Opinnäytetyö (YAMK)

Tradenomi (YAMK), teknologiaosaamisen johtaminen

2026

Päivi Pajunen

Muutosjohtaminen kyberturvallisuuskulttuurin mahdollistajana

Ajatustavan muutos tiedostamisesta arjen toimintatavoiksi

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (YAMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tradenomi (YAMK), teknologiaosaamisen johtaminen

2026 | 80 sivua

Päivi Pajunen

Muutosjohtaminen kyberturvallisuuskulttuurin mahdollistajana

Ajatustavan muutos tiedostamisesta arjen toimintatavoiksi

Tämän opinnäytetyön tavoitteena oli tarkastella kyberturvallisuuskulttuuria ja selvittää, voidaanko sitä muutosjohtamisen menetelmillä vahvistaa siten, että myös yksilöiden ajatusmallit ja sitä kautta arjen toimintatavat muuttuvat kyberturvallisemmiksi. Työ tehtiin, koska vaikka tutkimuksissa kyberturvallisuuskulttuurin merkitys on tunnistettu, sen käytännön johtamista ja arkeen juurtumista on tutkittu vähän. Tutkimus syntyi toimeksiantajan tarpeesta.

Opinnäytetyö toteutettiin kvalitatiivisena tutkimuksena. Teoreettinen viitekehys muodostui kyberturvallisuuden, organisaatiokulttuurin sekä muutosjohtamisen keskeisistä teorioista. Empiirinen aineisto kerättiin puolistrukturoiduilla asiantuntijahaastatteluilla eri toimialoilta.

Tulosten perusteella kybertuvallisuuskulttuurin vahvistamisessa keskeisiä tekijöitä ovat johdon sitoutuminen, yhteisön myönteinen asenneilmapiiri, toimivat prosessit sekä motivaatio ja osaaminen. Turvallisuus nähdään liiketoimintaa mahdollistavana tekijänä. Tutkimuksen pohjalta muutosjohtamisen malli ja kyberturvallisuustietoisuuden malli sovellettiin yhteen käytännönläheiseksi kokonaisuudeksi. Muutosjohtamisen ihmislähtöiset menetelmät voivat kasvattaa tietoisuuden kyberturvallisuuskulttuuriksi.

Asiasanat:

Muutosjohtaminen, kyberturvallisuus, organisaatiokulttuuri, tietoisuus, osaaminen, organisaatiokulttuurin muutos

Master’s Thesis | Abstract

Turku University of Applied Sciences

Master of Business Administration, Technological Competence Management

2026 | 80 pages

Päivi Pajunen

Change Management as an Enabler of Cybersecurity Culture

Transforming Awareness into Everyday Activities

The aim of this thesis was to examine cybersecurity culture and to assess whether it can be strengthened through change management methods so that individuals’ mindsets and everyday practices become more cybersecure. Although the importance of cybersecurity culture is recognized, its practical leadership and integration into daily work have not received so much research attention. This study was conducted based on commissioner needs.

The thesis was carried out as a qualitative study. The theoretical framework was based on key theories of cybersecurity, organizational culture, and change management. The empirical data was collected through semi-structured expert interviews across multiple industries.

The results indicate that management commitment, a positive organizational climate, effective processes, and individual motivation and competence are core to strengthening cybersecurity culture. Security is seen as a business enabler. Based on the study, a change management model and a cybersecurity awareness program were integrated into a practical, applied framework. The people-driven change management methods can grow awareness into cybersecure culture.

Keywords:

Change management, cybersecurity, organizational culture, awareness, knowledge, organizational culture change

