Anna-Liisa Ojala, Karo Saharinen & Tuomo Sipola

Suomalaisten oppilaitosten valmius kohdata kyberkriisejä

Loppuraportti

jamk | Jyväskylän ammattikorkeakoulu

Työsuojelurahasto
Arbetarskyddsfonden
The Finnish Work Environment Fund

Suomalaisten oppilaitosten valmius kohdata kyberkriisejä

Loppuraportti, 18 sivua

Tekijät: Anna-Liisa Ojala, Karo Saharinen & Tuomo Sipola

Tutkimushankkeen ovat rahoittaneet Työsuojelurahasto ja Jyväskylän Ammattikorkeakoulu

Taitto: Grano Oy, 2025

ISBN 978-951-830-793-1 (PDF)

Alkusanat

Tämä raportti sisältää kuvauksen Suomalaisten oppilaitosten valmius kohdata kyberkriisejä -hankkeen toteuttamisesta ja tuloksista. Osa tutkimusartikkeleista on vielä käsikirjoitusvaiheessa tutkimusjulkaisujen arviointiprosesseissa tätä kirjoitettaessa. Näin ollen hankkeen tulokset täydentyvät vielä lähikuukausina.

Hanke toteutettiin aikavälillä 1.1.2024-31.8.2025. Hanketta ei olisi ollut mahdollista toteuttaa ilman kolmen ammatillisen oppilaitoksen aktiivista osallistumista. Olemme heille kiitollisia tutkimusyhteistyöstä.

Hanketta rahoitti Työsuojelurahasto, jota kiitämme oppilaitosten kyberturvallisuuden tutkimuksen tukemisesta. Toivomme edistävämme hankkeen tuloksilla suomalaisen työn turvallisuutta tunnistamalla digitaalisen resilienssin keskeisiä tekijöitä oppilaitostyössä.

Jyväskylä 12.8.2025

Kirjoittajat

Sisältö

Tiivistelmä **5**

1. Työn aihe ja tarkoitus **6**

2. Keskeiset käsitteet **8**

3. Aineisto ja metodit **9**

4. Keskeiset tulokset **10**

4.1 Henkilöstön kyberturvallisuusosaaminen ja oppiminen 10

4.2 Poikkeamien havaitseminen ja niistä raportointi 11

4.3 Käytettävyyden ja turvallisuuden välinen jännite 12

4.4 Oppilaitosten kyberturvallisuus yhteiskunnallisena kysymyksenä 13

5. Johtopäätökset **14**

Lähteet **16**

Tiivistelmä

Tutkimushankkeen aiheena oli ammatillisten oppilaitosten kyberturvallisuusosaaminen ja -käytännöt. Tarkoituksena oli tuottaa uutta tietoa siitä, miten oppilaitosten henkilöstö ymmärtää ja toteuttaa kyberturvallisuutta omassa työssään, miten osaamista voidaan kehittää sekä millaisia organisatorisia ja teknisiä ratkaisuja tarvitaan oppilaitosten ja laajemmin työelämän turvallisuuden varmistamiseksi.

Aineisto kerättiin laadullisin menetelmin kolmessa ammatillisessa oppilaitoksessa eri puolilla Suomea. Tutkimukseen osallistui 27 henkilöä, joiden joukossa oli opettajia, erityisopettajia, opinto-ohjaajia, kuraattoreita, opintohallinnon työntekijöitä, tietohallinnon asiantuntijoita ja oppilaitosjohtoa. Haastattelut toteutettiin teemahaastatteluina, ja lisäksi kerättiin havainnointimuistiinpanoja oppitunneilta, johtamistyöstä ja tietohallinnon toiminnasta. Aineisto analysoitiin induktiivisella temaattisella analyysilla, ja tulkinnassa hyödynnettiin organisaation oppimisen teorioita, käytettävyyden ja turvallisuuden tasapainon malleja sekä tilannetietoisuuden ja vertaisoppimisen käsitteitä.

Tulokset osoittavat, että henkilöstön kyberturvallisuusosaaminen vaihtelee merkittävästi. Koulutukset koetaan usein liian yleisiksi suhteessa työroolien erityispiirteisiin, ja epävirallinen vertaisoppiminen on tärkeä mutta alihyödynnetty osaamisen kehittämisen muoto. Lisäksi työntekijät käyttävät mahdollisten poikkeamatapausten tulkitsemisessa ja ilmoittamisessa sellaisia toimintatapoja, jotka eivät organisaatioiden tietohallinnon mukaan ole toivottavimpia. Käytettävyyden ja turvallisuuden välinen jännite näkyy myös työn arjessa: liian monimutkaiset tai tarkoitukseen toimimattomat järjestelmät voivat johtaa kuormittuneisuuden lisääntymiseen tai turvakäytäntöjen kiertämiseen. Selkeät prosessit, käytännönläheinen koulutus ja roolikohtainen ohjeistus vahvistavat kyberturvallisuutta sekä oppilaitoksissa että työelämäyhteistyössä.

