fowler-Davis & Oldenburg 2023, 6.) Epävarmuuden ja pelon ohella työntekijöiden keskuudessa on havaittu myös välinpitämättömyyttä kyberturvallisuutta kohtaan, mikä on yhteydessä heidän kyberturvalliseen käyttäytymiseensä (Kessler, Pindek, Kleinman, Andel & Spector 2020, 462, 470; Yeo & Banfield 2022).

Magdalinou, Kalokairinou, Malamateniou ja Mantas (2022, 26) ovat todenneet kreikkalaisessa sairaalassa työskentelevien sairaanhoitajien asenteen tietoturvallisuuskäytäntöjä kohtaan hyväksi. Gebeyew, Wordofa, Muluneh, Shibabaw, Walle, Tizie, Mengistie, Takillo,Assaye, Senishaw, Hailye, Shimie ja Buttan mukaan etiopialaisen opetussairaalan henkilöstöstä hieman alle kolmannes (60,9 %) omaa suotuisan asenteen tietoturvallisuuskäytäntöjä kohtaan. Tutkimuksessa näiden toisistaan hieman poikkeavien tutkimustulosten on esitetty johtuvan maiden välisistä eroista resursseissa. Kehittyvissä maissa työntekijöiden asenteeseen saattaa vaikuttaa asianmukaisten teknologisten laitteiden saatavuus ja koulutuksen määrä tai näiden puutteet. (Gebeyew ym. 2024, 7.)

7.1.2 Yksilön tekijöiden ja ammatin vaikutus asenteeseen

Tutkimuksessa on pyritty tunnistamaan yksilöön liittyviä tekijöitä, jotka ennustavat työntekijän kyberturvallisuusasenteen tasoa. Kang, Kang ja Monsen (2022, 4) ovat tunnistaneet sukupuolella olevan vaikutusta asenteen tasoon. Nunes, Antunes ja Silva (2021, 179) eivät puolestaan tunnistaneet tilastollisesti merkittävää yhteyttä sukupuolen ja asenteen tai iän ja asenteen välillä. Tutkimuksissa

on havaittu, että työntekijät, joilla on sovinnollisuuden ja avoimuuden luonteenpiirteitä, suhtautuvat kyberturvallisuuteen myönteisemmin verrattuna muuhun henkilöstöön (Yeng, Fauzi & Yang 2022, 18).

Kyberturvallisuusasenteisiin on tunnistettu olevan vaikutusta työntekijän edustamalla ammattiryhmällä (Kessler ym. 2020, 469; Nunes ym.2021, 179). Kessler ja muiden (2020, 469) mukaan farmaseutit ovat asenteeltaan muita ammattiryhmiä positiivisempia sekä motivoituneempia erilaisia kyberturvallisuus toimenpiteitä kohtaan. Nunes ja muut (2021 ym. 179) ovat tunnistaneet ammatin vaikutuksen yksittäisiin kyberturvallisuusasennetta mittaaviin tekijöihin, mutta tilastollisesti merkittävää yhteyttä ei ole löytynyt asenteen ja ammatin välillä.

Kang ja muut ovat tunnistaneet tilastollisesti merkittävän yhteyden kyberturvallisuusasenteen ja työntekijän aseman välillä. Tutkimuksessa on todettu, että esihenkilöiden ja johtoportaan asenteet kyberturvallisuutta kohtaan ovat myönteisempiä verrattuna rivitason työntekijöihin. Tämän taustalla on pohdittu esihenkilöiden tarvetta toimia esimerkkinä johdettavilleen. (Kang ym. 2023, 4.) Lisäksi työntekijän ammatillisen tutkinnon laajuus ja taso voivat ennakoida asennetta kyberturvallisuutta kohtaan. Korkeamman koulutustason omaavat työntekijät osoittavat yleensä myönteisempiä asenteita kyberturvallisuutta kohtaan. (Gebeyew ym. 2024, 6.)

7.1.3 Kyberturvallisuuskoulutuksen vaikutus asenteeseen

Kang ja muut ovat tunnistaneet saadulla kyberturvallisuuskoulutuksella olevan merkittävä vaikutus työntekijöiden kyberturvallisuusasenteeseen. Koulutuksen saaneet työntekijät olivat kyberturvallisuusasenteeltaan merkittävästi myönteisempiä kuin kouluttamattomat työntekijät. Tutkimuksessa on lisäksi tunnistettu, että työntekijän kokemus saadun koulutuksen hyödyllisyydestä oman työn kannalta on merkittävä ennakoija positiiviselle asenteelle. (Kang ym. 2023, 4.) Hore, Tan, Kehoe, Beegan, Manson, Al Mane, Hughes, Kelly, Wells ja Magnerin (2024, 3) mukaan kuitenkin pieni osa henkilöstöstä (4 %) raportoi, ettei ollut lainkaan kiinnostunut kyberturvallisuuskoulutukseen osallistumisesta, mikä herättää huolta yleisen kyberturvallisuuden kannalta. Tutkimuksen mukaan sosiaali- ja terveydenhuollon työntekijät, jotka tunnistavat digitaalisuuden ja kyberturvallisuuden hyödyt omassa työssään, omaavat suotuisamman asenteen kyberturvallisuutta kohtaan (Dart & Ahmed 2023, 12; Gebeyew ym. 2024, 6 &7).

Taulukko 3. Kyberturvallisuusasenne ja siihen vaikuttavat tekijät

Asenteen taso	Asenteeseen vaikuttavat tekijät
Asenne teknologisia laitteita, digitaalisia palveluita ja näiden kyberturvallisuutta kohtaan on keskimääräistä	Sukupuoli - Sukupuolella vaikutus asenteen tasoon - Ei tilastollisesti merkittävää yhteyttä
Innostusta ja myönteistä asennetta, mutta samanaikaisesti epävarmuutta ja pelkoa uudenlaisten teknologisten palveluiden käyttöä kohtaan	Sovinnollisuus ja avoimuus ennakoivat positiivista asennetta
Välinpitämättömyys	Ammattiryhmä vaikuttaa asenteeseen
Asenne tietoturvallisuuskäytäntöjä kohtaan - Asenne tietoturvallisuuskäytäntöjä kohtaan hyvää - 60,9 % omaa suotuisan asenteen tietoturvallisuuskäytäntöjä kohtaan	Työntekijän asema - Tunnistettu vaikuttavan asenteeseen - Korkeampi positio ennakoi positiivisempaa asennetta
	Korkeampi koulutustausta ennakoi positiivisempaa asennetta
	Kyberturvallisuuskoulutus vaikuttaa asenteeseen
	Digitaalisuuden ja kyberturvallisuuden hyödyt omassa työssään tunnistavat asenteeltaan positiivisempia

7.2 Henkilöstön kyberturvallisuustietoisuus

Tässä kappaleessa tarkastellaan sosiaali- ja terveydenhuollon kyberturvallisuustietoisuutta ja siihen vaikuttavia tekijöitä. Tulokset on kuvattu taulukossa 4.

7.2.1 Tietoisuuden taso

Tutkimukset ovat osoittaneet sosiaali- ja terveydenhuollon ammattilaisten kyberturvallisuustietoisuuden olevan hyvällä tasolla tarkasteltaessa isompaa joukkoa ammattilaisia. Terveydenhuollon henkilöstö on suoriutunut erilaisista kyber- ja tietoturvallisuustietoisuutta mittaavissa testeissä keskiarvolta hyvin. (Albabtain, AlOtaibi, AlMazial, Aloudah, Alghosoon, Arafat, 2024, 97& 99; Hore ym. 2024, 2 & 5; Magdalinou ym. 2022, 26). Yleisesti ottaen hyvien tulosten taustalla on kuitenkin havaittavissa henkilöstön kyberturvallisuustietoisuuden laaja vaihteluväli. Tutkimuksissa enemmistö työntekijöistä suoriutui testeistä ja itsearvioista hyvillä arvosanoilla, mutta joukosta erottuu myös muutamia heikosti testeistä suoriutuneita yksilöitä. (Albabtain ym. 2024, 99; Hore ym. 2024, 2 & 5.) Yksikin heikon tietoisuuden omaava työntekijä voi toiminnallaan vaarantaa yrityksen kyberturvallisuuden ja tuottaa täten uhkaa organisaation toiminnalle.

Sosiaali- ja terveydenhuollon henkilöstön tietoisuus organisaation kyberturvallisuutta ylläpitävistä protokollista ja käytännöistä on tutkimuksien perusteella vaihtelevaa. Löydökset vaihtelevat hyvän ja heikon tietoisuuden välillä. Magdalinou ja muiden (2022, 26) mukaan ammattilaisten tietoisuus kyberturvallisista käytännöistä on hyvällä tasolla. Dart ja Ahmed ovat puolestaan todenneet henkilöstön puutteellisen tietoisuuden tietoturvallisuusohjeistuksista. Työntekijöistä kolme neljästä (76,8 %) koki, ettei kyberturvallisuusrikkomuksia juurikaan tapahdu omassa organisaatiossa. Kolmasosa (34 %) puolestaan ilmoitti, ettei ollut tietoinen yhdestäkään tietoturvarikkeestä viimeisen viiden vuoden aikana (Dart & Ahmed 2023, 10 & 13), mikä viittaa mahdollisesti työntekijöiden puutteellisen kyberturvallisuustietoisuuteen.

7.2.2 Ammatin ja kyberturvallisuuskoulutuksen vaikutus tietoisuuteen

Tutkimukset ovat osoittaneet sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuustietoisuuden olevan riippuvaista työntekijän ammattiryhmästä ja aikaisemmasta työkokemuksesta. Tutkimuksien mukaan sairaanhoitajat ovat suoriutuneet kyberturvallisuustietoisuutta mittaavista testeistä muita ammattiryhmiä paremmin tai yhtävertaisesti. Kyberturvallisuustietoisuuden osalta heikoimmin suoriutuneeksi ammattiryhmäksi on tunnistettu lääkärit. (Albabtain ym. 2024, 99; Alhuwail, Al-Jafar, Abdulsalam & AlDuaij 2021, 930; Hore ym., 2& 5; Schmidt, Nøhr & Koppel 2021, 638). Schmidt ja muut (2021, 638) ovat tunnistaneet työuran pituuden ja työvuosien tuoman ammatillisen kokemuksen positiiviset vaikutukset työntekijän kyberturvallisuustietoisuuteen.

Albabtain ja muut ovat todenneet kyberturvallisuustietoisuuden olevan parempaa terveydenhuollon ammattilaisilla, jotka ovat osallistuneet potilastyön lisäksi kliiniseen tutkimukseen. Kliiniseen tutkimukseen osallistunut henkilöstö on joutunut huomioimaan kyberturvallisuuden näkökulmaa suoraa potilastyötä tekevää henkilöstöä enemmän, johtuen kliinisen tutkimuksen valvonnan vaatimuksista. (Albabtain ym. 2024, 99). Organisaation muodolla, jossa ammattilainen työskentelee, ei ole havaittu olevan yhteyttä työntekijöiden kyberturvallisuustietoisuuden tasoon (Alhuwail ym. 2021, 930).

Kyberturvallisuustietoisuuteen on tunnistettu lisäksi vaikuttavan työntekijälle tarjottu kyberturvallisuuskoulutus ja -ohjelmat. Kyberturvallisuuskoulutuksen ja -ohjelmien, kuten Seta-ohjelman (se-

curity education, training and awareness program), läpikäyneet työntekijät suoriutuivat kyberturvallisuustietoisuutta mittaavista testeistä paremmin verrattuna kouluttamattomiin työntekijöihin. (Kuo, Talley & Lin 2021, 9.)

Taulukko 4. Kyberturvallisuustietoisuus ja siihen vaikuttavat tekijät

Tietoisuuden taso	Tietoisuuteen vaikuttavat tekijät
Tietoisuus yleisesti hyvää, muutamia heikon tietoisuuden omaavia	Tietoisuus riippuvaista työntekijän ammattiryhmästä
Tietoisuudessa merkittävää vaihteluväliä	Pitkä työura ja kokemus ennakoivat parempaa tietoisuutta
Tietoisuus organisaation kyberturvallisuusohjeistuksista ja -protokollista - Tietoisuus hyvää - Puutteellinen tietoisuus	Tietoisuus parempaa kliiniseen tutkimukseen osallistuneilla
	Tietoisuuteen vaikuttaa kyberturvallisuuskoulutus ja -ohjelmat

7.3 Henkilöstön kyberturvallisuustaidot

Tässä kappaleessa tarkastellaan sosiaali- ja terveydenhuollon kyberturvallisuustaitoja. Tulokset on kuvattu taulukossa 5.

7.3.1 Kyberturvallisuustaitojen taso

Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuustaidot ovat tutkimuksien mukaan keskimääräistä tai hyvää (Hore ym. 2024, 5; Morris ym. 2023, 3 & 5). Hyvästä kyberturvallisuustaitotasosta huolimatta työntekijät ovat raportoineet epävarmuutta omaa osaamistaan kohtaan (Hore ym. 2024, 5). Morrisin ja muiden mukaan henkilöstö on lisäksi raportoinut epävarmuutta olemassa olevista digitaalisista alustoista ja näiden käytöstä. Työntekijöiden epävarmuuteen on tunnistettu vaikuttavan teknologian nopea kehitys, mikä luo kasvavan kuilun henkilöstön osaamisen ja laitteiden kehittymisen välille. (Morris ym. 2023, 5–6.) Gebeyew ja muiden (2024, 5) mukaan henkilöstöstä hieman alle puolet (45,3 %) kokevat kyber- ja tietoturvallisuuden ylläpitämiseen liittyvien työkalujen käytön haastavana. Tutkimuksen tulosta tarkastellessa tulee huomioida tutkimuksen toteuttaminen kehittyvässä valtiossa. Kyseisen tutkimukseen osallistuneista työntekijöistä vain

noin kahden kolmesta (63 %) on todettu olevan pätevä digilukutaidon suhteen (Gebeyew ym. 2024, 5).

7.3.2 Kyberhygieniset taidot

Kyberhygienisistä taidoista salasanakäytäntöjen hallinnan on arvioitu olevan hyvää tai keskimääräistä. Sähköisen viestinnän on puolestaan todettu olevan keskimääräistä. Keskimääräistä tai välttävää taitoa on taas tunnistettu internetin käytön suhteen. Henkilöstö on raportoinut saavansa vierailla työajalla millä tahansa nettisivuilla. Tutkimusten perusteella työntekijöiden tietojenkäsittelytaidot ovat keskimääräiset. (Magdalinou ym. 2022, 25–26.) Alhuwail ja muiden mukaan työntekijöistä noin kaksi kolmasosaa (63 %) raportoi hallitsevansa salattujen tietojenkäsittelyn protokollat hyvin ja toimivansa organisaation asettamien ohjeiden mukaisesti. Yllättävänä tutkimustuloksena tutkijat havaitsivat, että eniten internetiä käyttävillä työntekijöillä oli heikoimmat taidot kyberturvallisuutta koskevien ohjeistusten osalta. (Alhuwail ym. 2021, 930 & supplementary material)

7.3.3 Kyberuhkien tunnistaminen ja raportointi

Sosiaali- ja terveydenhuollon henkilöstöstä noin kaksi viidesosaa ilmaisi epävarmuutta taidossa tunnistaa kyberhyökkäys (42 %) tai ylipäänsä keskustella kyberturvallisuudesta työpaikalla (36 %). Lisäksi vain pieni osa (15 %) ammattilaisista pystyi nimeämään kolme esimerkkiä haittaohjelman tunnistamiseksi. Poikkeuksena muuten heikkoon taitotasoon kyberuhkien suhteen, henkilöstön taito tunnistaa kohdistetut kalasteluyritykset olivat hyvät. (Hore ym. 2024, 4–5.)