Sisältö

Liitteet

Kuvat

Taulukot

Käytetyt lyhenteet

ADKAR	Prosci-yrityksen perustaja Jeffrey M. Hiattin esittelemä muutosjohtamisen malli. Proscin tekemän tutkimuksen pohjalta on tunnistettu, että muutos onnistuu, kun se tapahtuu yksilötasolla. (Prosci, 2025.)
ENISA	Euroopan unionin kyberturvallisuusvirasto ENISA (European Union Agency for Cybersecurity) edistää Euroopan kyberpolitiikkaa ja tukee maita valmistautumaan kyberturvallisuuden haasteisiin (ENISA, 2025).
IEC	International Electrotechnical Commission (IEC) on kansainvälinen sähköalan standardoija. IEC keskittyy varmistamaan, että sähkölaitteet ovat kansainvälisesti yhteensopivia ja turvallisia. (IEC, 2026.)
ISO	International Organization of Standardization (ISO) on kansainvälinen voittoa tavoittelematon standardointijärjestö. Järjestön tavoitteena on yhtenäistää toimintatapoja ja laadunhallintaa eri teollisuuden aloilla. (ISO, 2026.)
ISO/IEC	ISO ja IEC julkaisevat yhteisiä tietotekniikan ja tietoturvan kansainvälisiä standardeja (ISO/IEC 27001, 2022).
SANS	SANS Institute on kansainvälinen kyberturvallisuuskoulutuksia ja -sertifiointeja tarjoava yritys. Organisaation tavoitteena on tukea nykyisiä ja tulevia kyberturvallisuuden harjoittajia käytännön taidoilla ja tiedoilla. (SANS, 2026).

1 Johdanto

Maailma on teknologisessa murroksessa, ja uhkakuvat värittävät jokapäiväistä elämäämme. Poliittisessa tilanteessa on epävakauksia sotien ja talouden epävarmuuden muodossa. Teknologiat, laitteet ja järjestelmät kehittyvät valtavaa vauhtia ja kaikki tämä heijastuu turvallisuudentunteen muutoksina yksittäisen ihmisen arkeen. Tekoälyn hyödyntämisen räjähdysmäinen laajeneminen ja organisaatioiden työntekijöitä teknisesti aktivoivat hankkeet, vaativat yksilöltä laajempaa ja valveutuneempaa ymmärrystä myös tietoturvasta. Ideaalitilanteessa tietoturvaratkaisut olisivat niin tehokkaita, että käyttäjiltä ei tarvittaisi valveutuneisuutta lainkaan. Tämän hetken tilanne kuitenkin on se, että kyberturvallisuuden toteutuneista uhista jopa 70 % (Verizon, 2024) on ihmisen toiminnasta johtuvaa. Da Veiga ym. (2020) nostaa esiin useita tutkimuksia, joissa löydökset ovat osoittaneet työntekijöiden käyttäytymisen olleen suurin tekijä kyberturvallisuuden uhkien toteutumisessa. Tietoisuus, arvot, asenteet, motivaatio ja henkilön persoonallisuus vaikuttavat tämän käyttäytymiseen (da Veiga ym., 2020).

Työntekijöiden tulee pystyä omaksumaan uutta kiihtyvällä tempolla, ja pystyä toimimaan niin töissä kuin vapaa-ajalla tietoturvallisesti. Mallit ja säännöt tukevat tietoturvallista työtä, mutta niiden merkitys vähenee, jos ohjeistus ei kohtaa ihmistä tai ihminen syystä tai toisesta ei noudata niitä. Silloin henkilöstön arvot, asenteet ja ajatusmallit kohti tietoturvaa, organisaation yleinen kulttuuri ja sen käsitteen laajentaminen kyberturvallisuuskulttuuriksi nousee avaintekijäksi.

1.1 Tutkimuksen taustaa

Kyberturvallisuus ja sitä tukeva kulttuuri on nuori, kehittyvä ala. Kyberturvallisuuden tutkimus on usein teknologialähtöistä ja vaikka ihmisen toiminnan vaikutus on tunnistettu, se kuitenkin jää tutkimuksissa toiselle sijalle hallintamallien, teknisten tietoturvaratkaisujen ja tietoisuuskoulutusten alle. Haukilehto (2024) tutkii laajasti väitöskirjassaan terveydenhuollon

kyberturvallisuutta ja esittelee sen hallintaa tukevan mallin. PAR-malli (policies, awareness, reporting) tunnistaa henkilöstön tietoisuuden kasvattamisen (awareness) kriittisenä osana kyberturvallisuutta. Hän tunnistaa kulttuurin vaikutuksen tähän, mutta tutkimus ei keskity siihen vaan kulttuuriset aspektit ja asioiden käytäntö tunnistetaan jatkotutkimuskohteena.