Johtopäätöksenä voidaan todeta, että kyberturvallisuuden kehittäminen ammatillisissa oppilaitoksissa hyödyttää laajasti suomalaista työelämää. Parantunut osaaminen ja selkeytyneet toimintamallit vähentävät tietoturvapoikkeamien riskiä, tukevat toiminnan jatkuvuutta ja lisäävät resilienssiä myös niillä aloilla, joihin oppilaitokset kouluttavat työvoimaa.

1. Työn aihe ja tarkoitus

Tutkimuksessa tarkasteltiin ammatillisten oppilaitosten kyberturvallisuusriskien luonnetta ja työyhteisöjen valmiutta toimia kyberkriiseissä, ja luotiin alalle harjoittelu- ja toimintasuosituksia.

Tutkimuksella oli neljä tavoitetta:

- Tunnistaa ammatillisten oppilaitosten kyberturvallisuusriskien laatu.
- Tunnistaa ammatillisten oppilaitosten henkilöstön kokemus ja kyvykkyys tunnistaa kyberriskejä ja toimia työyhteisön kohdatessa mahdollisen kyberriskin.
- Luoda systemaattinen kuva ammatillisen oppilaitoksen henkilökunnan kyvykkyydestä toimia kyberkriisitilanteessa.
- Muodostaa konkreettisia harjoittelu- ja toimenpidesuosituksia ammatillisille oppilaitoksille, jotta ne olisivat jatkossa valmiimpia ja osaisivat toimia tehokkaasti ja järkevästi kyberhyökkäysten sattuessa.

Tutkimuksen tarpeellisuus syntyi siitä trendistä, että teknologia on muuttanut oppilaitostyötä, opetusta ja opettajien osaamisvaatimuksia, mutta digitaaliset järjestelmät ja opetusteknologiat ovat tuoneet myös kyberturvallisuusriskin (Ulven & Wangen, 2021). Digitalisaatio on muuttanut oppilaitosten toimintaympäristöä merkittävästi. Ammatillisissa oppilaitoksissa käytetään monimutkaisia oppimisympäristöjä, hallintojärjestelmiä ja opetusteknologioita, jotka samalla lisäävät hyökkäyspinta-alaa kyberuhille (Cains ym., 2021).

Ammatillisen oppilaitossektorin erityispiirre on läheinen yhteys työelämään (Ferm, 2021). Opiskelijat käsittelevät työpaikoilla aitoja asiakas- ja potilastietoja sekä käyttävät alan järjestelmiä, jolloin oppilaitosten kyberturvallisuus vaikuttaa suoraan myös työpaikkojen turvallisuuteen. Lisäksi viimeaikainen tutkimus on tunnistanut kasvavan riippuvuuden pilvipalveluista myös koulutussektorilla (Thavi ym., 2024). Pilvipalveluiden lisääntyminen muuttaa sitä kokonaisuutta, johon pitää kiinnittää huomiota, kun kyberturvallisuutta hallitaan ja tuetaan. Kun järjestelmät ovat yhä tiiviimmin ulkoisten palveluntarjoajien hallinnassa, myös oppilaitosten käytännöt, protokollat ja tukimekanismit rakentuvat entistä enemmän näiden tarjoajien varaan. Näin muodostuu mielenkiintoinen tutkimuskohde oppilaitostyöstä, jossa oppilaitoksen omat käytännöt ja prosessit yhdistyvät ulkoisten palveluntuottajien tarjoamiin digitaalisiin toimintaympäristöihin ja tukipalveluihin.

Tutkimusasetelma tuo esiin myös sen, että kyberturvallisuusosaaminen ei ole vain tietohallinnon asia, vaan koko työyhteisön yhteinen tehtävä. Jokaisen työntekijän kyvykkyys tunnistaa ja raportoida poikkeamia on osa työyhteisön resilienssiä. Tämä laajentaa työsuojelun käsitettä digitaaliselle alueelle: kyse ei ole vain siitä, että järjestelmät toimivat teknisesti oikein, vaan siitä, että työntekijät voivat kokea työnsä turvalliseksi ja hallittavaksi myös digitaalisessa ympäristössä. Lisäksi tutkimus vastaa ajankohtaisiin strategisiin tarpeisiin. Suomen kyberturvallisuusstrategia 2024–2035 korostaa koulutuksen merkitystä koko yhteiskunnan turvallisuuden vahvistajana. Euroopan parlamentin ja neuvoston direktiivi 2022/2555 verkko- ja tietojärjestelmien turvallisuudesta velvoittaa varsinkin kriittisillä toimialoilla toimivia organisaatioita riskiperustaiseen lähestymistapaan ja kriittisten digitaalisten omaisuuksien suojaamiseen, mikä heijastuu myös koulutussektorille.