Sosiaali- ja terveydenhuollon työntekijöiden taito kyberuhkien, -rikkeiden tai -onnettomuuksien raportoimisesta vaihtelee tutkimuksien välillä. Hore ja muiden (2024, 2) sekä Alhuwail ja muiden (2021, supplementary material) mukaan työntekijöistä noin kaksi viidestä (41 % / 39 %) koki osaavansa raportoida tietovuodon asianmukaisesti eteenpäin. Magdalinou ja muiden (2022, 25) mukaan tietoturvarikkeiden ilmoittamisen taito henkilöstön keskuudessa on puolestaan keskimääräistä tai hyvää.

Taulukko 5. Kyberturvallisuustaidot ja siihen vaikuttavat tekijät

Taitojen taso
Taidot keskimääräiset tai hyvät
Hyvistä taidoista huolimatta, epävarmuutta omasta osaamisesta
45,3 % koki kyber- ja tietoturvallisuustyökalujen käytön haastavana
Salasanakäytäntöjen hallinta hyvää tai keskimääräistä
Sähköinen viestintä keskimääräistä
Internetin käyttö keskimääräistä tai välttävää
Tietojenkäsittely - Keskimääräistä - 63 % hallitsee tietojenkäsittelyn protokollat hyvin
Kyberhyökkäyksien tunnistaminen - 42 % epävarma taidostaan tunnistaa kyberhyökkäys - 15 % osasi nimetä 3 erimerkkiä haittaohjelman tunnistamiseksi - Kalasteluyrityksien tunnistus hyvää
36 % epävarma taidostaan keskustella kyberturvallisuudesta työpaikalla
Kyberuhkien, -rikkeiden tai -onnettomuuksien raportoiminen - Kaksi viidestä (41 % ja 39 %) koki osaavansa raportoida tietovuodon - Tietoturvarikkeiden ilmoittaminen keskimääräistä tai hyvää

7.4 Henkilöstön kyberturvallisuuskäyttäytyminen

Tässä kappaleessa tarkastellaan sosiaali- ja terveydenhuollon kyberturvallisuuskäyttäytymistä ja siihen vaikuttavia tekijöitä. Tulokset on kuvattu taulukossa 5.

7.4.1 Käyttäytymisen taso

Henkilöstön kyberturvallisuusosaaminen ilmenee työympäristöissä käyttäytymisen muodossa. Tutkimuksien perusteella sosiaali- ja terveydenhuollon ammattilaisten kyberturvallisuuskäyttäytyminen näyttäytyy vaihtelevana. Tutkimustulokset osoittavat, että työntekijöiden kyberturvallisuuskäyttäytyminen vaihtelee hyvästä ja keskimääräisestä aina välttävään ja heikkoon, mikä luo kokonaisuudesta hajanaisen ja epäyhtenäisen kuvan. (Alhuwail ym. 2021, supplementary material; Hore ym. 2024, 5; Magdalinou ym. 2022, 26; Nunes ym. 2021, 178–179).

Tutkimuksissa on tunnistettu työntekijöiden keskuudessa olevan välinpitämätöntä ja huolimatonta kyberturvallisuuskäyttäytymistä (Kessler ym. 2020, 462, 470; Yeo & Banfield 2022). Yeo ja Banfieldin (2022) mukaan suurin osa sosiaali- ja terveydenhuollon palveluissa toteutuneista tietovuodoista tai kyberrikkeistä johtui työntekijöiden välinpitämättömyydestä ja huolimattomuudesta. Tutkimuksessa on ehdotettu, että asiattoman kyberturvallisuuskäyttäytymisen taustalla voi olla työntekijän kokemus kyberuhan toteutumisen epätodennäköisyydestä omalla kohdalla. (Hore ym. 2024, 5). Välinpitämättömyyden ja huolimattomuuden lisäksi sosiaali- ja terveydenhuollon työntekijöiden keskuudessa on tunnistettu käyttäytymismalleja, joissa vastuu kyberturvallisuudesta pyritään kiertämään tai siirtämään muille. Useat työntekijät kokevat, että vastuu kyberturvallisuudesta kuuluu organisaation IT-osastolle tai tietohallinnolle, eikä ole heidän omalla vastuullaan. (Dart & Ahmed 2023, 10; Hore ym. 2024, 2.)

Henkilöstön keskeinen keino ylläpitää organisaation kyberturvallisuutta on toimia organisaation annettujen kyberturvallisuusohjeiden ja -käytäntöjen mukaisesti. Alhuwail ja muiden (2021, supplementary material) mukaan työntekijöistä kaksi kolmesta (65 %) kertoo noudattavansa annettuja kyberturvallisuusohjeita asianmukaisesti kaikessa toiminnassaan. Työntekijöistä kuitenkin vain puolet (49,5 %) koki, ettei poikkeaisi annetuista turvaohjeista edes potilaan parhaan hoidon saavuttamiseksi (Dart & Ahmedin 2023, 10). Työntekijöiden valmius rikkoa tai kiertää kyberturvallisuusohjeita potilaan etua tavoiteltaessa, viestii kyberrikkeen tai -uhkan mahdollisuudesta kriittisessä hoitotilanteessa.

7.4.2 Verkkoyhteyden käyttö

Teknologisten lääkintälaitteiden ja muiden digitaalisten laitteiden, kuten tietokoneiden, tablettien ja älypuhelimien, turvallisen käytön yhtenä perustana on suojatun verkkoyhteyden käyttäminen. Hore ja muiden mukaan henkilöstö valitsee pääsääntöisesti käyttöönsä sairaalan suojatun ja turvatun verkkoyhteyden. Poikkeuksena on kuitenkin raportoitu tapauksia, joissa työntekijät vikatilanteiden ilmetessä turvautuvat julkisiin verkkoyhteyksiin tai henkilökohtaisen mobiilitukiaseman käyttöön. Tämä toimintamalli saattaa heikentää organisaation kyberturvallisuuskäytäntöjen toteutumista ja altistaa tietojärjestelmät tietoturvariskeille (Hore ym. 2024, 5.) Alhuwail ja muiden (2021, supplementary material) mukaan työntekijöistä neljännes (26 %) on raportoinut yhdistäneensä henkilökohtaisen älylaitteen sairaalan verkkoon, mikä voi toimia väylänä kyberhyökkäyksen levittämisessä.

7.4.3 Kirjautumiskäyttäytyminen

Sosiaali- ja terveydenhuollon tietojärjestelmiin kirjauduttaessa on keskeistä ylläpitää turvallisia kirjautumiskäytäntöjä. Tutkimuksien mukaan sosiaali- ja terveydenhuollon henkilöstö tiedostaa henkilökohtaisten salasanojen jakamisen ulkopuoliselle henkilölle olevan kiellettyä. Neljä viidestä (74 %) työntekijästä raportoi, ettei ole koskaan jakanut salasanaansa kollegalleen tai muulle osapuolelle. (Alhuwail ym. 2021, supplementary material; Hore ym. 2024, 4).

Henkilöstön salasanakäyttäytymisessä on kuitenkin tunnistettu puutteita riittävän turvallisen ja uniikin salasanan asettamisessa. Työntekijöistä vain kolmannes (31 %) käyttää riittävän monimuotoista ja yksilöllistä salasanaa kirjautuessaan terveydenhuollon järjestelmiin. (Alhuwail ym. 2021, supplementary material). Syyksi ”helppojen” salasanojen käytölle on raportoitu haaste muistaa monimutkaiset ja jatkuvasti päivittyvät salasanat (Hore ym. 2024, 5). Henkilöstöstä 15 % on raportoinut kirjoittaneensa salasanan itselleen ylös yleisestä kiellosta huolimatta (Alhuwail ym. 2021, supplementary material).

Vastoin hyviä kyberturvallisiakäytäntöjä sosiaali- ja terveydenhuollon työntekijät ovat raportoineet kokevansa turvalliseksi käyttää samaa salasanaa sekä työpaikan järjestelmissä että henkilökohtaisissa vapaa-ajan ja sosiaalisen median palveluissa. (Magdalinou ym. 2022, 26). Saman salasanan käyttö useissa eri järjestelmissä lisää sekä terveydenhuollon järjestelmien että yksilön henkilökohtaisten tietojen turvallisuusriskiä.

Sosiaali- ja terveydenhuollon työntekijöistä kaksi kolmasosaa (61,5 %) on raportoinut tietokoneelle kirjautumisen olevan helppoa (Mohammed, Chandran, Mansoor & Mohaddis 2021, 5–7). Turvallisen terveydenhuollon laitteisiin ja järjestelmiin kirjautumisen lisäksi on keskeistä suojata käytössä olevat laitteet myös poistuttaessa työvälineeltä. Alhuwail ym (2021, supplementary material) mukaan vain reilu kolmannes (35 %) työntekijöistä käyttää lukittua näyttöä poistuttaessa älylaitteelta. Työntekijöistä reilu neljännes (23 %) raportoi, ettei tiennyt tietokoneen auki jättämisen olevan tietoturvallisuusrikkomus ja vain kolmannes (30 %) koki tietokoneen sulkemisen säännön tärkeäksi noudattaa. (Mohammed ym. 2021, 5–7).

Mohammed ja muut ovat tutkineet havainnoinnin ja haastattelun keinoin terveydenhuollon henkilöstön tietokoneiden lukitsemiskäytäntöjä ja syitä tämän taustalla. Tutkimuksen ensimmäisellä havainnointi kerralla lukitsemattomia tietokoneita löytyi 18kpl/ 58kpl ja toisella kerralla 15kpl/ 110kpl. Ensimmäisellä havainnointi kerralla avoinna olevista tietokoneista 22 %:ssa ja toisella havainnointi kerralla 20 %:ssä oli useampi käyttäjä samanaikaisesti. Havainnointitilanteiden jälkeen toteutetuissa haastatteluissa tutkittavat kuvasivat tietokoneiden auki jättämisen syiksi mm. tietojen menettämisen pelon, toisen asian ilmaantumisen, pikaisen poistumisen ja palaamisen tilanteeseen sekä vapaiden tietokoneiden vähyyden. (Mohammed ym. 2021, 5–7.)

7.4.4 Tietojenkäsittely

Terveydenhuollon ammattilaisista kolme neljästä (74 %) raportoi varmistavansa aina, ettei ulkopuolisilla ole näköyhteyttä tai pääsyä tietoihin potilastietoihin näitä käsiteltäessä. (Alhuwail ym. 2021, supplementary material.) Työntekijöistä pieni osa (10 %) kertoo jakaneensa arkaluonteisia tietoja ulkopuoliselle rikkoen potilaan yksityisyydensuojaa (Alhuwail ym. 2021, supplementary material; Yeo ja Banfield 2022). Lisäksi henkilöstöstä hieman alle kolmannes (29 %) on raportoinut rikkoneensa virkavelvollisuutta ja katsoneensa potilastietoja ilman hoitosuhdetta potilaaseen. Työntekijöistä pieni osa on myös (9 %) on raportoinut ladanneensa potilastietoja käyttöönsä kotona ilman tarvittavia oikeuksia. (Alhuwail ym. 2021, supplementary material.)

Tutkimuksien mukaan sosiaali- ja terveydenhuollon työntekijöiden kyberturvallisuuskäyttäytyminen ulkoisten tiedostojen kuten USB-muistitikkujen käytössä on hyvää. Työntekijät raportoivat, etteivät yhdistä vieraita USB-tikkuja työlaitteisiin, koska ovat tietoisia näiden riskeistä ja mahdollisuudesta välittää virus tai haittaohjelma laitteeseen. (Hore ym. 2024, 4; Magdalinou ym. 2022, 26.) Työntekijät raportoivat lisäksi välttävänsä erinäisten tiedostojen lataamista työlaitteilleen kyberuhkien ehkäisemiseksi. Työn kannalta välttämättömiä tiedostoja ladattaessa, työntekijät kertovat huomioivansa tiedoston turvallisuuden ja valitsevat käyttöönsä sairaalan turvatun verkkoyhteyden. (Alhuwail ym. 2021, supplementary material; Magdalinou ym. 2022, 26.) Yeo ja Banfieldin (2022) mukaan vain muutama prosentti toteutuneista tietovuodoista tai rikkeistä on aiheutunut työntekijän ladatessa turvattomia tiedostoja laitteelle tai hukatessa tiedostoja.

7.4.5 Sähköinen viestintä ja henkilökohtaisten älylaitteiden käyttö

Sosiaali- ja terveydenhuollon työntekijöiden sähköisen viestinnän ja tämän turvallisuuden on todettu olevan keskimääräistä (Magdalinou ym. 2022, 25). Alhuwail ja muiden (2021, supplementary material) mukaan työntekijöistä vain pieni osa (10 %) on hyödyntänyt omaa henkilökohtaista sähköpostia potilastietojen viestinnässä. Poikkeuksena yleisesti hyvään sähköisen viestinnän käyttäytymiseen sosiaali- ja terveydenhuollon palveluissa on havaittu työntekijöiden yhteiskäytössä olevia sähköposteja, joissa viestitään potilasasioista. Henkilöstön yhteinen ja avoin käytössä oleva sähköposti rikkoo potilaiden tietosuojaa sekä altistaa tietovuodoille. (Hore ym. 2024, 5.)

Henkilökohtaisten älylaitteiden käyttö on yleistynyt merkittävästi sosiaali- ja terveydenhuollon työtehtävissä. Työntekijät raportoivat hyödyntävänsä omia älylaitteitaan tiedonhaussa, tiedon säilytyksessä sekä viestinnässä potilaiden ja kollegoiden kanssa. Tutkimuksien mukaan henkilökohtaisia älylaiteita käytettäessä työntekijät unohtavat herkästi kyberturvalliset käytänteet ja toimivat potilaan kannalta tietoturvattomasti. (Albabtain ym. 2024, 98; Dart & Ahmed 2023, 15.)