Onnistuneen kyberturvallisuuskulttuurin toteutumisesta tiedetään kovin vähän. Kyberturvallisuustietoisuuden lisääviä ohjelmia on kehitetty ja tutkittu (ENISA, 2023; AlHogail, 2015), mutta silti ohjelmien hyödyntäminen on usein haasteellista ja tämän takia harvassa organisaatiossa kyberturvallisuuskulttuuri todella on osa yrityksen organisaatiokulttuuria (Alshaikh, 2020). Alshaikh nostaa esiin tutkimuksia, joissa todetaan, että ohjelmat yksin eivät riitä, ne hyödyttävät vasta kun ne laajamittaisesti ovat käytössä arjessa. Tutkimuksessa analysoidaan ja tunnistetaan elementtejä, joita onnistuneesta kyberturvallisuuskulttuurista löytyy ja perustellaan myös niiden tarve. Tässäkin tutkimuksessa kuitenkin keskitytään kyberturvallisuuskulttuurin vahvistamisen elementteihin enemmän tietoisuuden näkökulmasta. Elementeiksi on tunnistettu mm. kyberturvallisuusverkoston luominen tai kyberturvallisuustiimin nimeäminen. Vaikka nämä ovatkin tärkeitä elementtejä, organisaatiokulttuuriin vaikuttaminen vaatii laajempaa näkökulmaa. Tutkimuksen ulkopuolelle jää myös käytännön tason toteutus, miten mallia ja elementtejä voidaan käytännön tasolla toteuttaa tavoitteiden saavuttamiseksi. Tämä tunnistetaan myös tutkimuksen jatkokehityskohteissa. (Alshaikh, 2020.)

Kyberturvallisuus on siis kulttuurillinen teema, jossa ihmisen toiminnalla on suuri rooli. On tunnistettu mitkä tekijät mahdollisesti vaikuttavat kulttuurin vahvistumiseen ja miksi. Epäselväksi jää kuitenkin se, miten tämä käytännön tasolla toteutetaan siten, että myös ajatusmallit muuttuvat kyberturvallisuuden huomioiviksi. Tällä työllä on toimeksiantaja. Toimeksiantaja haluaa tarkastella kyberturvallisuuskulttuurin toteutumista muutosjohtamisen näkökulmasta, voiko sen menetelmillä ja työkaluilla edesauttaa kulttuurin vahvistumista ajatusmallien näkökulmasta.

1.2 Työn rajaus ja tutkimuskysymykset

Tässä työssä keskitytään erityisesti ihmisen rooliin kyberturvallisuudessa, miten henkilöstön ajatusmallit ja toiminta voidaan muuntaa kyberturvatietoisuudeksi ja vielä pidemmälle, kyberturvallisen arjen teoiksi. Miten muutosjohtaminen keinoilla voidaan luoda ja johtaa kyberturvallisuuskulttuuria siten, että tiedon ja organisaation turvaaminen voidaan kääntää innostavaksi ja positiiviseksi mahdollisuudeksi. Miten varmistetaan, että ihmiset todella haluavat toimia tietoturvallisesti ja löytävät tarvitsemansa tiedon sen saavuttamiseksi. Tätä tarkastellaan myös siitä näkökulmasta, tuovatko toimialat eroavaisuuksia.

Tutkimusongelma: Voiko muutosjohtamisen ja sen käytännönläheiset työkalut olla työväline laajentaa olemassa oleva organisaatiokulttuuri kyberturvallisuuden huomioivaksi kulttuuriksi, jossa myös ajattelutavat muuttuvat kyberturvallisemmaksi?

Tukevat tutkimuskysymykset: Mitkä ovat keskeiset kulttuuriset haasteet ja menestystekijät kyberturvallisuuskulttuurin kehittämisessä?

Miten toimiala vaikuttaa kyberturvallisuuskulttuuriin?

Rajaus: Opinnäytetyön näkökulmana on muutosjohtamisen mallin soveltamisen kuvaaminen kyberturvallisuustietoisuuden ohjelmalle, teoreettisen viitekehyksen ja haastattelututkimuksen avulla.

Työssä ei rakenneta kyberturvallisuuskulttuurin luomiselle uutta mallia, vaan sidotaan jo olemassa oleva malli käytännön tasolle Proscin ADKAR-muutosjohtamisen (2025) menetelmien kautta. Tutkimuskysymykset auttavat mallin luonnissa ja siinä mihin erityisesti tulee keskittyä, jotta onnistutaan laajentamaan organisaatiokulttuuri kyberturvallisuuskulttuuriksi.