Kyberturvallisuusosaaminen ei ole vain tietohallinnon asia, vaan koko työyhteisön yhteinen tehtävä.

2. Keskeiset käsitteet

Kyberturvallisuus on tämän tutkimuksen kattokäsite, joka sisältää tässä sekä tietosuojan että tietoturvan (ks. Ojala, Sipola & Saharinen, 2025). **Tietosuoja** tarkoittaa yksilöihin ja organisaatioihin liittyvien tietojen suojaamista lainsäädännön ja ohjeistusten avulla, kun taas **tietoturva** viittaa tiedon suojaamiseen teknisistä konteksteista riippumatta. Kyberturvallisuudella tarkoitetaan toimenpiteitä, joilla suojataan viestintä- ja tietojärjestelmät, käyttäjät, tiedot ja laitteet erilaisia uhkia vastaan. Ihmisillä on keskeinen rooli osana kyberturvallisuutta. Digitaaliset uhkat syntyvät usein inhimillisistä virheistä tai valinnoista, joten käyttäjät voivat toiminnallaan sekä vahvistaa että heikentää organisaation turvallisuutta (Adams & Sasse, 1999; Cains ym., 2021). Kyberturvallisuuden ei tule jäädä vain teknisten ratkaisujen tasolle, vaan sen on ulotuttava käyttäjien toimintaan, asenteisiin ja osaamiseen (NIST, 2014).

Keskeisiä peruskäsitteitä ovat myös **uhka, riski, poikkeama ja digitaalinen omaisuus**. Uhalla tarkoitetaan mahdollista tapahtumaa tai toimijaa, joka voi vahingoittaa järjestelmiä tai tietoja, ja ne voidaan jaotella esimerkiksi teknisiin, tunnuksiin liittyviin tai käyttäytymispohjaisiin uhkiin (Przymus ym., 2024). **Kyberturvallisuusriskillä** viitataan uhkan todennäköisyyden ja seurauksen yhdistelmään (Lacey, 2009). **Poikkeama** on tilanne, jossa uhka toteutuu ja vaarantaa tiedon luottamuksellisuuden, eheyden tai saatavuuden (NIST, 2025b). **Digitaalinen omaisuus** puolestaan viittaa organisaation toiminnalle keskeisiin resursseihin, kuten tietoon, prosesseihin, palveluihin ja laitteisiin (NIST, 2025a).

Kyberturvallisuudessa korostuu riskiperustainen lähestymistapa. Kaikkea ei voida suojata yhtä vahvasti, joten resurssit kannattaa kohdistaa kriittisimpiin digitaalisiin omaisuuksiin. NISTin (National Institute of Standards and Technology) riskienhallintakehys (Force, 2018) painottaa uhkien arviointia ja hallintatoimenpiteiden priorisointia suhteessa organisaation toiminnan jatkuvuuteen. Lisäksi NISTin kyberturvallisuusviitekehys korostaa viittä perusfunktiota, tunnista, suojaa, havaitse, reagoi ja toivu, joihin organisaatioiden tulisi rakentaa kyberturvallisuuden hallinta (NIST, 2024). Näihin perusfunktioihin liittyy myös resilienssin käsite: organisaatioiden painopiste ei tule olla vain hyökkäysten estämisessä, vaan myös siinä, että organisaatio kykenee toipumaan nopeasti poikkeamatilanteista ja jatkamaan toimintaansa häiriöistä huolimatta.

Kyberturvallisuus on jaettua vastuuta. Se ei kuulu vain tietohallinnolle, vaan jokainen oppilaitoksen työntekijä opettajista ja rehtoreista oppilaanohjaajiin, siivoojiin ja kirjastonhoitajiin tekee päivittäin valintoja, joiden seuraukset voivat vahvistaa tai heikentää oppilaitoksen kyberturvallisuutta. Turvallisuus rakentuu siis koko yhteisön arjen käytännöistä, roolikohtaisista vastuista ja yhteisistä toimintatavoista (Ojala, Sipola & Saharinen, 2025).

3. Aineisto ja metodit

Tutkimuksen aineisto kerättiin keväällä 2024 kolmessa ammatillisessa oppilaitoksessa, joista yksi oli ammatillinen erityisoppilaitos. Oppilaitokset toimivat useilla paikkakunnilla eri puolilla Suomea. Jokaisen osallistuneen oppilaitoksen rehtori tai vararehtori valitsi oman organisaationsa haastateltavat. Pyysimme kuitenkin, että pääsisimme haastattelemaan digitaalisuuden kannalta monenlaisia oppilaitosrooleja. Kysyimme tutkimusluvan jokaiselta haastateltavalta erikseen ja lisäksi tiedotimme, ettei kieltäytymisestä seuraa mitään, eivätkä esimiehet tule tietämään osallistumiseen kieltäytymisestä.