7.4.6 Kyberuhka- tai hyökkäys tilanteessa käyttäytyminen

Teknologisia laitteita käytettäessä sosiaali- ja terveydenhuollon ammattilaisten on tärkeää tiedostaa kyberhyökkäyksien mahdollisuus. Tutkimuksien perusteella työntekijöiden käyttäytyminen kyberhyökkäystilanteessa näyttäytyy vaihtelevana. Kvantitatiivisilla menetelmillä toteutetuissa tutkimuksissa henkilöstön taito tunnistaa kalasteluyritykset näyttäytyy hyvänä (Alhuwail ym. 2021, supplementary material; Yeo & Banfieldin 2022). Kun taas terveydenhuollon ammattilaisille toteutetuissa simulaatiotutkimuksissa työntekijöiden kyky tunnistaa erilaisia kyberhyökkäyksiä ja toimia tilanteessa kyberturvallisesti näyttäytyy puutteellisena (Jalali, Bruckes, Westmattelmann & Schewen 2020, 6 & 8; Rizzoni, Magalini, Casaroli, Mari, Dixon & Coventry 2022, 5–6; Willing, Dresen, Gerlitz, Haering, Smith, Binnewies, Guess, Haverkamp ja Schinzel 2021).

Alhuwail ja muiden (2021, supplementary material) sekä Yeo ja Banfieldin (2022) mukaan työntekijöistä reilu kymmenes (15 %) on raportoinut avanneensa vaaralliseksi osoittautuneen viestin tai linkin ja täten mahdollisesti aiheuttaneensa uhkaa organisaation kyberturvallisuudelle. Sosiaali- ja terveydenhuollon palveluissa toteutetuissa simulaatioharjoituksissa kuitenkin työntekijöiden kalasteluviesteihin lankeaminen oli merkittävää.

Rizzonin ja muiden kolmivaiheisessa kalastusviesti-simulaatiossa sairaalan henkilöstölle lähetettiin standardoituja ja kustomoituja kalasteluviestejä. Ensimmäisessä simulaatiossa lähetetyistä standardoiduista viesteistä reilu kolmannes (36 %) avattiin ja kustomoiduista viesteistä kaksi kolmasosaa (62 %). Standardoidun viestin avanneista vajaa viidennes (18 %) klikkasi viestin linkkiä ja kustomoidun viestin avanneista yhdeksän kymmenestä (88 %) klikkasi linkkiä. Toisella viestikierroksella lähetettiin pelkästään kustomoituja viestejä, joista vajaa kaksi kolmesta (58 %) avattiin. Viestin avanneista lähes yhdeksän kymmenestä (87 %) klikkasi viestin linkkiä. Kolmannella kierroksella lähetettiin vain standardoituja viestejä, joista reilu kaksi viidestä (44 %) avattiin. Viestin avanneista vain alle kymmenes (7 %) klikkasi linkkiä. (Rizzoni ym. 2022, 5–6.)

Jalali ja muiden tutkimuksessa kalasteluviestejä lähetettiin kahden eri sairaalan henkilöstölle. Sairaalan A simulaatiossa 122 työntekijää klikkasi lähetettyä linkkiä ja 50 ei eli työntekijöistä n. 70 % lankesi kalasteluviestiin. Sairaalan B simulaatiossa 110 työntekijää klikkasi linkkiä ja 116 ei eli työntekijöistä 48 % lankesi kalasteluviestiin. Tutkimuksessa kalasteluviesteihin lankeamisen yhdeksi syyksi tunnistettiin työkuorma. (Jalali ym. 2020, 6 & 8)

Willing ja muut ovat puolestaan toteuttaneet kyberhyökkäys simulaation päivystysvalvontaosaston sairaanhoitohenkilökunnalle. Simulaatiossa tehohoidon valvontalaitteeseen kohdistettiin kyberhyökkäys. Sairaanhoitajien taito tunnistaa kyberhyökkäys vaihteli merkittävästi. Kahdestakymmenestä (20) simulaatioon osallistuneesta sairaanhoitajasta kaksitoista (12) hoitajaa suoriutui harjoituksesta hyvin ja kahdeksan (8) heikosti. Hyvin suoriutuneet hoitajat tunnistivat laitteiden teknisen ongelman ja korjasivat potilaan hoitoa sen mukaisesti. Kymmenen (10) hyvin suoriutunutta sairaanhoitajaa oli simulaation aikana yhteydessä IT-tukeen teknisestä ongelmasta ja pyysi apua tilanteeseen. Hyvin suoriutuneiden sairaanhoitajien ryhmästä kuitenkin vain yksi (1) suoriutui simulaatiosta ilman vihjeitä. Heikosti suoriutuneiden kahdeksan (8) sairaanhoitajan joukosta kolme (3) hoitajaa ei tunnistanut kyberhyökkäystä koko simulaation aikana. (Willing ym. 2021.)

Kyberturvallisuusrikkeiden ja -uhkien eteenpäin raportointi on yksi keskeinen keino edistää organisaation kyberturvallisuutta. Henkilöstöstä reilu viidennes (22 %) on ilmaissut epävarmuuttaan siitä, miten toimia kyberrikettä ilmoitettaessa ja jopa reilu kymmenes (12 %) on raportoinut jättäneensä kyberrikkeen ilmoittamatta. Työntekijöistä neljännes (22 %) on myöntänyt, että ei koe olevansa vastuussa toteutuneiden rikkeiden ilmoittamisesta. (Hore ym. 2024, 2 & 5). Dart ja Ahmed (2023,

10) mukaan henkilöstöstä kolme neljästä (74 %) kertoo, ettei ole ikinä raportoinut kyberrikettä, mikä kertoo mahdollisesti rikkeiden raportointikäytäntöjen puutteellisesta hallinnasta. Työntekijöistä suuri osa kuitenkin ilmaisee raportoivansa kollegan tahalliset tai tahattomat rikkeet eteenpäin (Hore ym. 2024, 2; Magdalinou 2022, 25–26).

7.4.7 Yksilön tekijöiden vaikutus käyttäytymiseen

Kyberturvallisuuskäyttäytymiseen on tunnistettu vaikuttavan lukuisia erilaisia yksilöön liittyviä tekijöitä. Kessler ja muiden sekä Alhuwail ja muiden mukaan naiset ovat toiminnassaan kyberturvallisempia kuin miehet. Naisten on todettu noudattavan tietoturvallisia käytänteitä miehiä useammin, minkä seurauksena heidän riskikäyttäytymisensä on vähäisempää. (Alhuwail ym. 2021, 929; Kessler ym. 2020, 467.) Nunes ja muut (2021, 177–178) eivät puolestaan ole tunnistaneet tilastollisesti merkittävää yhteyttä riskikäyttäytymisen ja sukupuolen välillä.

Sukupuolen lisäksi on tutkittu iän vaikutusta kyberturvalliseen käyttäytymiseen. Tutkimusten tulokset ovat olleet eriäviä. Kessler ja muut ovat todenneet vanhempien työntekijöiden olevan varovaisempia toiminnassaan ja aiheuttaen täten vähemmän tietoturvauhkia. Iäkkäämpien työntekijöiden on lisäksi todettu olevan halukkaampia osallistumaan erilaisiin tietoturvallisuutta ylläpitäviin toimenpiteisiin osana kyberturvallisuuden ylläpitämistä. (Kessler ym. 2020, 467 & 470.) Nunes ja muut eivät puolestaan ei ole tunnistaneet iällä ja kyberturvallisella käyttäytymisellä olevan merkittävää tilastollista yhteyttä. Tulosten yksittäisessä tarkastelussa kuitenkin havaittu eroja ikäluokkien välisessä käyttäytymisessä. Erityisesti salasanakäyttäytymisessä, verkkoyhteyksien valinnassa sekä tietojen lataamisessa ja USB-tikkujen käytössä tiedonsiirron välineenä. (Nunes ym. 2021, 177–179.)

Yksilön luonteenpiirteiden vaikutus kyberturvalliseen käyttäytymiseen on tunnistettu. Tutkimusten mukaan työntekijät, joilla on luonteenpiirteinä avoimuutta, mukautuvuutta ja yhteistyökykyisyyttä, noudattavat päivittäisessä työssään todennäköisemmin kyberturvallista käyttäytymistä. Neuroottisuuden pirteiden ja emotionaalisen epävakauden on puolestaan todettu ennakoivan korkeampaa riskikäyttäytymistä. Poikkeuksena aikaisempaan tutkittuun tietoon, Yeng ja muut ovat todenneet tunnollisuuden luonteenpiirteen ennakoivan turvattomampaa käyttäytymistä. Syyksi tälle on pohdittu liiallista itsevarmuutta ja tämän aiheuttamaa huolimattomuutta työssä. (Yeng

ym. 2022, 17–18.) Jalalin ja muiden (2020, 8) mukaan yksilön subjektiiviset normit ja positiivinen asenne ennakoivat aikomusta käyttäytyä kyberturvallisesti.

Kyberturvalliseen käyttäytymiseen on tunnistettu vaikuttavan myös yksilön kulttuuritausta. Tutkimukset ovat osoittaneet eroavaisuutta afrikkalaisen ja länsimaisen kulttuurin yksityisyyden käsityksessä ja sen vaikutuksessa käyttäytymiseen. Afrikkalaisesta kulttuurista lähtöisin olevat työntekijät ovat usein tottuneet avoimempaan kulttuuriin, jossa tietosuoja-asiat ja yksityisyys eivät ole korostuneet. Australiassa on puolestaan todettu eroavaisuuksia syrjäalueiden ja kaupunkien terveydenhuollon välisessä viestinnässä ja toisen ymmärryksessä. (Dart & Ahmed 2023, 15.) Tutkimuksissa on lisäksi havaittu eroja käyttäytymismalleissa Saudi-Arabian ja länsimaisten kulttuurien välillä erityisesti potilasasioiden viestinnässä ja potilasturvallisuuden toteutumisessa. Saudikulttuurissa hoitosuhde nähdään usein henkilökohtaisempana eikä se rajoitu pelkästään työpaikalle. Lääkärit saattavat käsitellä potilasasioita vapaa-ajallaan henkilökohtaisilla työlaitteillaan, mikä voi heikentää tietosuojaa ja kyberturvallisuutta. (Albabtain ym. 2024, 98.)

7.4.8 Ammatin, työtehtävien ja työvälineiden vaikutus käyttäytymiseen

Kyberturvallisuuskäyttäytymiseen on tunnistettu olevan vaikutusta ammattiryhmällä ja työkokemuksella. Kessler ja muut ovat todenneet eroavaisuuksia ammattiryhmien välisessä käyttäytymisessä. Erityisesti lääkäreiden on tunnistettu olevan toimissaan muita ammattiryhmiä riskialttiimpia. Tunnollisimmin kyberturvallisuus käytäntöjä on puolestaan todettu noudattavan farmaseutit. (Kessler ym. 2020, 469–470.) Nunes ja muut eivät puolestaan ole todenneet tilastollisesti merkittävää eroa ammattiryhmien ja käyttäytymisen välillä. Yksittäisiä tuloksia tarkastellessa on kuitenkin havaittu eroa ammattiryhmien välisessä käyttäytymisessä mm. verkkoyhteyksien ja sähköpostin käytön välillä. (Nunes ym. 2021, 178.) Alhuwail ja muiden (2021, 929) mukaan pidemmät työuran tehneiden ammattilaisten kyberturvallinen käyttäytyminen olisi parempaa perustuen kokemukseen.

Ammattiryhmän lisäksi työtehtävien vaikutus kybertuvallisuuskäyttäytymiseen on tunnistettu. Erityisesti ensiavussa on todettu olevan suurempi riski kyberturvallisuusuhkille ja -rikkomuksille, koska työntekijät saattavat joutua priorisoimaan potilaan kriittisenhoidon kyberturvallisen toiminnan edelle (Yeng ym. 2022, 17). Työtehtävien kiireellisyys ja hätätilanteet korreloivat lisääntyneen riskikäyttäytymisen kanssa, ja voivat johtaa täten turvatoimien kiertämiseen (Hore ym. 2024, 5;

Schmidt ym. 2021, 639; Yeng ym. 2022, 16–17). Poikkeuksena muihin tuloksiin Yeng ja muut (2022, 16–17) eivät ole tunnistaneet varsinaisen työkuorman ja riskikäyttäytymisen yhteyttä. Hore ja muut ovat tunnistaneet väsymyksen ja stressin vaikutukset työntekijän kapasiteettiin toimia kyberturvallisesti (Hore ym. 2024, 5). Työntekijän kokema väsymys ja stressi saattavatkin olla usein työperäisiä, ja johtua työtehtävien laadusta.

Työtehtävien lisäksi työntekijöiden kyberturvallisuuskäyttäytymiseen vaikuttavat käytössä olevat työvälineet. Tutkimukset ovat osoittaneet puutteellisten työvälineiden ja olemassa olevien välineiden toiminnallisuuden vaikutukset kyberturvallisuuteen. Riittämätön kalusto, puutteelliset verkkoyhteydet sekä järjestelmien hitaus ja monimutkaisuus voivat johtaa turvallisuuskäytäntöjen kiertämiseen, mikä puolestaan luo haavoittuvuuksia organisaation kyberturvallisuuteen. (Hore ym. 2024, 5; Morris ym. 2023 6; Schmidt ym. 2021, 639.) Dart ja Ahmed ovat lisäksi tunnistaneet henkilöstön keskuudessa luottamuspulaa käytössä olevia työvälineitä kohtaan. Henkilöstöstä vain alle puolet on raportoinut luottavansa organisaation tarjoamien laitteiden ja järjestelmien turvallisuuteen (Dart & Ahmed 2023, 11).

7.4.9 Kyberturvallisuuskulttuurin ja johtamisen vaikutus käyttäytymiseen

Sosiaali- ja terveydenhuollon organisaatioiden kyberturvallisuuskulttuurin ja -ilmapiirin on tunnistettu olevan yhteydessä työntekijöiden kyberturvallisuuskäyttäytymiseen (Yeng ym. 2022, 18). Myönteisen ilmapiirin on todettu ennakoivan kyberturvallisempaa ja riskittömämpää käyttäytymistä päivittäisessä toiminnassa, kun taas huonon ilmapiirin on tunnistettu olevan haitallista kyberturvallisuuden ylläpitämiselle. (Kessler ym. 2020, 467). Välinpitämätön tai huoleton kyberturvallisuuskulttuuri voi pahimmillaan levitä yhteisössä ja aiheuttaa kyberuhkia toiminnalle. Horen ja muiden mukaan organisaation johdolla ja esihenkilöstöllä on merkittävä rooli kyberturvallisuuskulttuurin ja -ilmapiirin ylläpitämisessä. Johtamismenetelmien on todettu olevan suorassa yhteydessä työntekijöiden kyberturvalliseen käyttäytymiseen. Johdon esimerkillinen toiminta ja kyberturvallisuuden priorisointi kannustaa ja ohjaa työntekijöitä vastaavaan käyttäytymiseen. (Hore, ym. 2024, 5.) Jalalin ja muut (2022, 8) ovat lisäksi todenneet henkilöstölle toteutettujen käyttäytymisen kontrollien olevan positiivisesti yhteydessä työntekijän aikomukseen käyttäytyä kyberturvallisesti.