Hypoteesi: Tutkimuksen hypoteesi on, että vaikka kyberturvallisuustietoisuuden malleja on paljon, niiden käytännön soveltaminen on haasteellista, eikä niiden käyttöönotto takaa onnistunutta kyberturvallisuuskulttuuria. Johdon sitoutuminen, arjen prosessit ja ihmisten asenteet sekä pelot turvallisuutta

kohden estävät kyberturvallisuuskulttuurin toteutumisen. Toimialoittain on eroavaisuuksia, toisilla suhtautuminen sääntöihin ja niiden noudattamiseen on luontevampaa kuin toisilla. Muutosjohtamisen ihmislähtöisillä työkaluilla kyberturvallisuus voidaan tuoda lähelle yksilöä ja tämän arkea, ja ymmärryksen kautta juurruttaa kyberturvallisuus osaksi organisaatiokulttuuria, ihmisten arvoja ja ajatusmalleja.

2 Tutkimusmenetelmät ja aineiston hankinta

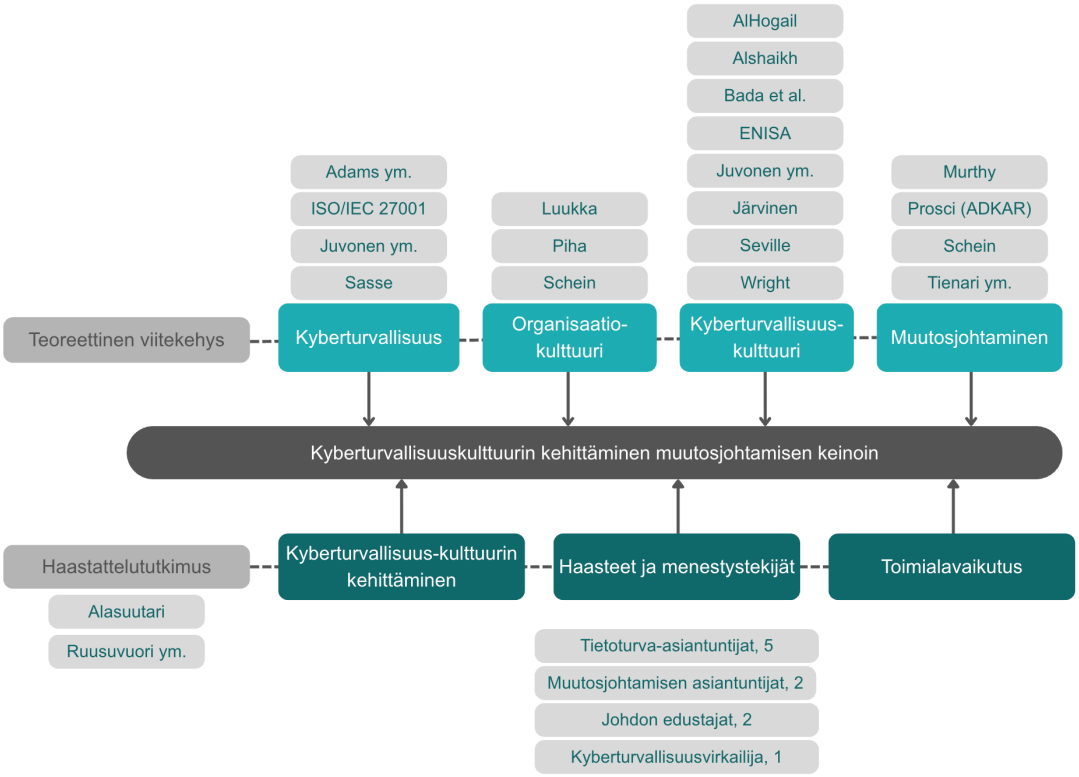
Opinnäytetyön tutkimusmenetelmäksi on valittu kvalitatiivinen tutkimusmenetelmä, eli laadullinen tutkimus. Kvalitatiivinen tutkimusmenetelmä pohjautuu laajaan tietomäärään, missä aineistoa pyritään ymmärtämään kokonaisuutena ja sen perusteella luomaan ratkaisuja tutkimuskysymyksiin (Alasuutari, 2011). Tässä työssä taustalla on teoreettinen tietopohja ja laadullisena tutkimusmenetelmänä haastattelututkimus.

Teoreettisen tietopohjan muodostavat kyberturvallisuuden, organisaatiokulttuurin kehittämisen sekä muutosjohtamisen olennaiset teemat.