Haastatteluihin osallistui yhteensä 27 henkilöä, jotka edustivat monipuolisesti oppilaitosten henkilöstöä: opettajia ja erityisopettajia, opinto-ohjaajia, opintohallinnon työntekijöitä, digipedagogisia tukihenkilöitä, tietosuojavastaavia, tietohallinnon asiantuntijoita sekä oppilaitosjohtoa. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina (Amis, 2005; Ruslin ym., 2022), mikä mahdollisti sekä vertailtavuuden eri osallistujien välillä että joustavuuden seurata esiin nousevia teemoja. Haastattelujen kesto oli keskimäärin hieman yli 50 minuuttia. Yksi haastattelu toteutettiin kolmen hengen ryhmähaastatteluna, muut yksilöhaastatteluina.

Haastattelujen ohella kerättiin havainnointimuistiinpanoja oppilaitosten arjesta. Havainnointi kohdistui muun muassa opetustilanteisiin, johtamisen käytäntöihin ja tietohallinnon toimintaan. Havainnointia ei ollut mahdollista toteuttaa alkuperäisen suunnitelman mukaisesti päiviä kestävänä osallistuvana havainnointina, mutta kertynyt aineisto toi silti arvokasta kontekstuaalista tietoa haastattelujen tueksi.

Aineisto litteroitiin kauttaaltaan. Aineistoa analysoitiin kunkin artikkelin tutkimuskysymyksiin vastattaessa induktiivisella temaattisella analyysilla (Thomas, 2006; Braun & Clarke, 2006), joka on joustava mutta systemaattinen lähestymistapa merkitysten ja toistuvien teemojen tunnistamiseen. Luotettavuuden varmistamisessa noudatettiin Nowellin ja kumppaneiden (2017) esittämiä periaatteita, kuten analyysin vaiheiden läpinäkyvää dokumentointia ja koodaustulosten vertailua tutkijoiden kesken. Analyysissa etsittiin toistuvia teemoja ja merkityksiä, jotka liittyivät kyberturvallisuusosaamiseen, sen kehittämiseen ja arjen toimintatapoihin. Tulkinnassa hyödynnettiin organisaation oppimisen teorioita, erityisesti single-loop ja double-loop learning -lähestymistapaa (Argyris & Schön, 1978; Argyris, 1982; 1990; 1999), käytettävyyden ja turvallisuuden tasapainon viitekehystä (Kainda ym. 2010) sekä tilannetietoisuuden ja turvallisuuspoikkeamiin reagoimisen malleja (Endsley, 1995; Ahmad ym., 2021). Lisäksi sovellettiin Vygotskyn (1978) lähikehityksen vyöhykkeen käsitettä aikuisoppimiseen ja vertaisoppimiseen, mikä auttoi ymmärtämään, miten henkilöstö oppii ja ratkaisee ongelmia yhdessä.

4. Keskeiset tulokset

Tutkimuksen tulokset vastaavat hankkeen tavoitteisiin kolmen toisiaan täydentävän tutkimusartikkelin sekä ammatilliselle yleisölle kohdistuvien artikkelien kautta.

Näistä muodostuu neljä keskeistä tuloskokonaisuutta:

- henkilöstön kyberturvallisuusosaaminen ja oppiminen
- poikkeamien havaitseminen ja niistä raportointi
- käytettävyyden ja turvallisuuden välinen jännite sekä
- oppilaitosten kyberturvallisuuden yhteiskunnallinen merkitys.

Näiden teemojen tarkastelu tarjoaa sekä yksityiskohtaista tietoa oppilaitosten arjen turvallisuuskäytännöistä että laajempia näkökulmia siihen, miten kyberturvallisuutta voidaan kehittää työsuojelun ja koko suomalaisen työelämän jatkuvuuden näkökulmasta.

4.1 Henkilöstön kyberturvallisuusosaaminen ja oppiminen

Tutkimus osoitti, että kyberturvallisuusosaaminen vaihtelee merkittävästi eri henkilöstöryhmien välillä. Kuten luonnollista on, teknisiin rooleihin kuuluvilla henkilöillä oli yleensä syvällisempää tietämystä, kun taas opetuksen ja hallinnon tehtävissä osaaminen perustui usein arjessa vastaan tulleisiin kokemuksiin ja organisaation sisäisiin ohjeisiin. Koulutukset koettiin tärkeiksi, mutta niiden sisältö oli usein liian yleisluonteista eikä vastannut riittävästi työroolien erityistarpeisiin. Toisaalta koulutuksiin tai tietoiskuihin ei otettu välttämättä osaa, jollei ollut pakko. Tämä havainto tukee Argyrisin ja Schönin (1978) organisaation oppimisen mallia. Sen mukaan pelkkä yksikehäinen oppiminen, jossa toiminta mukautetaan vastaamaan annettuja sääntöjä ja ohjeita, ei riitä. Lisäksi tarvitaan kaksikehäistä oppimista, jossa kyseenalaistetaan ja uudistetaan itse toimintaperiaatteita ja taustalla olevia oletuksia. Silloin oppiminen on syvempää.