7.4.10 Kyberturvallisuuskoulutuksien ja -ohjelmien vaikutus käyttäytymiseen

Tutkimukset ovat osoittaneet sosiaali- ja terveydenhuollon organisaatioissa käytössä olevien kyberturvallisuusohjelmien (seta-program) ja -koulutuksien, turvallisuuskontrollien (security control framework) sekä auditoinnin positiiviset vaikutukset ammattilaisten kyberturvalliseen käyttäytymiseen. (Dart & Ahmed 2023, 1; Kang ym. 2023, 4; Kuo 2021, 8). Huolimatta koulutuksien positiivisista vaikutuksista työntekijöiden käyttäytymiseen, nämä eivät ole säännöllinen osa sosiaali- ja terveydenhuollon arkea. Tutkimukset ovat osoittaneet, ettei asianmukaista koulutusta kyberturvallisuuden ylläpitämiseksi ole aina tarjolla. Koulutuksien saatavuuden lisäksi myös sen laadulla on todettu olevan merkitystä. (Albabtain ym. 2024, 98; Gebeyew ym. 2024 5). Kang ja muut ovat tunnistaneet yhteyden yksilön kyberturvallisuuskoulutus kokemuksen ja käyttäytymisen välillä. Hyvän koulutuskokemuksen saaneet toimivat arjessa kyberturvallisemmin ja noudattavat annettuja ohjeistuksia. (Kang ym. 2023, 4.)

Kuo ja muut ovat tutkineet sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuuskäyttäytymisen yhteyttä kyberrikkomuksien ja näiden seuraamuksien tietoisuuteen. Tutkimuksessa on todettu, että yksilö, joka on tietoinen mahdollisesta rikkomuksen aiheuttamasta rangaistuksesta, sen laadusta ja varmuudesta, noudattaa kyberturvallisia käytäntöjä paremmin. (Kuo ym. 2021, 7 & 9.)

Taulukko 6. Kyberturvallisuuskäyttäytyminen ja siihen vaikuttavat tekijät

Käyttäytymisen taso	Käyttäytymiseen vaikuttavat tekijät
käyttäytyminen näyttäytyy vaihtelevana tutkimusten välillä (hyvä-keskimääräinen-välttävä-heikko)	Sukupuoli - Naiset käyttäytyvät turvallisemmin - Ei tunnistettu tilastollista yhteyttä
Välinpitämättömyys, huolimattomuus, vastuullisuuden puute	Ikä - Iäkkäämmät toimissaan turvallisempia - Ei tunnistettu tilastollisesti merkittävää yhteyttä. Yksittäisiä tekijöitä tarkasteltaessa havaittu eroja ikäryhmien välillä.
Ohjeiden noudattaminen - 65 % noudattaa annettuja kyberturvallisuusohjeita - 49,5 % ei poikkeaisi annetuista turvaohjeista	Luonteenpiirteet - Avoimuuden, mukautuvuuden ja yhteistyökykyisyyden piirteitä omaavat toimivat turvallisemmin - Subjektiiviset normit ja positiivinen asenne ennakoivat aikomusta käyttäytyä kyberturvallisesti. - Tunnollisuus voi ennakoida turvattomampaa käyttäytymistä

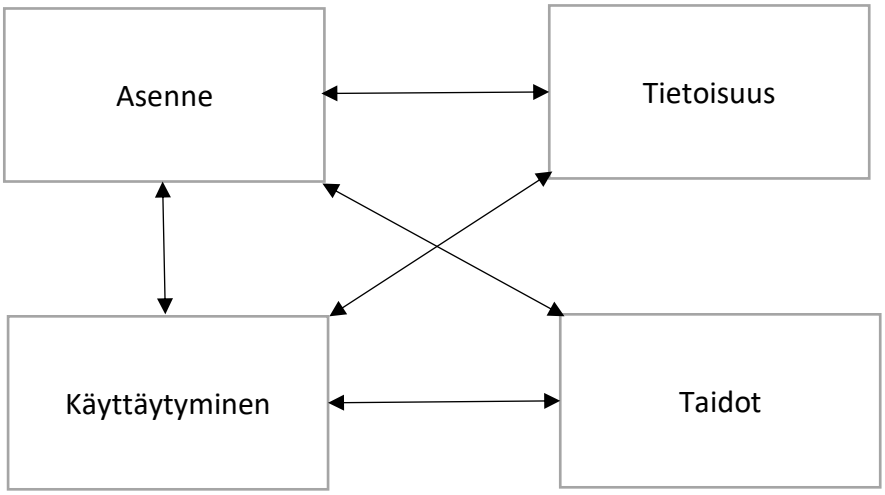
	- Neuroottisuuden piirteet ja emotionaalinen epävakaus ennakoi korkeampaa riskikäyttäytymistä
Verkkoyhteyden käyttö - Pääsääntöisesti käytetään sairaalan turvattua verkkoyhteyttä - Vikatilanteessa saatetaan turvautua suojaamattomiin yhteyksiin - 26 % yhdistänyt henkilökohtaisen älylaitteen sairaalan verkkoon	Kulttuuritausta - Erot afrikkalaisen ja länsimaisen kulttuurin yksityisyyden käsityksessä. - Australiassa erot syrjäalueiden ja kaupunkien terveydenhuollon välisessä viestinnässä - Saudi-Arabian ja länsimaisen kulttuurin ero potilasasioiden viestinnässä ja potilasturvallisuuden toteutumisessa
Salasanakäyttäytyminen - 74 % ei jaa salasanaa - 31 % käyttää riittävän uniikkia salasanaa - 15 % kirjoittanut salasanan ylös - koetaan saman salasanan käyttö eri järjestelmissä turvalliseksi	Ammatti - Tunnistettu ero ammattiryhmien välisessä käyttäytymisessä. Lääkärit toimissaan muita ammattiryhmiä riskialttiimpia. Tunnollisimpia farmaseutit - Ei ole tunnistettu tilastollisesti merkittävää yhteyttä. Yksittäisiä tuloksia tarkastellessa havaittu eroa ammattiryhmien välisessä käyttäytymisessä
Kirjautumiskäyttäytyminen - 61,5 % kokee tietokoneelle kirjautumisen helpoksi - 35 % käyttää lukittua näyttöä - Lukitsemattomia tietokoneita 18kpl/ 58kpl ja 15kpl/ 110kpl. Avoimissa koneissa useampi käyttäjä samanaikaisesti (20 %, 22 %)	Pidemmän uran tehneet toimivat turvallisemmin
Tietojenkäsittely - 74 % varmistaa, ettei ulkopuolisella ei pääsyä/ näköyhteyttä potilastietoihin - 10 % jakanut arkaluonteista tietoa ulkopuoliselle - 29 %) katsonut potilastietoja ilman hoitosuhdetta potilaaseen. - 9 % ladannut potilastietoja käyttöönsä kotona	Työtehtävät - Ensiavussa on todettu olevan suurempi riski kyberturvattomalla käyttäytymiselle - Työtehtävien kiireellisyys ja hätätilanteet korreloivat lisääntyneen riskikäyttäytymisen kanssa - Ei tunnistettu työkuorman ja riskikäyttäytymisen yhteyttä. - Väsymys ja stressi vaikuttavat turvalliseen käyttäytymiseen
Ulkoisten muistitikkujen (USB) käyttö hyvää	Työvälineiden vaikutus käyttäytymiseen tunnistettu
Tietojen lataaminen turvallista	Positiivinen kyberturvallisuuskulttuuri ja ilmapiiri ennakoivat riskittömämpää käyttäytymistä
Sähköinen viestintä - Keskimääräistä - 10 % hyödyntänyt henkilökohtaista spostia viestinnässä - Yhteissähköposteja käytössä	Johtaminen - Johtaminen vaikuttaa kyberturvallisuuskulttuuriin ja -ilmapiiriin - Johtamismenetelmät suorassa yhteydessä kyberturvalliseen käyttäytymiseen - Johdon esimerkillinen toiminta tukee henkilöstön turvallista käyttäytymistä
Henkilökohtaisten älylaitteiden työkäyttö turvatonta	Koulutukset

	- Kyberturvallisuusohjelmien ja -koulutuksien, turvallisuus kontrollien sekä auditoinnin positiiviset vaikutukset käyttäytymiseen tunnistettu - Saadun koulutuksen laatu ja koetut hyödyt vaikuttavat käyttäytymiseen - Koulutuksen puute aiheuttaa turvattomampaa käyttäytymistä
Kyberhyökkäystilanteessa käyttäytyminen - Kalasteluviestien tunnistaminen hyvää - 15 % avannut vaaralliseksi osoittautuneen viestin tai linkin - Lähetetyistä standardoiduista viesteistä 36 % avattiin ja kustomoiduista viesteistä 62 %. Standardoidun viestin avanneista vajaa 18 % klikkasi viestin linkkiä ja kustomoidun viestin avanneista 88 % klikkasi linkkiä - Kustomoiduista viesteistä avattiin 58 %, ja avanneista 87 % klikkasi linkkiä - Standardoiduista viesteistä 44 % avattiin, ja viestin avanneista 7 %) klikkasi linkkiä - A simulaatiossa n. 70 % lankesi kalasteluviestiin. B simulaatiossa 48 % lankesi kalasteluviestiin - Valvontalaitteeseen kohdistetussa kyberhyökkäys simulaatiossa 12/20 hoitajaa suoriutui hyvin. Kuitenkin vain 1 suoriutui ilman vihjeitä koko simulaatiosta	Käyttäytymisen kontrollien positiivinen yhteys turvalliseen käyttäytymiseen tunnistettu
Kyberrikkeen raportointi - 22 % epävarma miten toimia - 12 % jättänyt raportoimatta rikkeen - 22 % ei koe olevan omalla vastuulla - 74 % ei ole ikinä raportoinut rikettä - Raportoidaan kollegoiden tahattomat tai tahalliset virheet	Kyberrikkomuksien ja näiden seuraamuksien tietoisuuden vaikutus käyttäytymiseen tunnistettu

7.5 Asenteen, tietoisuuden, taitojen ja käyttäytymisen yhteys

Tutkimuksissa on korostunut terveydenhuollon henkilöstön kyberturvallisuusasenteen, -tietoisuuden, -taitojen ja kyberturvallisen käyttäytymisen väliset yhteydet. Tutkimuksessa on tunnistettu työntekijöiden kyberturvallisuusasenteen, -tietoisuuden ja -taitojen korreloivan kyberturvallisuuskäyttäytymisen kanssa. Työntekijöiden positiivinen asenne kyberturvallisuutta kohtaan edistää heidän kyberturvallista käyttäytymistään päivittäisessä toiminnassa. (Kang ym. 2023, 4; Magdalinou ym. 2022, 26; Nunes ym. 2021, 180; Yeng ym. 2022, 18.) Tutkimuksen mukaan henkilöstö, joka omaa hyvän kyberturvallisuustietoisuuden ja -taidot, käyttäytyy keskimääräisesti kyberturvallisemmin kuin henkilöstö, jolla on heikompi tietoisuus ja taidot kyberturvallisuudesta (Albabtain

ym. 2024, 98; Magdalinou ym. 2022, 26; Yeng ym. 2022, 18). Hore ym (2024, 5) mukaan yksi selitys työntekijöiden mahdolliselle riskikäyttäytymiselle onkin tietoisuuden puute. Tutkimuksissa työntekijöiden kyberturvallisuusasenteisiin on todettu vaikuttavan keskeisesti yksilön kyberturvallisuustietoisuuden ja -taitojen taso. Työntekijöiden tietotekninen osaaminen ja tietoturvakäytänteiden hallitseminen ennakoivat työntekijän positiivista asennetta. (Gebeyew ym. 2024, 6; Kang ym. 2023, 4.) Kyberturvallisuusosaamisen tekijöiden yhteydet kuvattu kuviossa 5.



Kuvio 5. Kyberturvallisuusosaamisen tekijöiden yhteys

7.6 Kyberturvallisuusosaamisen kehittämistarpeet

Tämän opinnäytetyönä toteutetun tutkimuksen perusteella sosiaali- ja terveydenhuollon kyberturvallisuusosaamisessa ilmeni selkeitä kehittämistarpeita, joita tarkastellaan erillisenä tässä kappaleessa. Tulokset kuvattu lisäksi taulukossa 3.

Työntekijöiden kyberturvallisuusasenteessa on tunnistettu vaihtelua ja kehittämistarvetta. Asenne teknologisia laitteita, digitaalisia palveluita ja näiden kyberturvallisuutta kohtaan on keskimääräistä. Tutkimukset ovat osoittaneet työntekijöiden keskuudessa innostusta ja positiivista asennetta teknologiaa ja sen käyttöä kohtaan, mutta myös osittain pelkoa ja epävarmuutta uusia palveluita kohtaan. (Gebeyew ym. 2024, 7; Magdalinou ym. 2022, 26; Morris ym. 2023, 6.)
Tutkimuksessa on todettu puutteita yksilöiden vastuullisuudessa kyberturvallisuutta kohtaan, mikä

herättää huolta sosiaali- ja terveydenhuollon palveluiden kokonaisturvallisuudesta. (Kessler ym. 2020, 462, 470; Yeo & Banfield 2022).

Kyberturvallisuustietoisuus on tutkimuksien mukaan henkilöstön keskuudessa pääsääntöisesti hyvää. Tulokset ovat kuitenkin tunnistaneet työntekijöiden joukosta myös muutamia heikon tietoisuuden omaavia yksilöitä (Albabtain ym. 2024, 97 & 99; Hore ym. 2024, 2 & 5; Magdalinou ym. 2022, 26), joiden osaamiseen olisi tärkeää panostaa. Yksikin heikon kyberturvallisuustietoisuuden omaava henkilö voi toiminnallaan altistaa organisaation erilaisille uhkille. Yksittäisiä tietoisuustekijöitä tarkasteltaessa havaittiin kehittämistarpeita erityisesti henkilöstön kyber- ja tietoturvauhkien tietoisuudessa (Dart & Ahmed 2023, 10 & 13). Tutkimuksen mukaan kyberturvallisuusohjeistuksien ja -käytäntöjen tietoisuus näyttäytyi vaihtelevana riippuen tutkimuksesta (Dart & Ahmed 2023, 14; Magdalinou ym. 2022, 26), jonka vuoksi aihealue tulee laskea mukaan kehittämistarpeisiin.

Tutkimuksen perusteella sosiaali- ja terveydenhuollon työntekijöiden kyberturvallisuustaidot ovat keskimääräistä tai hyvää (Hore ym. 2024, 5; Morris ym. 2023, 3 & 5). Hyvistä taidoista huolimatta työntekijät ovat raportoineet epävarmuutta omia taitoja kohtaan (Hore ym. 2024, 5). Epävarmuus omia kykyjä kohtaan voi vaikuttaa työntekijän kyberturvalliseen käyttäytymiseen. Yksittäisiä kyberturvallisuustaitoja tarkasteltaessa on tunnistettu kehittämistarpeita kyberturvallisten työkalujen käytön, internetin käytön, sähköisen viestinnän sekä kyber- ja tietoturvauhkien tunnistamisen suhteen (Gebeyew ym. 2024, 5; Magdalinou ym. 2022, 25–26; Morris ym. 2023, 5–6; Hore ym. 2024, 4–5). Kyberrikkeiden ja -uhkien raportoinnin suhteen tutkimuksen tulokset olivat eriäviä (Hore ym. 2024, 2; Magdalinou ym. 2022, 25), joten näitä tulisi tarkastella myös kehittämistarpeita tarkasteltaessa.

Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuuskäyttäytyminen näyttäytyy tutkimuksien mukaan vaihtelevana. Tuloksissa on tunnistettu erilaista kyberturvallisuuskäyttäytymistä, joka vaihtelee hyvän ja heikon tason välillä. (Alhuwail ym. 2021, supplementary material; Hore ym. 2024, 5; Magdalinou ym. 2022, 26; Nunes ym. 2021, 178–179.) Yksittäisiä tekijöitä tarkasteltaessa kyberturvallisuuskäyttäytymisessä on tunnistettu kehittämistarpeita kyberturvallisuuskäytäntöjen ja -ohjeiden noudattamisessa, riittävän uniikin salasanan asettamisessa, henkilökohtaisen älypuhe-

limen työkäytössä, tietokoneelta uloskirjautumisessa, kyberhyökkäyksen tunnistamisessa ja kyberuhka tilanteessa toimimisessa sekä kyberrikkeiden raportoinnissa eteenpäin. Lisäksi työntekijöiden keskuudessa on tunnistettu välinpitämätöntä ja huolimatonta käyttäytymistä, mihin tulisi kehittämistyössä erityisesti puuttua (Albabtain ym. 2024, 98; Alhuwail ym. 2021, supplementary material; Dart & Ahmedin 2023, 10 & 15; Hore ym. 2024, 2 & 5; Jalali ym. 2022, 5–6; Kessler ym. 2020, 462, 470; Magdalinou ym. 2022, 25–26; Mohammed ym. 2021, 5–7; Rizzoni ym. 2022, 5–6; Yeo & Banfield 2022; Willing ym. 2021)

Sosiaali- ja terveydenhuollon työntekijöiden kyberturvallisuusosaamisen kehittämistarpeita tarkasteltaessa ja korjaavia toimenpiteitä suunniteltaessa on keskeistä arvioida työntekijöiden osaamista kokonaisvaltaisesti. Tutkimus on osoittanut yhteyden asenteen, tietoisuuden, taitojen ja käyttäytymisen välillä. Näiden kyberturvallisuusosaamisen tekijöiden on tunnistettu korreloivan toistensa kanssa, jonka vuoksi kehittämistarpeiden tarkastelu on tärkeää toteuttaa yhtenä kokonaisuutena. (Albabtain ym. 2024, 98; Gebeyew ym. 2024, 6; Kang ym. 2023, 4; Magdalinou ym. 2022, 26; Nunes ym. 2021, 180; Yeng ym. 2022, 18.)

Taulukko 7. Kyberturvallisuusosaamisen kehittämistarpeet

Kyberturvallisuusosaamisen kehittämistarpeet			
Asenne	**Tietoisuus**	**Taidot**	**Käyttäytyminen**
Kyberturvallisuuteen asennoituminen	Yksittäisten työntekijöiden tietoisuuden tason huomiointi. Tietoisuuden vaihteluväli merkittävää	Itsevarmuuden tukeminen. Hyvistä taidoista huolimatta työntekijöillä epävarmuuden tunnetta omia taitoja kohtaan	Kyberturvallisuuskäytäntöjen ja -ohjeiden noudattaminen
Työntekijät ilmaisseet epävarmuutta ja pelkoa teknologisten laitteiden käyttöä kohtaan	Kyber- ja tietoturvauhkien tietoisuus	Kyberturvallisten työkalujen käyttö	Riittävän uniikin salasanan käyttäminen
Vastuullisuuden puute	Kyberturvallisuusohjeistuksien ja -käytäntöjen tietoisuus	Internetin käyttö	Henkilökohtaisen älypuhelimen työkäyttö
		Sähköinen viestintä	Tietokoneelta uloskirjautuminen
		Kyber- ja tietoturvauhkien tunnistaminen	Kyberhyökkäyksen tunnistaminen ja kyberuhka tilanteessa toimiminen
		Kyberrikkeiden ja -uhkien raportointi	Kyberrikkeiden raportointi
			Välinpitämätön ja huolimaton käyttäytyminen

8 Pohdinta

8.1 Tulosten käsittely

Tämän kirjallisuuskatsauksen tavoitteena oli tutkia aikaisempia jo olemassa olevia tutkimuksia sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen nykytilasta ja sen kehittämistarpeista sekä lisätä teoreettista tietämystä aiheesta. Tutkimuskirjallisuus osoittaa, että terveydenhuollon palveluiden digitalisoitumisen ja digitaalisen kehityksen myötä on syntynyt uusia kyberturvallisuushaasteita. Samalla henkilöstön rooli organisaation kyberturvallisuuden ylläpitämisessä on korostunut entisestään.

Teoreettisessa kirjallisuudessa sekä kirjallisuuskatsaukseen sisältyvissä tutkimuksissa korostui yksittäisten sosiaali- ja terveydenhuollon ammattilaisten kyberturvallisuusosaamisen merkitys ja sen suora vaikutus koko organisaation kyberturvallisuuden tasoon. Yksittäisen työntekijän toiminta voi joko edistää organisaation kyberturvallisuutta tai heikentää sitä, aiheuttaen potentiaalisen uhkan tai huomattavan haitan koko organisaation toiminnalle. Organisaatioiden kyberturvallisuuden varmistamiseksi sekä terveydenhuollon ammattilaisten kyberturvallisuusosaamisen edistämiseksi on olennaista tarkastella työntekijöiden osaamisen nykytilaa ja kehittämistarpeita kokonaisvaltaisesti ja systemaattisesti.

Tämän kirjallisuuskatsauksen tulokset viittaavat sosiaali- ja terveydenhuollon ammattilaisten kyberturvallisuusosaamisen olevan vaihtelevaa. Kyberturvallisuusosaamisen tekijöitä, asennetta, tietoisuutta, taitoja ja käyttäytymistä, tarkasteltaessa tunnistettiin vaihtelevasti niin hyvän, keskimääräisen, välttävän kuin heikon osaamisen osa-alueita. Tuloksista nousi esiin merkittäviä kyberturvallisuusosaamisen kehittämistarpeita. Kehittämistarpeissa korostui erityisesti kyberuhkatilanteiden hallinta, uhkien ja rikkeiden eteenpäin raportointi sekä henkilöstön asenteisiin liittyvät haasteet kuten välinpitämättömyys, huolimattomuus ja epävarmuus omaa toimintaa kohtaan. Kyberturvallisuusosaamisen vaihtelevat kehittämistarpeet viittaavat siihen, että osaamista kehitettäessä on tärkeää huomioida käsitteen kokonaisvaltaisuus sekä hyödyntää koulutuksessa ihmislähtöistä ja oppimista tukevaa lähestymistapaa.

Kirjallisuuskatsauksen tulosten perusteella kyberturvallisuusasenteet, -tietoisuus, -taidot ja -käyttäytyminen muodostavat toisiinsa kytkeytyvän kokonaisuuden, jossa eri kyberturvallisuusosaamisen tekijät ovat keskinäisessä vuorovaikutuksessa. Tekijöiden tunnistettu yhteys vaikuttaa merkittävästi yksilön toimintaan kyberturvallisuustilanteissa. Yhteyden vuoksi henkilöstön kyberturvallisuusosaamisen kehittämisessä on keskeistä huomioida kaikki osaamisen tekijät tasavertaisesti, jotta työntekijöiden osaaminen vahvistuu kokonaisvaltaisesti ja siirtyy tehokkaasti käytännön toimintaan. Osaamisen siirtymistä päivittäiseen toimintaan voidaan tukea tarjoamalla säännöllistä ja työtehtäviin sidottua koulutusta sekä hyödyntämällä käytännön harjoittelua ja erilaisia järjestettyjä simulaatioita.

Kyberturvallisuusosaamisen yksittäisiä osa-alueita syvällisemmin tarkasteltaessa havaittiin merkittävää vaihteluväliä työntekijöiden osaamisen tasossa. Osaamisen suuret vaihteluvälit kertovat yksittäisten työntekijöiden hyvin eritasoisesta kyberturvallisuusosaamisesta ja lähtökodista ylläpitää kyberturvallisuutta. Osaamisen vaihteluvälien taustalla voivat olla muun muassa työntekijöiden asenteet ja vaihtelevat käsitykset kyberturvallisuudesta, organisaation koulutusresurssien vähäisyys tai niiden puute, puutteelliset kyberturvallisuusohjeistukset ja -käytännöt sekä johdon vähäinen panostus tai priorisointi kyberturvallisuuteen. Henkilöstön osaamisen moninaisuus asettaa haastetta organisaatioiden kyberturvallisuuden kehittämiselle, sillä yhtenäiset koulutukset ja perehdytysmallit eivät välttämättä vastaa kaikkien ammattilaisten tarpeisiin.

Kirjallisuuskatsauksesta saatujen tuloksien mukaan sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuuskouluttaminen ja harjoitukset eivät ole järjestelmällinen osa terveysalan organisaatioiden toimintaa. Tuloksien perusteella asianmukaista koulusta ei ole aina edes tarjolla. Kyberturvallisuuskouluttamisen positiiviset vaikutukset työntekijöiden asenteisiin, tietoisuuteen ja käyttäytymiseen on kuitenkin tunnistettu, jonka vuoksi organisaatioiden olisi keskeistä panostaa tähän. Koulutuksien saatavuuden lisäksi myös niiden laadun on tunnistettu olevan yhteydessä kyberturvallisuuskäyttäytymiseen.

Sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuuskoulutuksien suunnitellussa on hyvä tarkastella kirjallisuuskatsauksessa nousseita kehittämistarpeita. Tunnistettuja kehittämistarpeita voidaan hyödyntää kyberturvallisuuskoulutuksien suuntauksien ja päälinjauksien suunnittelussa. Kehittämistarpeiden lisäksi koulutuksien suunnittelussa on keskeistä huomioida tutkimuksessa

tunnistettu työntekijöiden kyberturvallisuusosaamisen merkittävä vaihteluväli. Työntekijöiden osaamisen variaatio viittaa siihen, että yhtenäisen koulutuksen tarjoaminen koko henkilöstölle ei välttämättä ole tehokkain eikä tarkoituksenmukaisin tapa edistää kyberturvallisuusosaamista. Työntekijöiden lähtökohtien, yksilöllisen osaamisen tason ja nykyisen työnkuvan huomioiminen mahdollistaa koulutuksen kohdentamisen todellisiin tarpeisiin ja tukee kyberturvallisen käyttäytymisen juurtumista osaksi päivittäistä työtä.

Työntekijöiden kyberturvallisuusosaamisen kehittämisessä on tärkeää huomioida organisaation johtaminen ja sen muodot. Johdon tulee olla sitoutunut organisaation kyberturvallisuustavoitteisiin ja toimintaan. Johdon esimerkillinen kyberturvallisuustoiminta sekä kyberturvallisuuden priorisointi organisaation päivittäisessä toiminnassa toimivat tärkeinä esimerkkeinä työntekijöille ja voivat merkittävästi motivoida heitä omaksumaan kyberturvallista käyttäytymistä. Johdon tuen lisäksi organisaatiolle asetetut ajantasaiset ja käytännön työtä tukevat kyberturvallisuusprotokollat toimivat keskeisinä työkaluina ja ohjeina henkilöstölle. Kyberturvallisuusprotokollien päivittämisen tulisi olla osa jokaisen organisaation keskeistä toimintaa.

Sosiaali- ja terveydenhuollon henkilöstön säännölliset ja tarvelähtöiset kyberturvallisuuskoulutukset, esimerkillinen johtajuus sekä organisaation ajantasaiset kyberturvallisuusprotokollat muodostavat yhdessä perustan myönteiselle kyberturvallisuuskulttuurille ja -ilmapiirille. Tutkimukset osoittivat työnpaikan positiivisen kyberturvallisuusilmapiirin ja -kulttuurin tukevan työntekijöiden kyberturvallisuusosaamista ja -käyttäytymistä sekä vahvistavan motivaatiota kyberturvallisen toiminnan kehittämiseen. Henkilöstön avoin ja rehellinen keskustelu kyberturvallisuuteen liittyvistä kysymyksistä ja haasteista edistää työympäristön turvallisuutta sekä toimii myönteisen ja luottamuksellisen kyberturvallisuusilmapiirin ja -kulttuurin perustana ja ylläpitäjänä. Tällainen vuorovaikutus vahvistaa työntekijöiden luottamusta organisaation sisällä sekä edistää jatkuvaa oppimista ja kehitystä.

Henkilöstön kyberturvallisuusosaamisen edistämiseksi organisaatioiden on tärkeää huomioida työntekijöille tarjottujen työvälineiden asianmukaisuus ja kapasiteetti. Erityisesti sosiaali- ja terveydenhuollon palveluissa, jossa kiire ja vähäiset resurssit ovat osa arkea, tulisi teknologiset laitteet, digitaaliset palvelut ja niiden kyberturvallisuus suunnitella siten, että ne tukevat ja mahdollistavat henkilöstön tehokasta työskentelyä eivätkä lisää työkuormaa. Käyttäjäystävälliset

kyberturvallisuusratkaisut parantavat henkilöstön motivaatiota noudattaa turvallisuusohjeita ja -käytäntöjä sekä vähentävät uusien järjestelmien ja laitteiden käyttöönoton vastustusta.

Kyberturvallisuuden ylläpitämisessä on ulkoisten tekijöiden lisäksi tärkeää huomioida yksittäisen työntekijän vastuu ja velvollisuus huolehtia organisaation kyberturvallisuudesta. Henkilöstön tulee sitoutua oman osaamisensa jatkuvaan päivittämiseen ja sen laadun ylläpitämiseen. Työntekijöiden tulee kyetä toimimaan päivittäisessä toiminnassa, ulkoisista häiriötekijöistä ja työkuormasta huolimatta, tunnollisesti ja tarkasti, jotta potilasturvallisuus ja terveydenhuollon palveluiden jatkuvuus voidaan taata.

Tämän kirjallisuuskatsauksen tulokset sosiaali- ja terveydenhuollon kyberturvallisuusosaamisen nykytilasta ja sen kehitystarpeista koostuivat työntekijöiden itsearvioinneista ja haastatteluista, tilastotutkimuksesta sekä henkilöstölle toteutetuista stimulaatiotesteistä. Katsaukseen valikoituneet tutkimukset painottuivat itsearviointiin, mikä saattaa vaikuttaa tuloksien luotettavuuteen. Katsaukseen valikoituneista eri menetelmin toteutetuista tutkimuksista nousi osittain ristiriitaisia tuloksia työntekijöiden kyberturvallisuusosaamisen nykytilasta. Eriävät tulokset saavat pohtimaan työntekijöiden kykyä tunnistaa ja arvioida realistisesti omaa kyberturvallisuusosaamistaan ja sen kehittämistarpeita.

Kyberturvallisuuden ja siihen liittyvien haasteiden ulottuessa yhä laajemmin sosiaali- ja terveydenhuollon palveluihin, on toimialan kyberturvallisuuden tutkimiseen ja kehittämiseen tärkeää panostaa. Kyberturvallisuuteen perustuvassa tutkimuksessa on tunnistettu ihmisen keskeinen rooli kyberturvallisuuden ylläpitäjänä ja turvaajana. Mitä paremmin ymmärretään henkilöstön kyberturvallisuusosaamisen nykytilaa, siihen vaikuttavia tekijöitä ja kehittämistarpeita, sitä tehokkaammin voidaan tukea työntekijöiden osaamisen vahvistamista ja edistää organisaation kyberturvallista toimintakulttuuria.

8.2 Tutkimuksen eettisyys ja luotettavuus

Tämän opinnäytetyön tutkimusmenetelmänä toimi integratiivinen kirjallisuuskatsaus, jonka tekemisessä noudatettiin hyvän tieteellisen käytännön (HTK) perusperiaatteita eli luotettavuutta, rehellisyyttä, arvostusta sekä vastuunkantoa. Luotettavuudella tarkoitetaan tieteellisen toiminnan

laadun varmistamista suunnittelussa. Rehellisyydellä tarkoitetaan tieteellisen toiminnan suunnittelua, toteutusta ja arviointia sekä avointa ja puolueetonta viestintää asiasta. Arvostuksella tarkoitetaan muiden ja ympäristöjen olemassaolon arvostusta. Vastuunkanto taas tarkoittaa tutkijan vastuun ottoa koko tieteellisen toiminnan elinkaaresta. (Hyvä tieteellinen käytäntö 2021, 11–12). Ennen tutkimuksen tekoa tutkija perehtyi hyvään tieteelliseen käytäntöön Jyväskylän ammattikorkeakoulun opetuksessa sekä omatoimisesti lukemalla Tutkimuseettisen neuvottelukunnan (TENK) laatimia ohjeita. Tutkija sitoutui noudattamaan hyvää tieteellistä käytäntöä ja siihen liittyviä menettelytapoja koko tutkimustoiminnan ajan.

Tutkimuksen teossa tulee kunnioittaa aikaisempaa tutkimustietoa antamalla arvo niiden saavutuksille (Hyvä tieteellinen käytäntö 2021, 14). Tämän opinnäytetyön teossa muiden tekemää työtä ja julkaistua tutkimustietoa kunnioitettiin viittaamalla julkaisuihin asianmukaisella tavalla. Luotettavan raportoinnin tueksi tutkija suoritti ylemmän korkeakouluopintojen aikana tekstitaidot haltuun opintokokonaisuuden, jossa käsiteltiin referointia ja lähdeviittauksia tieteellisessä kirjoittamisessa.

Opinnäytetyö tulee suunnitella, toteuttaa ja dokumentoida huolellisesti ja rehellisesti avoimen tieteen periaatteita noudattaen. Tutkimuksen tuloksien käsittely tulee toteuttaa tarkasti ja järjestelmällisesti, sekä tuloksien julkaisussa tulee noudattaa avoimuuden ja oikeudenmukaisuuden periaatetta. (Hyvä tieteellinen käytäntö 2021, 13). Tämän opinnäytetyön teossa hyödynnettiin tarkkojen muistiinpanojen laatimista koko prosessin ajan sen luotettavuuden varmistamiseksi. Muistiinpanojen avulla tutkija pystyi helposti palaamaan työn aikaisempiin vaiheisiin ja varmistamaan tutkimuksen uskottavuutta. Opinnäytetyön suunnittelua ja toteutusta tuki tehty opinnäytetyösuunnitelma sekä ohjauskeskustelut opinnäytetyönohjaajan ja työelämän kontaktin kanssa. Tuloksien analysoinnissa ja raportoinnissa tuloksia ei muunneltu vaan ne käsiteltiin ja julkaistiin alkuperäisessä muodossa saatuja tuloksia kunnioittaen.

Opinnäytetyössä toteutetun kirjallisuuskatsauksen luotettavuutta varmistettiin monimuotoisella hakuprosessilla, johon oli asetettu tutkimuskysymystä tukevat kelpoisuus-, mukaanotto- ja poissulkukriteerit sekä kirjallisuuskatsaukseen valikoituneen aineiston laadunarviointi. Aineiston laadun arvioinnissa hyödynnettiin Kangasniemen ja muiden (2015) luomaa kriteeristöä, joka havainnoi tutkimuksen tarkoitusta ja tavoitteita, tutkimusasetelmaa, teoreettista viitekehystä, tutkimuksen

rajoituksia sekä keskustelua ja johtopäätöksiä. Kangasniemen ja kollegoiden luoma malli pohjautuu Bowlingin (2002) ja Gazarian (2013) tietoon arvioinnista. (Kangasniemi ym. 2015, 3, 5–7.)

Tässä opinnäytetyöprojektissa noudatettiin avoimuuden periaatetta, ja avattiin tutkimuksen tarve, lähtökohdat sekä työelämänkontakti rehellisesti. Opinnäytetyöllä ei ollut toimeksiantajan lisäksi muita sidonnaisuuksia ja rahoitusta, jonka vuoksi tarkempaa lupa-asioiden selvittelyä ei prosessissa tarvinnut toteuttaa.

Tämä opinnäytetyö oli yksilötehtävä, jonka tutkija suoritti itsenäisesti. Itsenäisen työskentely tutkimuksen parissa saattaa heikentää tutkimuksen luotettavuutta, koska tutkimuksen tuloksia ei ole analysoitu kahden tutkijan toimesta (Systemaattinen tiedonhaku opas nd.). Itsenäisen työskentelyn tueksi ja tutkimuksen luotettavuuden edistämiseksi tutkija hyödynsi kirjallisuuskatsauksen toteutuksessa kirjaston informaatikon sekä opinnäytetyön ohjaajan asiantuntemusta ja ohjausta sekä tarkkaa dokumentointia tutkimuksen toteutuksesta.

8.3 Johtopäätökset ja jatkotutkimusehdotukset

Tästä kirjallisuuskatsauksesta saadut tutkimustulokset viittaavat sosiaali- ja terveydenhuollon työntekijöiden vaihtelevaan kyberturvallisuusosaamiseen. Tutkimuksessa tunnistettiin ammattilaisten keskuudessa niin keskimääräisen ja hyvän kyberturvallisuusosaamisen osa-alueita kuin välttävän ja heikon osaamisen osa-alueita. Kirjallisuuskatsauksen tulokset kertovat työntekijöiden kyberturvallisuusosaamisessa olevan lisäksi merkittävää vaihteluväliä yksittäisten työntekijöiden välillä. Suuri osaamisen vaihteluväli kertoo työntekijöiden hyvin eritasoisista lähtökohdista toimia kyberturvallisesti arjessa. Tutkimuksessa tunnistettiin runsaasti kyberturvallisuusosaamisen kehittämistarpeita.

Tänä päivänä kyberrikollisuuden kohdistuessa entistä enemmän sosiaali- ja terveydenhuollon palveluihin voi yksikin heikon kyberturvallisuusosaamisen omaava työntekijä aiheuttaa toiminnallaan uhkaa potilaille sekä koko organisaation toiminnalle ja sen jatkuvuudelle. Hyvällä kyberturvallisuusosaamisella varmistamme kyberturvallista sosiaali- ja terveydenhuollon arkea. Kyberuhkatilanteiden ehkäisemiseksi organisaatioiden tulisi panostaa työntekijöidensä kyberturvallisuusosaamisen säännölliseen ylläpitämiseen ja kehittämiseen.

Tämän kirjallisuuskatsauksen tuottamia tuloksia sosiaali- ja terveydenhuollon henkilöstön kyberturvallisuusosaamisen nykytilasta ja kehittämistarpeista voidaan jatkossa hyödyntää kyberturvallisuusosaamisen kehittämistoiminnassa sekä muussa toimialan kyberturvallisuuteen liittyvässä tutkimuksessa. Kirjallisuuskatsauksen tulokset toimitetaan opinnäytetyön toimeksiantajalle, KyberSote- projektille, hyödynnettäväksi projektin tutkimus- ja kehittämistoiminnassa. Tuloksia voidaan hyödyntää projektin suunnitelman mukaisesti kyberturvallisuutta edistävien työkalujen ja toimintamallien kehittämisessä.

Kirjallisuuskatsaukseen sisältyneiden tutkimusten menetelmällinen painopiste oli itsearvioinnissa. Tutkimukset oli toteutettu pääasiassa kvantitatiivisilla kyselylomakkeilla tai monimenetelmällisinä tutkimuksina, joissa oli yhdistetty määrällinen kyselyaineisto ja haastattelu. Kirjallisuuskatsauksen aineistoa analysoitaessa havaittiin tuloksellisia eroavaisuuksia itsearviointiin ja simulaatioihin perustuvien tutkimusten välillä, mikä herättää kysymyksen työntekijöiden itsearvioinnin luotettavuudesta. Sosiaali- ja terveydenhuollon kyberturvallisuusosaamisen nykytilan ja kehittämistarpeiden kokonaisvaltaisemman ymmärtämisen saavuttamiseksi olisi suositeltavaa tutkia aihetta laajemmin havainnointiin perustuvien tutkimusmenetelmien avulla.

Lähteet

Albabtain, A.M., AlOtaibi, D., AlMazial, N., Aloudah, N., Alghosoon, H.M. & Arafat, A.A. 2024, Healthcare Professional's Knowledge, Awareness, and Attitude toward Patients' Data Privacy and Security in Clinical Research. Saudi Journal of Health Systems Research 4, 2, 92–102. Viitattu 9.5.2025. https://karger.com/sjh/article/4/2/92/906700/Healthcare-Professional-s-Knowledge-Awareness-and.

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y. & AlDuaij, S. 2021, Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. Applied Clinical Informatics 29, 12,4, 924–932. Viitattu 9.5.2025. https://www.thieme-connect.de/products/ejournals/abstract/10.1055/s-0041-1735527.

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Zamorano, J. M., Papachristou, P., & Bonacina S. 2023. Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. Journal of Medical Internet Research 25, e41294. Viitattu 17.1.2025. https://www.jmir.org/2023/1/e41294/PDF.

Asenne Nd. Tieteentermipankki. Viitattu 22.1.2025. Https://tieteentermipankki.fi/wiki/Nimitys:asenne.

Behavior Nd. Cambridge Dictionary. Viitattu 22.1.2025. Https://dictionary.cambridge.org/dictionary/english/behaviour.

Blek T., Lahdenperä, E. & Lehosmaa, J. 2024. Sote-ammattilaisten kyberturvallisella toiminnalla varmistetaan asiakas- ja potilasturvallisuutta. Julkaisu Jamk Areena nettisivuilla 2.7.2024. Viitattu 11.12.2024. https://arena.jamk.fi/fi/arena-pro/sote-ammattilaisten-kyberturvallisella-toiminnalla-varmistetaan-asiakas-ja-potilasturvallisuutta/.

Blek, T. & Solankallio- Vahteri, T. 2022. Terveydenhuollon henkilöstön tieto- ja kyberturvallisuusosaaminen. Jyväskylän ammattikorkeakoulu, Hyvinvointiyksikkö, Jyväskylä. Finnish Journal of eHealth and eWelfare 14, 4, 352–363. Viitattu 2.9.2024. https://journal.fi/finjehew/article/view/115829.

Cartwrigh, A., J. 2023. The elephant in the room: cybersecurity in healthcare. Journal of Clinical Monitoring and Computing 37, 1123–1132. Viitattu 14.12.2024 Https://pubmed.ncbi.nlm.nih.gov/37088852/.

Clarke, M & Martin, K. 2024. Managing cybersecurity risk in healthcare settings. Healthcare Management Forum 25,37,1, 17–20. Viitattu 15.1.2025. https://pmc.ncbi.nlm.nih.gov/articles/PMC10725101/.

Dart, M. & Ahmed, M. 2023, Evaluating Staff Attitudes, Intentions, and Behaviors Related to Cyber Security in Large Australian Health Care Environments: Mixed Methods Study. JMIR Hum Factors 10, e48220. Viitattu 9.5.2025. https://humanfactors.jmir.org/2023/1/e48220.

Defining ”skill” and ”competence” Nd. EU Sience Hub. Julkaisu Europan Unionin internet-sivuilla. Viitattu 22.1.2025. https://joint-research-centre.ec.europa.eu/scientific-activities-z/skills-and-competences/defining-skill-and-competence_en.

Digitaitotasot nd. Tieke – Tietoyhteiskunnan kehittämiskeskus ry. Julkaisu Tieke:n internet-sivuilla. Viitattu 30.8.2024. https://tieke.fi/digitaitotasot/.

Digitalisaatio ja työ N.d. Julkaisu työterveyslaitoksen internet-sivuilla. Viitattu 16.1.2025. Https://www.ttl.fi/teemat/tyoelaman-muutos/digitalisaatio-ja-tyo.

Digitalisaatio on keino kehittää toimintaa N.d. Vipuvoimaa EU:lta hanke. Julkaisu työterveyslaitoksen internet- sivuilla. Viitattu 16.1.2025. https://www.ttl.fi/yrittajan-digitieto-opas-digiajan-yrityksselle/teema-1-digi-muuttaa-tyota/digitalisaatio-on-keino-kehittaa-toimintaa.

Elo, S., Kajula, O., Tohmola, A. & Kääriäinen, M. 2022. Laadullisen sisällönanalyysin vaiheet ja eteneminen. Hoitotiede. 34, 4, 215–225. Viitattu 29.11.2024. https://www.theseus.fi/bitstream/handle/10024/789349/Laadullisen_sisallonanalyysin_vaiheet_ja_eteneminen.pdf?sequence=1&isAllowed=.

Gebeyew, A. S., Wordofa, Z.R., Muluneh, A. A., Shibaba, A.A., Walle, A.D., Tizie, S.B., Mengistie, M.B., Takillo, M.K., Assaye, B.T., Senishaw, A.F., Hailye, G., Shimie,A.W. & Butta, F.W. 2024. Attitudes of Health Professionals Toward Digital Health Data Security in Northwest Ethiopia: Cross-Sectional Study. Online Journal of Public Health Informatics 16, e57764. Viitattu 9.5.2025. https://ojphi.jmir.org/2024/1/e57764.

Hanhinen, T. 2010 Työelämäosaaminen: Kvalifikaatioiden luokitusjärjestelmän konstruointi. Tampereen yliopiston julkaisuja. Viitattu 28.5.2024. https://trepo.tuni.fi/bitstream/handle/10024/66674/978-951-44-8290-8.pdf?sequence=1&isAllowed=y.