Epävirallinen vertaisoppiminen ja kollegiaalinen tuki nousivat tärkeäksi osaamisen kehittämisen muodoksi, vaikka sen hyödyntäminen oli osin satunnaista. Tilanteissa, joissa oma osaaminen ei riittänyt, työntekijät turvautuivat usein kokeneempien kollegojen apuun. Tämä tukee Vygotskyn (1978) lähikehityksen vyöhykkeen käsitettä, jossa oppiminen tapahtuu yhteistyössä muiden kanssa. Työsuojelun näkökulmasta tällainen vertaisoppiminen on olennainen osa työyhteisön resilienssiä: työntekijät kokevat turvaa siitä, että epävarmassa tilanteessa voi tukeutua kollegoihin. (Ojala, Sipola & Saharinen, painossa). Samoin työsuojelun näkökul-

Vertaisoppiminen on olennainen osa työyhteisön resilienssiä: työntekijät kokevat turvaa siitä, että epävarmassa tilanteessa voi tukeutua kollegoihin.

masta on merkittävää, että osaamisen puutteet eivät ilmene vain teknisinä virheinä, vaan myös epävarmuutena ja psyykkisenä kuormituksena. Kun työntekijä ei ole varma, kuinka hänen tulee toimia esimerkiksi poikkeamatilanteessa, kokemus työn hallinnasta voi heiketä ja turvattomuuden tunne kasvaa.

4.2 Poikkeamien havaitseminen ja niistä raportointi

Poikkeamailmoitusten tulkitsemisen ja ilmoittamisen käytännöissä havaittiin, että henkilöstö raportoi epäillyistä tietoturvapoikkeamista useilla eri tavoilla ja eri tahoille, mikä muodosti nelitasoisen eskalaatiopolun. Ensisijaisesti oppilaitoksissa käännyttiin lähimmän kollegan tai esihenkilön puoleen, tämän jälkeen oppilaitoksen IT-tuen, sitten digipalveluista vastaavan johdon ja lopulta tarvittaessa ulkopuolisten toimijoiden, kuten palveluntarjoajien tai viranomaisten, puoleen. Eskalaatiopolku heijastaa Endsleyn (1995) mallin mukaista tilannetietoisuuden rakentumista vaiheittain sekä Ahmadin ja kumppaneiden (2021) SA-CIR-mallin mukaista organisoitua tiedon ja vastuun siirtymistä roolitasolta toiselle. Prosessien selkeys vaihteli oppilaitoksittain.

Nostimme esiin Endsleyn (1995) tilannetietoisuuden mallin ensimmäisten tasojen, eli havainnoinnin ja siihen liittyvän ymmärryksen merkitystä poikkeamatilanteiden hallinnassa. **Oppilaitoksen opettajille tai vaikkapa opintosihteereille ei ole tärkeää osata ratkaista poikkeamaa itse. Tärkeämpää on ymmärtää milloin kohtaa sellaisen poikkeaman, josta on syytä ilmoittaa eteenpäin oppilaitoksen tietohallinnolle.**

Poikkeamatilanteiden raportointikanavina käytettiin pääasiassa sähköpostia ja puhelinta, mutta myös pikaviestimiä ja tikettijärjestelmiä. Kanavavalintaan vaikutti sekä tapahtuman kiireellisyys että henkilön oma tottumus. Erityisesti nopeaa reagointia vaativissa tilanteissa osa työntekijöistä tukeutui epävirallisiin kanaviin, mikä voi heikentää tapahtumien dokumentointia ja jatkokäsittelyä. Tämä ilmiö liittyy SA-CIR-malliin (Ahmadin ym., 2021), joka painottaa tiedon oikea-aikaisuutta ja standardoitua dokumentointia osana organisaation kyberturvallisuuden kypsyystasoa. Toisaalta löydös osoittaa, että työntekijät tarvitsevat tukea myös analysoidessaan, onko kyseessä sellainen poikkeama, josta tulee raportoida.

4.3 Käytettävyyden ja turvallisuuden välinen jännite

Käytettävyyden ja turvallisuuden välinen jännite oli havaittavissa tavalla tai toisella kaikissa tutkituissa organisaatioissa, mikä ei sinällään ole tutkimustuloksena työpaikoissa yllättävä (ks. esim. Agboola ym., 2024; Lennartsson ym., 2021). Monimutkaiset järjestelmät ja hankalakäyttöiset prosessit saattoivat johtaa siihen, että syntyi vähintäänkin houkutus kiertää tietoturvakäytäntöjä työn sujuvoittamiseksi. Joissain tilanteissa turvallisuuskäytäntöjen kiertäminen oli ikään kuin pakollista, koska järjestelmä ei mahdollistanut työtehtävän suorittamista ilman itsenäistä soveltamista. Tämä huomio tukee Normanin (2005) aiempaa tutkimusta siitä, että järjestelmiä tulisi suunnitella käyttäjien toiminnasta lähtien. Kaindan ja kumppanien (2010) mukaan hyvä käytettävyys on edellytys sille, että turvallisuuskäytäntöjä noudatetaan johdonmukaisesti.