Heinäsenaho, M., Äyräs-Blumberg, O. & Lähesmaa, J. 2023. Tekoäly mullistaa terveydenhuoltoa - mahdollisuudet hyödynnettävä viipymättä. Uusia tekoälymalleja käsittelevän kolumnisarjan 1. osa. Julkaisu valtioneuvoston internet-sivuilla 14.4.2023. Viitattu 23.1.2025. https://valtioneuvosto.fi/-//1271139/tekoaly-mullistaa-terveydenhuoltoa-mahdollisuudet-hyodynnettava-viipymatta.

Hore, K., Tan, M.H., Kehoe, A., Beegan, A., Mason, S., Al Mane, N., Hughes, D., Kelly, C., Wells, J. & Magner, C. 2024, Cybersecurity and critical care staff: A mixed methods study. International Journal of Medical Informatics 185, 105412. Viitattu 9.5.2025. https://www.sciencedirect.com/science/article/pii/S1386505624000753?via%3Dihub.

Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen suomessa 2023. Tutkimuseettisen neuvottelukunnan julkaisema ohje. Viitattu 20.5.2024. https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf.

Jalali, M.S., Bruckes, M., Westmattelmann, D. & Schewe, G. 2020. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. Journal of Medical Internet Research 22, 1, e16775. Viitattu 9.5.2025. https://www.jmir.org/2020/1/e16775/.

Järvinen, P. 2022. Yrityksen tietoturvaopas. Helsinki: Helsingin seudun kauppakamari.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas – tunnista uhat, hallitse riskit. Helsinki: Alma Talent.

Kajander- Unkuri, S. 2015. Nurse competence of graduating nursing students. Turun yliopiston julkaisuja, sarja D osa 1158. Viitattu 31.5.2024. https://www.utupub.fi/bitstream/handle/10024/103403/AnnalesD1158Kajander-Unkuri.pdf?sequence=2&isAllowed=y.

Kangasniemi, M., Pakkanen, P. & Korhonen, A. 2015. Professional ethics in nursing: an integrative review. Journal of Advanced Nursing 71,8, 1744–57. Viitattu 29.11.2024. https://www.researchgate.net/publication/271139792_Professional_ethics_in_nursing_An_integrative_review.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas – Näin kirjoitat opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kang, P. Kang, J. & Monsen, K.A. 2022. Nurse Information Security Policy Compliance, Information Competence, and Information Security Attitudes Predict Information Security Behavior. CIN: Computers, Informatics, Nursing 41, 8, 595–602. Viitattu 9.5.2025. https://onlinelibrary.wiley.com/doi/10.1111/jan.12619.

Kantola, A. & Grönholm, P. 2020. Terapiapotilaisiin kohdistunut tietomurto on voinut vaarantaa tuhansien ihmisten tietosuojan, kyseessä on täysin ”poikkeuksellinen tapahtuma”. Helsingin Sanomat 22.10.2020. Viitattu 4.6.2024. https://www.hs.fi/suomi/art-2000006687766.html.

Kessler, S.R., Pindek, S., Kleinman, G. Andel, S.A. & Specto, P.E. 2020, Information security climate and the assessment of information security risk among healthcare employees. Health Informatics Journal 26, 2, 461–473. Viitattu 9.5.2025. https://journals.sagepub.com/doi/epub/10.1177/1460458219832048.

Kioskli, K., Fotis, T., Nifakos, S. & Mouratidis, H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Journal of Applied Science 13, 6, 3410. Viitattu 11.12.2024. https://www.mdpi.com/2076-3417/13/6/3410.

Kuo, K., Talley, P.C. & Lin D.Y. 2021, Hospital Staff’s Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables. INQUIRY: Journal of Healthcare Provision and Public Health 58, 1–12. Viitattu 9.5.2025. https://journals.sagepub.com/doi/10.1177/00469580211029599.

KyberSoTe nd. JAMK. Julkaisu Jyväskylän Ammattikorkeakoulun internet-sivuilla. Viitattu 16.5.2024. https://www.jamk.fi/fi/projekti/kybersote.

KyberSoTe- Kyberturvallisuutta sote-arkeen nd. JAMK. Julkaisu Jyväskylän Ammattikorkeakoulun internet-sivuilla. Viitattu 16.5.2024. https://www.jamk.fi/fi/tutkimus-ja-kehitys/tki-projektit/kybersote-kyberturvallisuutta-sote-arkeen.

Kyberturvallisuuden sanasto 2018. Sanastokeskuksen julkaisuja. Viitattu 16.5.2024. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Kyberturvallisuuslaki on hyväksytty eduskunnassa - NIS2-direktiivin mukaiset velvoitteet astuvat voimaan 8.4.2025, 2025. Julkaisu traficom liikenne- ja viestintäviraston internet-sivuilla 8.4.2025. Viitattu 14.5.2025. https://traficom.fi/fi/ajankohtaista/kyberturvallisuuslaki-hyvaksytty-eduskunnassa-nis2-direktiivin-mukaiset-velvoitteet.

Kyberturvallisuus – Ohje sosiaali- ja terveydenhuollon toimijoille 2019. Sosiaali- ja terveysministeriön julkaisuja. Viitattu 16.5.2024. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161683/J14_Kyberturvallisuus_WEB.pdf?sequence=1&isAllowed=y.

Kyberturvallisuus vaatii jatkuvaa työtä 2022. Julkaisu Huoltovarmuuskeskuksen internetsivuilla 7.3.2022. Viitattu 13.5.2025. https://www.huoltovarmuuskeskus.fi/a/kyberturvallisuus-vaatii-jatkuvaa-tyota.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtionneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Viitattu 22.1.2025. https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila,+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213/30_Suomen+kyberturvallisuuden+nykytila,+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf?version=1.0&t=1487318599000.

Lehto, Ma., Pöyhönen, J. & Lehto, Mi. 2019. Kyberturvallisuus sosiaali- ja terveydenhuollossa – Loppuraportti vol. 2. Jyväskylän yliopiston julkaisuja. Viitattu 3.9.2024. https://jyx.jyu.fi/bitstream/handle/123456789/63325/Kyberturvallisuus_Vol2FINAL.pdf.

Lehtiö, L. & Johansson, E. 2016. Järjestelmällinen tiedonhaku hoitotieteessä. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. Stolt, M., Axelin, A. & Suhonen, R. Turku: Turun Yliopisto. 35–55. Hoitotieteen laitoksen julkaisuja, tutkimuksia ja raportteja.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy.

Lintulahti, M. 2024. Miten hallita tekoälyn käytön tietoturvariskejä?. Artikkeli Huoltovarmuuskeskuksen verkkolehti Varmuuden vuoksi- sivuilla. Julkaistu 12.2.2024. Viitattu 12.5.2025. https://www.varmuudenvuoksi.fi/artikkeli/miten-hallita-tekoalyn-kayton-tietoturvariskeja.

Loula, P. 2024. Uutta tietoa laajasta tietomurrosta: Jopa turvakiellon alaisten tietoja saattanut vuotaa. Teksti Helsingin Sanomien nettisivuilla 13.5.2024. Viitattu 3.9.2024. https://www.hs.fi/helsinki/art-2000010422340.html.

Magdalinou, A., Kalokairinou, A., Malamateniou, F. & Mantas, J. 2022. Assessing Internal Consistency of HAIS-Q: A Survey Conducted in Greek Hospitals. Advances in Informatics, Management and Technology in Healthcare. 29, 295, 24–27. Viitattu 9.5.2025. https://ebooks.iospress.nl/volumearticle/60158.

Mitä on tietoturva? nd. Jyväskylän yliopisto. Julkaisu Jyväskylän yliopiston internet- sivuilla. Viitattu 14.12.2024. Https://www.jyu.fi/fi/yliopistopalvelut/digipalvelut/palvelut/tietoturva/mita-on-tietoturva.

Mohammed, G.D.F., Chandran, P., Mansoor, Z. & Mohaddi, M. 2021, Locked the Car, Why Not the Computer: A Qualitative and Quantitative Study on Data Safety Compliance. Cureus 13, 8, e17513. Viitattu 9.5.2025. https://www.cureus.com/articles/68150-locked-the-car-why-not-the-computer-a-qualitative-and-quantitative-study-on-data-safety-compliance#!/.

Morris, M.E., Brusco, N.K., Jones, J., Taylor, N.F., East, C.E., Semciw, A.I., Edvardsson, K., Thwaites, C., Bourke, S.L., Khan, U.R., Fowler-Davis, S. & Oldenburg, B. 2023. The Widening Gap between the Digital Capability of the Care Workforce and Technology-Enabled Healthcare Delivery: A Nursing and Allied Health Analysis. Healthcare 11, 7, 994. Viitattu 9.5.2025. https://www.mdpi.com/2227-9032/11/7/994.

Nifakos, S., Chandramouli, K., Papachristou, P., Koch, S., Nikolaou, C. K., Panaousis, E., & Bonacina, S. 2021. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors 21, 15, 5119. Viitattu 7.1.2025. https://www.mdpi.com/1424-8220/21/15/5119.

Niela-Vilén, H. & Hamar, L. 2016. Kirjallisuuskatsauksen vaiheet. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. Stolt, M., Axelin, A. & Suhonen, R. Turku: Turun Yliopisto. 23–34. Hoitotieteen laitoksen julkaisuja, tutkimuksia ja raportteja.

Nunes, P., Antunes, M. & Silva, C. 2021, Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. Procedia Computer Science 181, 173–181. https://www.sciencedirect.com/science/article/pii/S1877050921001563.

Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille 2019. Liikenne- ja viestintävirasto ja kyberturvallisuuskeskus Traficomin julkaisuja 123/2019. Viitattu 13.5.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf.

Peltomäki, J. & Norppa, K. 2015. Rikos meni verkkoon – Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum.

Pöyhönen, J., Lehto, Ma. & Lehto, Mi. 2019. Kyberturvallisuus sairaalajärjestelmissä: osa 2 Toiminnan kehittäminen. Jyväskylän Yliopisto. Informaatioteknologian tiedekunnan julkaisuja no. 75/2019. Viitattu 17.5.2025. https://urn.fi/URN:ISBN:978-951-39-7699-6.

Rajamäki, J., Rathod, P. & Kioskli, K. 2023. Demand Analysis of the Cybersecurity Knowledge Areas and Skills for Nurses: Preliminary Findings. Proceedings of the 22nd European Conference on Cyber Warfare and Security 22, 1, 711–716. Viitattu 22.12.2024. https://www.theseus.fi/bitstream/handle/10024/804915/Rajamaki_Rathod_Kioskli.pdf?sequence=1&isAllowed=y.

Rizzoni, F. Magalini, S. Casaroli, S., Mari, P., Dixon, M. & Coventry, L. 2022, Phishing simulation exercise in a large hospital: A case study. Digital Health 16, 8, 20552076221081716. Viitattu 9.5.2025. https://journals.sagepub.com/doi/10.1177/20552076221081716.

Sanmark, J. & Sanmark, E. 2024. Mitä tiedämme generatiivisen tekoälyn hyödyistä terveydenhuollossa? Lääketieteellinen Aikakauskirja Duodecim 140,12, 1023–30. Viitattu 23.1.2025. Https://www.duodecimlehti.fi/lehti/2024/12/duo18143.

Salminen, A 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston opetusjulkaisuja 62. Viitattu 20.5.2024. https://osuva.uwasa.fi/bitstream/handle/10024/7961/isbn_978-952-476-349-3.pdf?sequence=1&isAllowed=y.

Schmidt, T., NØhr, C. & Koppel, R. 2021. A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions. Public health and informatics 27, 281, 635–639. Viitattu 9.5.2025. https://ebooks.iospress.nl/doi/10.3233/SHTI210248.

Sulosaari, V. & Kajander-Unkuri, S. 2016. Integroitu kirjallisuuskatsaus. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. Stolt, M., Axelin, A. & Suhonen, R. Turku: Turun Yliopisto. 107–117. Hoitotieteen laitoksen julkaisuja, tutkimuksia ja raportteja.

Systemaattinen tiedonhaku: opas 2024. Opas Tampereen Yliopiston kirjaston internet-sivuilla. Viitattu 18.10.2024. https://libguides.tuni.fi/systemaattinen-tiedonhaku.

Taidot Nd. Finto- yleinen suomalainen asiasanasto ja ontologiapalvelu. YSO yleinen suomalainen ontologia. Viitattu 22.1.2025. https://finto.fi/yso/fi/page/p5798.

Tekoäly tulee muuttamaan myös kyberhyökkäyksiä 2022. Julkaisu Traficom:n internet-sivuilla 13.12.2022. Viitattu 23.1.2025. Https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekoaly-tulee-muuttamaan-myos-kyberhyokkayksia.

Terveydenhuolto nd. Teksti Huoltovarmuuskeskuksen nettisivuilla. Viitattu 17.5.2024. https://www.huoltovarmuuskeskus.fi/toimialat/terveydenhuolto.

The NIST Cybersecurity Framework (CSF) 2.0, 2024. National Institute of Standards and Technology. Julkaistu February 26, 2024. Viitattu 17.5.2025. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

Tiedonhaun opas: 2024. Opas Tampereen Yliopiston kirjaston internet- sivuilla. Viitattu 18.9.2024. https://libguides.tuni.fi/tiedonhaun-opas.

Tietoturvasuunnitelma 2024. Terveyden- ja hyvinvoinnin laitos THL. Julkaisu THL:n internet sivuilla, päivitetty 7.6.2024. Viitattu 16.5.2025. https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/tiedonhallinnan-ohjaus/tietoturvasuunnitelma.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällön analyysi. Helsinki: Kustannusosakeyhtiö Tammi.

Valkeapää, 2016. Tutkimusaineiston valinta systemaattisessa kirjallisuuskatsauksessa. Julkaisussa Kirjallisuuskatsaus hoitotieteessä. Toim. Stolt, M., Axelin, A. & Suhonen, R. Turku: Turun Yliopisto. 56–66. Hoitotieteen laitoksen julkaisuja, tutkimuksia ja raportteja.

Vilkka, H. 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. Helsinki: Art House.

Vuorikari, R., Kluzer, S. & Punie, Y. 2022. DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes. Luxembourgh: Publications Office of the European Union. Viitattu 31.5.2024. https://publications.jrc.ec.europa.eu/repository/handle/JRC128415.

Willing, M., Dresen, D., Gerlitz, E., Haering, M., Smith, M., Binnewies, C., Guess, T., Haverkamp, U. & Schinzel, S. 2021, Behavioral responses to a cyber attack in a hospital environment. Scientific reports 29, 11, 19352. Viitattu 9.5.2025. https://pmc.ncbi.nlm.nih.gov/articles/PMC8481235/.

Yeo, L. H. & Banfield, J. 2022. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Online Research Journal Perspectives in health Information Management 15, 19, 2, 1i. Viitattu 9.5.2025. https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/.

Yeng, P.K., Fauzi, M.A. & Yang, B. 2022. A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. Journal Information 13, 7, 335. Viitattu 9.5.2025. https://www.mdpi.com/2078-2489/13/7/335.

Liitteet

Liite 1. Tutkimuksessa käytetyt tietokannat ja hakusanat

Hakulausekkeet	Tietokanta: CINAHL
Hakutuloksia: 63kpl	(MH Professionalism) OR (MH ”Health personnel”) OR "Health care personnel" OR "Health personnel" OR "Health care professional*" OR "Health professional*" OR Hospital* OR ”Social Work*” OR (MH ”Social worker”) OR (MH ”Social work service”) OR "Health care" AND (MH ”Data security”) OR ”Cyber security” OR ”Data security” OR "information security" AND (MH ”Professional competence”) OR (MH ”Professional Knowledge”) OR competen* OR skill* OR attitude OR awareness OR behavior
Hakulausekkeet	Tietokanta: ProQuest
Hakutuloksia: 45kpl	"Health care" OR "Health care personnel" OR "Health personnel" OR "Health care professional*" OR "Health professional*" OR "social work*" AND "Cyber Security" OR "Data Security" OR "It Security" OR "Information security" AND competen* OR skill* OR knowled* OR attitude OR awareness OR behavior
Hakulausekkeet	Tietokanta: PubMed
Hakutuloksia: 201kpl	("Health Personnel"[Mesh] OR "Health care personnel" OR "Health care professional*" OR "Social work*" OR "Social workers" [Mesh] OR "Health care") AND ("Computer Security"[Mesh] OR "Cyber security" OR "Digital security" OR "Information security")) AND (competen* OR skill* OR attitude OR awareness OR knowled* OR behavior OR "professional competence"[Mesh] OR behivor [Mesh])
Hakulausekkeet	Tietokanta: Sage Journals
Hakutuloksia: 57kpl	”Health care” OR ”health professional” OR "Health personnel" OR hospital* OR nursing*AND ”cyber security” OR information security” OR ”data security” AND competence OR knowledge OR skill OR attitude OR awareness OR behavior
Hakulausekkeet	Tietokanta: Sience Direct
Hakutuloksia: 141kpl	”Cyber security” AND ”health care” AND competence OR skill OR attitude OR awareness OR behavior

Liite 2. Aineiston laadun arviointi Kangasniemi, Pakkasen ja Korhosen mukaan (2015) (Muokattu Bowling 2002 ja Gazaria 2013)

Julkaisu, Tekijä(t), vuosi, julkaisumaa	**Tarkoitus**	**Tutkimusmenetelmä**	**Otos ja ominaisuudet**	**Laadun arviointi kriteerit** (K= kyllä, H= heikko, E= ei raportoitu)
A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals Prosper Kandabongee Yeng, Muhammad Ali Fauzi, and Bian Yang, 2022, Ghana	Arvioida terveydenhuollon henkilöstön kykyä noudattaa kyberturvallisuus käytäntöjä paperittomissa sairaaloissa	Monimenetelmällinen tutkimus, joka toteutettiin kvantitatiivisella kyselylomakkeella sekä haastatteluilla ja ryhmäkeskusteluilla. Tulokset analysointiin tilastollisin ja laadullisin menetelmin	212 vastaajaa, joista miehiä 50,5 % ja naisia 49,5 %. Vastaajista 50,9 % oli hoitajia	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions Thomas Schmidt, Christian NØhr ja Ross Koppel, 2021, Tanska	Arvioida sairaalahenkilökunnan tietoturvatietoisuutta Tanskan viidellä eri alueella	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylomakkeella. Tulokset analysoitu tilastollisin menetelmin	1136 vastaajaa, joista lääkäreitä 202, hoitajia 464, sihteeri 379, röntgenhoitaja 91. Henkilöstö työskentelee viidellä eri alueella Tanskassa	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (E) Keskustelu ja johtopäätökset kuvattu (K)
Assessing Internal Consistency of HAIS-Q: A Survey Conducted in Greek Hospitals Andriana Magdalinou, Athena Kalokairinou, Flora Malamateniou ja John Mantas, 2022, Kreikka	Arvioida Health Information Security Awareness Questionnaire (HAIS-Q) -mittarin luotettavuutta ja johdonmukaisuutta terveydenhuollossa	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylomakkeella. Tulokset analysoitu tilastollisin menetelmin	165 hoitajaa, joista 82,4 % oli naisia ja 17,6 % miehiä	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Attitudes of Health Professionals Toward Digital Health Data Security in Northwest Ethiopia: Cross-Sectional Study Ayenew Sisay Gebeyew, Zegeye Regasa Wordofa, Ayana Alebachew Muluneh, Adamu	Arvioida terveydenhuollon ammattilaisten asenteita ja tietoisuutta digitaalisten terveystietojen turvallisuudesta	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylomakkeella. Tulokset analysoitu tilastollisin menetelmin	402 vastaajaa, joista miehiä 63,2 % ja naisia 26,8 %. Tutkimukseen otettiin mukaan vain henkilöt, jotka käyttävät digitaalisia työkaluja työnsä tukena. Kyselyt toteutettiin opetussairaaloissa	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)

Ambachew Shibabaw, Agmasie Damtew Walle, Sefefe Birhanu Tizie, Muluken Belachew Mengistie, Mitiku Kassaw Takillo, Bayou Tilahun Assaye, Adualem Fentahun Senishaw, Gizaw Hailye, Aynadis Worku Shimie, Fikadu Wake Butta, 2024, Ethiopia				
Behavioral responses to a cyber attack in a hospital environment Markus Willing, Christian Dresen, Eva Gerlitz, Maximilian Haering, Matthew Smith, Carmen Binnewies, Tim Guess, Uwe Haverkamp, Sebastian Schinzel, 2021, Saksa	Tutkia henkilöstön käyttäytymistä ja reaktioita kyberhyökkäyksissä	Stimulaatio testi. Tulokset analysoitu laadullisin menetelmin	20 osallistujaa tehohoito ympäristöstä	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Cybersecurity and critical care staff: A mixed methods study Kevin Hore, Mong Hoi Tan, Anne Kehoe, Aidan Beegan, Sabina Mason, Nader Al Mane, Deirdre Hughes, Caroline Kelly, John Wells, and Claire Magner, 2024, Irlanti	Arvioida tehohoitohenkilöstön kyberturvallisuuskäytäntöjä, asenteita ja käyttäytymistä terveydenhuollossa	Monimenetelmällinen tutkimus, joka toteutettiin kvantitatiivisella kyselylomakkeella sekä haastatteluilla ja ryhmäkeskusteluilla. Tulokset analysointiin tilastollisin ja laadullisin menetelmin	259 vastaajaa, joista naisia 75 %, miehiä 23 % ja ”en halua sanoa” 2 %. Hoitajia oli 61 %, lääkäreitä 24 % ja loput 16 % muita ammattilaisia.	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (E) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions Paulo Nunes, Mário Antunes, Carina Silva, 2021, Portugali	Arvioida kyberturvallisuusasenteita ja -käyttäytymistä terveydenhuollossa	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylomakkeella. Tulokset analysoitu tilastollisin menetelmin	56 vastaajaa, joista naisia 71 % ja miehiä 29 %	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (E) Keskustelu (E) ja johtopäätökset kuvattu (K)
Evaluating Staff Attitudes, Intentions, and Behaviors Related to Cyber Security in Large Australian Health Care Environments: Mixed	Tutkia henkilöstön asenteita, aikomuksia ja käyttäytymistä suhteessa kyberturvallisuuteen	Monimenetelmällinen tutkimus, joka toteutettiin kvantitatiivisella kyselylomakkeella ja haastatteluilla. Tulokset analysoitiin tilastollisin ja laadullisin menetelmin.	Internet kyselyllä 103 vastaajaa. Haastatteluissa 9 haastateltavaa	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K)

Methods Study Martin Dart, Mohiuddin Ahmed, 2023, Australia				Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Healthcare Professional's Knowledge, Awareness, and Attitude toward Patients' Data Privacy and Security in Clinical Research Monirah A. Albabtain, Dalal AlOtaibi, Nourah AlMazial, Nouf Aloudah, Haneen Mohammed Alghosoon, Amr A. Arafat, 2024, Saudi Arabia	Arvioida terveydenhuollon ammattilaisten tietämystä, tietoisuutta ja asenteita potilastietojen yksityisyyteen ja turvallisuuteen liittyen kliinisessä tutkimuksessa	Monimenetelmällinen tutkimus, joka toteutettiin kyselylomakkeella, joka sisälsi strukturoituja ja avoimia kysymyksiä. Tulokset analysointiin tilastollisin ja laadullisin menetelmin.	108 vastaajaa, joista 20,37 % oli lääkäreitä ja loput 80,63 % ei-lääkäreitä.	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables Kuang-Ming Kuo, Paul C. Talley, Dyi-Yih Michael Lin, 2021, Taiwan	Tutkia mitkä tekijät vaikuttavat henkilöstön tietoturvakäytäntöihin sitoutumiseen. Erityisesti tarkastelun alla on pelotetekijä osana käyttäytymistä	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylomakkeella. Tulokset analysoitu tilastollisin menetelmin	299 vastaajaa, joista naisia 70,57 % ja miehiä 19,47 %. Vastaajista työskenteli terveyskeskuksessa 47.49 % ja alueellisessa sairaalassa 40,80 %.	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis Liu Hua Yeo, James Banfield, 2022, Yhdysvallat	Tutkia terveydenhuollon tietomurtoja vuosien 2015–2020 välillä	Tutkiva analyysi. Tulokset analysoitu laadullisin menetelmin.	Tietomurrot käsitelty ja luokiteltu teemojen mukaisesti	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (E) Keskustelu ja johtopäätökset kuvattu (K)
Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities Dari Alhuwail, Eiman Al-Jafar, Yousef Abdulsalam, Shaikha AlDuaij, 2021, Kuwait	Tutkia terveydenhuollon ammattilaisten tietoisuutta ja käyttäytymistä tietoturvan suhteen julkisessa terveydenhuollossa	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylomakkeella. Tulokset analysoitu tilastollisin menetelmin	453 vastaajaa, joista 69,4 % naisia ja 30,6 % miehiä. Osallistujat lääkäreitä (64.5 %), hoitajia (30.8 %) ja muita ammattilaisia (4.6 %)	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Information security climate and the assessment of	tutkia terveydenhuollon työntekijöiden tietoisuutta	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylo-	252 vastaajaa, joista 91 miehiä, 136 naisia ja 25 sukupuolen	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K)

information security risk among healthcare employees Stacey R Kessler, Shani Pindek, Gary Kleinman, Stephanie A Andel, Paul E Specto, 2020, Yhdysvallat	ja asenteita tietoturvaan liittyvistä riskeistä.	makkeella. Tulokset analysoitu tilastollisin menetelmin	ilmoittamatta jättänyttä. Vastaajien ammattiryhmät; farmaseutti, hoitoapulaiset, hammaslääkärit ja lääkärin avustajat. Työntekijät eri organisaatioista	tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Locked the Car, Why Not the Computer: A Qualitative and Quantitative Study on Data Safety Compliance Ghulam Dastagir Faisal Mohammed, Prakash Chandran, Zaina Mansoor, Momin Mohaddi, 2021, Iso-Britannia	Arvioida miksi työntekijät eivät noudata digitaalisia turvallisuus käytäntöjä yhtä huolellisesti kuin fyysisiä turvallisuustoimenpiteitä	Monimenetelmällinen tutkimus, joka toteutettiin havainnoinnilla/ interventiolla sekä laadullisilla haastatteluilla. Tulokset analysoitiin tilastollisin ja laadullisin menetelmin.	13 lääkärin haastattelua, sekä 2 havainnointi-/ interventiopäivää sairaalakontekstissa.	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (E) Tutkimuksen rajoitukset kuvattu (E) Keskustelu ja johtopäätökset kuvattu (K)
Nurse Information Security Policy Compliance, Information Competence, and Information Security Attitudes Predict Information Security Behavior Purum Kang, Jiwon Kang, Karen A. Monsen, 2022, Korea	tutkia sairaanhoitajien tietoturvapolitiikan noudattamisen, tietoturvakompetenssin ja asenteiden vaikutusta käytännön tietoturvakäyttäytymiseen	Kvantitatiivinen tutkimus. Tiedot kerätty kyselylomakkeella. Tulokset analysoitu tilastollisin menetelmin	200 vastaajaa, joista 182 naisia ja 18 miehiä. Kaikki ammatiltaan hoitajia.	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Phishing simulation exercise in a large hospital: A case study Fabio Rizzoni, Sabina Magalini, Alessandra Casaroli, Pasquale Mari, Matt Dixon, Lynne Coventry, 2022, Italia	Tutkia sairaalan henkilöstön kykyä tunnistaa kalastelu-viestit	Stimulaatio tutkimus. Tulokset analysoitu tilastollisin menetelmin.	Lähetetty kalastelu-viestejä 3 erässä (5313kpl, 2700kpl, 5198kpl) koko sairaalan henkilökunnalle	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (E) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
The Widening Gap between the Digital Capability of the Care Workforce and Technology-Enabled	Artikkeli tarkastelee kuilua terveydenhuollon työntekijöiden digitaalisten taitojen ja terveydenhuollon kehittyneen teknologian välillä. Artikkelissa tutkitaan hoitohenkilökunnan valmiuksia	Monimenetelmällinen kaksi vaiheinen tutkimus. Aineisto kerättiin kvantitatiivisella kyselylomakkeella ja haastatte-	24 terveydenhuollon työntekijää (17 naista ja 7 miestä) eri terveydenhuollon piireistä Australiasta.	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K)

Healthcare Delivery: A Nursing and Allied Health Analysis Meg E. Morris, Natasha K. Brusco, Jeff Jones, Nicholas F. Taylor, Christine E. East, Adam I. Semciw, Kristina Edvardsson, Claire Thwaites, Sharon L. Bourke, Urooj Raza Khan, Sally Fowler-Davis, Brian Oldenburg 2023, Australia	käyttää digitaalisia työkaluja ja teknologioita, jotka ovat yhä keskeisempi osa terveydenhuoltoa	luilla. Tulokset analysoitiin tilastollisin ja laadullisin menetelmin.		Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)
Why Employees (Still) Click on Phishing Links: Investigation in Hospitals Mohammad S. Jalali, Maike Bruckes, Daniel Westmattelmann, Gerhard Schewe, 2020, Yhdysvallat	Tutkia, miksi työntekijät edelleen lankeavat tietojen kalasteluviesteihin koulutuksesta ja ohjeista huolimatta	Monimenetelmällinen tutkimus, joka toteutettiin interventiolla sekä kvantitatiivisella kyselylomakkeella. Tulokset analysoitiin tilastollisin menetelmin.	397 vastaajaa, joista 309 naisia ja 82 miehiä. Osallistujat kahdesta eri sairaalasta	Tutkimuksen tarkoitus ja tavoitteet kuvattu (K) tutkimusasetelma kuvattu (K) tutkimusmenetelmät asianmukaiset (K) Teoreettinen viitekehys kuvattu (K) Tutkimuksen rajoitukset kuvattu (K) Keskustelu ja johtopäätökset kuvattu (K)