Haastatteluissa nousi esiin myös kokemuksia siitä, että huonosti suunnitellut järjestelmät lisäsivät työn kuormittavuutta ja epävarmuutta. Kun turvallisuutta edistävät käytännöt koettiin työtä vaikeuttaviksi, ne eivät juurtuneet osaksi arkea. Vastaavasti järjestelmät, jotka olivat helppokäyttöisiä ja selkeitä, tukivat työntekijöiden sitoutumista turvallisuuskäytäntöihin. Työsuojelun näkökulmasta tämä jännite korostaa sitä, että tekniset ratkaisut eivät saa lisätä työn psykososiaalista kuormitusta, vaan niiden tulee vahvistaa työn hallittavuutta ja työntekijöiden turvallisuuden tunnetta. Tämä ei ole alati kehittyvässä digitaalisessa työympäristössä välttämättä ihan triviaali asia, kuten aiemmat tutkimukset osoittavat (ks. Alanko-Turunen ym., 2024; Agboola ym., 2024; Lennartsson ym., 2021).

Koska ammatilliset oppilaitokset toimivat tiiviissä yhteistyössä työelämän kanssa ja opiskelijat käsittelevät työpaikoilla opiskeltavan alan mukaan myös aitoja asiakastietoja sekä käyttävät alan järjestelmiä, on oppilaitosten kyberturvallisuuskäytännöillä suora yhteys työelämän ja jopa kriittisten alojen turvallisuuteen. Tämä laajentaa kyberturvallisuusvastuuta oppilaitosympäristöstä yhteiskunnan muihin keskeisiin toimintoihin.

Järjestelmät, jotka olivat helppokäyttöisiä ja selkeitä, tukivat työntekijöiden sitoutumista turvallisuuskäytäntöihin.

4.4 Oppilaitosten kyberturvallisuus yhteiskunnallisena kysymyksenä

Ammatillisten oppilaitosten kyberturvallisuus ei rajoitu yksittäisten organisaatioiden sisäisiin käytäntöihin, vaan sillä on laajempia yhteiskunnallisia ulottuvuuksia. Oppilaitokset kouluttavat tulevia ammattilaisia aloille, joilla käsitellään arkaluonteisia tietoja ja ylläpidetään yhteiskunnan keskeisiä toimintoja, kuten sosiaali- ja terveydenhuoltoa, logistiikkaa ja tietotekniikkaa. Kun opiskelijat käyttävät opintojensa aikana aitoja työelämän järjestelmiä ja kohtaavat tietosuojaan liittyviä kysymyksiä, he sisäistävät samalla sen, miten turvallisuus ymmärretään ja toteutetaan osana työyhteisön arkea.

Oppilaitosten henkilöstön toimintamallit ja asenteet muovaavat suoraan opiskelijoiden käsityksiä turvallisesta ja vastuullisesta työstä. Kyberturvallisuudesta tulee näin myös pedagoginen kysymys. Henkilöstön arjen ratkaisut, kuten poikkeamien raportointikäytännöt, salasanojen hallinta ja digitaalisten työkalujen käyttö (ks. esim. Sipola, 2025; Ojala, Sipola & Saharinen, 2025) parantavat toisaalta oppilaitoksen omaa turvallisuutta, mutta luovat myös sen toimintakulttuurin, josta opiskelijat ponnistavat osaksi työelämää. Jos esimerkiksi turvallisuutta pidetään työn sujuvuuden esteenä, sama ajattelu voi siirtyä opiskelijoille ja sitä kautta tulevaisuuden työpaikoille. Jos taas turvallisuus on luonteva osa työn tekemistä, siitä tulee osa myös työelämän arkea. Kyberturvallisuuden kehittämistä voidaan näin pitää investointina koko suomalaisen työelämän työturvallisuuteen ja jatkuvuuteen.

Jos turvallisuus on luonteva osa työn tekemistä, siitä tulee osa myös työelämän arkea.

5. Johtopäätökset

Hankkeen tulokset osoittavat, että ammatillisten oppilaitosten kyberturvallisuus on monitasoinen ilmiö, jossa tekniset ratkaisut, ihmisten toiminta ja organisaation rakenteet kytkeytyvät toisiinsa. Osaamisen ja toimintatapojen kehittäminen vaatii yhtä aikaa strategista, organisatorista ja yksilötason kehittämistä. Kehittämisen vastuun tulee olla oppilaitoksen johdolla. Työroolikohtainen ja käytännönläheinen koulutus on tutkimuksen mukaan keskeinen kehittämiskohde. Nykyiset yleisluontoiset koulutusmallit tukevat lähinnä Argyrisin ja Schönin (1978) kuvaamaa yksikehäistä oppimista, jossa käyttäjät oppivat noudattamaan olemassa olevia sääntöjä. Kyberturvallisuuden kestävä kehittäminen kuitenkin edellyttää kaksikehäistä oppimista, jossa organisaation toimintaperiaatteita ja käytäntöjä arvioidaan kriittisesti ja sisäistetään omaan työrooliin sopien. Tämä tarkoittaa esimerkiksi sitä, että esimerkiksi poikkeamien käsittelyprosessit tai salasanojen hallintakäytännöt eivät ole vain ohjeita, vaan niitä tarkastellaan säännöllisesti suhteessa kullekin ajalle ominaisiin uhkiin, omaan työrooliin, talon sisäisiin ja ulkoisiin yhteistyökumppaneihin, salattavaan ja turvattavaan tietoon ja järjestelmiin, sekä työpaikan prosesseihin.

Lisäksi tutkimuksessa todettiin, että poikkeamien havainnoimiseen ja ilmoittamiseen liittyvien prosessien selkeys ja toimivuus myös työajan ulkopuolella on olennainen osa organisaation resilienssiä. Havainto poikkeamasta syntyy usein lähellä käyttäjää, mutta sen varmentaminen ja eskalointi etenee vaiheittain (Endsley, 1995; Ahmad ym., 2021), ja prosessien aukot esimerkiksi toimistotyöaikojen ulkopuolella tarjottavassa tuessa heikentävät kykyä reagoida nopeasti ja tehokkaasti. Tutkimuksessa näkynyt epävirallisen vertaisoppimisen merkitys oli omiaan kasvattamaan myös organisaatioiden kyberturvallisuus-resilienssiä. Kun työntekijä saa kollegaltaan tukea tilanteissa, joissa oma osaaminen ei vielä riitä, kynnys toimia epävarmassa tilanteessa madaltuu ja samalla organisaation tilannetietoisuus vahvistuu (vrt. Vygotsky, 1978). Jotta tämä voimavara ei jäisi sattumanvaraiseksi, vertaisoppimista kannattaa edistää esimerkiksi mentorointiohjelmien tai sisäisten vertaisverkostojen avulla.

Ammatillisten oppilaitosten kyberturvallisuus on monitasoinen ilmiö, jossa tekniset ratkaisut, ihmisten toiminta ja organisaation rakenteet kytkeytyvät toisiinsa.

On syytä huomioida myös käytettävyyden ja turvallisuuden välinen tasapaino, joka on ratkaiseva tekijä turvallisen työkulttuurin juurruttamisessa. Helppokäyttöiset järjestelmät tukevat turvallisuuskäytäntöjen noudattamista, kun taas monimutkaiset tai huonosti suunnitellut ratkaisut altistavat sääntöjen kiertämiselle (Kainda ym., 2010). Tämän vuoksi tietoturvapäätöksissä on huomioitava myös käyttäjäkokemus, ei vain tekniset vaatimukset.

Tutkimuksesta voi huomata, että ammatillisten oppilaitosten kyberturvallisuudella on suora vaikutus suomalaisen työelämän turvallisuuteen. Oppilaitokset kouluttavat osaajia aloille, joilla käsitellään kriittistä tietoa ja ylläpidetään yhteiskunnan keskeisiä toimintoja. Kyberturvallisuusosaaminen, joka on juurrutettu jo opintojen aikana ja vahvistettu työelämäyhteistyössä, vähentää riskejä myös niissä organisaatioissa, joihin opiskelijat sijoittuvat työssäoppimisen tai valmistumisen jälkeen. Kaiken kaikkiaan hanke osoittaa, että kyberturvallisuuden kehittämistä ei voida nähdä pelkkänä teknisenä kysymyksenä. Se on osa laajempaa työturvallisuuskulttuuria, joka edellyttää johdon sitoutumista, selkeitä prosesseja, jatkuvaa oppimista ja sen tukemista sekä käyttäjälähtöistä järjestelmäsuunnittelua. Näiden tekijöiden systemaattinen kehittäminen luo oppilaitoksille ja työelämälle paremmat edellytykset ehkäistä, havaita ja hallita kyberturvallisuuspoikkeamia sekä palautua niistä nopeasti ja hallitusti.

Ammatillisten oppilaitosten kyberturvallisuudella on suora vaikutus suomalaisen työelämän turvallisuuteen.

Lähteet

Adams, A. & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42 (12), 40–46. https://doi.org/10.1145/322796.322806.

Agboola, T. O., Adegede, J. & Jacob, J. G. (2024). Balancing usability and security in secure system design: A comprehensive study on principles, implementation, and impact on usability. International Journal of Computing Sciences Research, 8, 2995–3009.

Agyris, C. (1999). On organizational learning (2. painos). Blackwell Publishing.

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939–953.

Alanko-Turunen, M., Heinilä, H. & Vainio, V. (2024). Digitalisoituvien käytänteiden kehittäminen ammatillisessa koulutuksessa – digitalisaatiota ja tunteita yhteensovittamassa. eSignals Research, 5(1). http://urn.fi/URN:NBN:fi-fe202402055586.

Amis, J. (2005). Interviewing for case study research, teoksessa Andrews, D. L., Mason D. S. and Silk M. L. (toim.), Qualitative methods in sports studies. Berg, 104 –138.

Argyris, C. (1982). Reasoning, learning and action: Individual and organizational. Jossey-Bass.

Argyris, C. (1990). Overcoming organizational defenses: Facilitating organizational learning. Prentice Hall.

Argyris, C. & Schon, D. (1978). Organizational learning: A theory of action perspective. Addison-Wesley.

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77–101.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643–1669.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. Human factors, 37(1), 32–64. https://doi.org/10.1518/001872095779049543.

Euroopan parlamentin ja neuvoston direktiivi 2022/2555 verkko- ja tietojärjestelmien turvallisuudesta. Haettu 25.6.2025 osoitteesta: https://eur-lex.europa.eu/legal-content/fi/LSU/?uri=oj:JOL_2022_333_R_0002.

Ferm, L. (2021). Vocational Students' Ways of Handling the Academic/Vocational Divide. International Journal for Research in Vocational Education and Training, 8 (1). https://doi.org/10.13152/ijrvet.8.1.1.

Force, J. T. (2018). Risk management framework for information systems and organizations. NIST Special Publication 800–37. National Institute of Standards and Technology.

Kainda, R., Flechais, I. & Roscoe, A. W. (2010). Security and usability: Analysis and evaluation. Proceedings of the 2010 International Conference on Availability, Reliability and Security, 275–282.

Lennartsson, M., Kävrestad, J. & Nohlberg, M. (2021). Exploring the meaning of usable security – A literature review. Information & Computer Security, 29(4), 647–663. https://doi.org/10.1108/ICS-10-2020-0167.

NIST (2024). The NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. Haettu 25.6.2025 osoitteesta https://doi.org/10.6028/NIST.CSWP.29

NIST (2025a). Asset. NIST Computer Security Resource Center Glossary. Haettu 25.6.2025 osoitteesta https://csrc.nist.gov/glossary/term/asset

NIST (2025b). Incident. NIST Computer Security Resource Center Glossary. Haettu 25.6.2025 osoitteesta https://csrc.nist.gov/glossary/term/incident

Norman, D. A. (2005) The Design of Everyday Things. Revised edition. Basic Books.

Nowell, L. S., Norris, J. M., White, D. E. & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International journal of qualitative methods, 16(1). https://doi.org/10.1177/1609406917733847.

Ojala, A-L., Sipola, T. & Saharinen, K. (2025). Miten jokainen oppilaitoksen työntekijä voi vahvistaa kyberturvallisuutta? Jamk Arena Public. https://urn.fi/urn:nbn:fi:jamk-issn-2984-0791-226.

Przymus, Z., Małagocka, K., & Przybyszewski, K. (2024). The human factor in cybersecurity: from risk profiles to resilience. Procedia Computer Science, 246, 1437–1445.

Ruslin, R., Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). Semi-structured Interview: A methodological reflection on the development of a qualitative research instrument in educational studies. IOSR Journal of Research & Method in Education, 12(1), 22–29.

Sipola, T. (2025). Salasanojen hallinta on yhä ajankohtaista oppilaitoksissa. Jamk Arena Pro. https://urn.fi/urn:nbn:fi:jamk-issn-2984-0783-171.

Suomen kyberturvallisuusstrategia 2024–2035. Valtioneuvoston kanslian julkaisuja 2024:11. Valtioneuvoston kanslia. http://urn.fi/URN:ISBN:978-952-383-376-0.

Thavi, R., Jhaveri, R., Narwane, V., Gardas, B., & Jafari Navimipour, N. (2024). Role of cloud computing technology in the education sector. Journal of Engineering, Design and Technology, 22(1), 182–213.

Thomas, D.R. (2006). A general inductive approach for analysing qualitative evaluation data. American Journal of Evaluation, 27(2), 237–246.

Ulven, J. B. & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.

Vygotsky, L.S. (1978). Mind in society: the development of higher psychological processes. Harvard University Press.

jamk | Jyväskylän ammattikorkeakoulu

Työsuojelurahasto
Arbetarskyddsfonden
The Finnish Work Environment Fund