- Informaatiotekniikan turvallisuus kuvaa turvallisuuden kokonaiskenttää ja kyberturvallisuuden paikkaa siinä.
- Organisaatiokulttuurin kohdalta on avattu olennaisimmat lainalaisuudet, mitkä sen kehittämiseen liittyvät.
- Kyberturvallisuuskulttuuri on organisaatiokulttuurin ilmentymä.
- Muutosjohtamisen tehtävä on toimia muutoksen ihmispuolen ajurina ja työvälineenä kyberturvallisuustietoisuuden laajentamiseksi kyberturvallisuuskulttuuriksi.

Lähteinä on käytetty kirjallisuutta ja vertaisarvioituja artikkeleita, sekä tunnustettuja alan malleja. Työn tietopohja on esitelty kuvassa 1.

Kvalitatiivinen tutkimus ja sen aineistot ovat tyypillisesti monitasoisia ja komplekseja (Alasuutari, 2011). Niin myös tämä aihepiiri ja tietopohja on laaja ja siksi haasteellinen. Haastattelututkimuksen tuomalla asiantuntijuusnäkökulmalla oli mahdollista tuottaa lopputulos, joka saattaa käytännön ja teorian yhteen.



Kuva 1. Työn tietoperusta

2.1 Haastattelututkimus

Asiantuntijahaastatteluissa korostuu asiantuntijan rooli jonkun ilmiökentän asiantuntijana, näin ollen heitä on vaikea korvata haastateltavana. Asiantuntijahaastattelulla kerätään erilaista tietoa liittyen prosesseihin, faktoihin, erilaisiin käytäntöihin ja analyysivaiheessa on hyvä muistaa, että tieto on subjektiivista ja voi näin ollen olla myös virheellistä tai ajan värittämää. (Ruusuvuori ym., 2010.)

Haastattelututkimus perustui tietoturva-asiantuntijoiden sekä muutosjohtamisen asiantuntijoiden puolistrukturoituihin haastatteluihin, sekä muutosjohtamisen asiantuntijoiden kohdalla myös ryhmähaastatteluun. Haastateltavat valittiin heidän pitkän kokemuksensa perusteella, he eivät edustaneet haastatteluissa yksittäistä organisaatiota vaan heitä haastateltiin heidän oman pitkän uransa tuoman asiantuntijuuden pohjalta.

2.2 Haastateltavat

Haastateltavista haluttiin tunnistaa erityisesti kolme ryhmää: johdon edustajat, tietoturvallisuuden asiantuntijat sekä muutosjohtamisen asiantuntijat. Haastateltavista kaksi oli johdon edustajia, toinen vahvemmin yksityisen ja toinen julkisen puolen edustaja, mutta kummallakin kokemusta laajasti molemmista niin Suomessa kuin kansainvälisesti. Tietoturva-asiantuntijoissa korostui laaja-alainen kokemus eri toimialoilta ja erilaisista organisaatioista aihepiirin ympäriltä. Muutosjohtamisen konsultit olivat senioritason osaajia sekä muutosjohtamisen, organisaatiokulttuurin että tietoturvakulttuurin alueelta.

Haastateltavia oli yhteensä 10, haastattelut pidettiin aikavälillä toukokuu – elokuu 2025. Haastattelujen edetessä oli tunnistettavaa, että työn sisällön kannalta lisähaastattelut eivät olisi tuoneet merkittävää lisäinformaatiota. Tässä kontekstissa ja kokoluokassa tarpeellinen määrä tietoa saavutettiin näillä haastatteluilla, ja samat tunnistettavat teemat alkoivat toistua ilman merkittäviä uusia muutoksia. Haastateltavat on esitelty liitteessä 2 haastattelujen roolin, erityisasiantuntijuuden ja toimialan kautta (Liite 2: Haastatellut, 2025).

2.3 Haastattelukysymykset ja analyysi

Haastattelun pohjakysymykset olivat valmiina sekä suomeksi että englanniksi, kysymykset on esitelty liitteessä 1 (Liite 1: Haastattelurungot, 2025). Haastattelutekniikkana käytettiin puolistrukturoitua mallia, joka mahdollistaa kysymysten puitteissa myös vapaata keskustelua. Näin haastattelun rakennetta voitiin muuttaa sen mukaisesti mihin asiantuntija vastauksillaan sitä vei. Vapaan keskustelun myötä päästiin myös paljon syvemmälle aitoihin kokemuksiin ja löydöksiin, keskustelu muuttui vapaamuotoisemmaksi luonnostaan. Aihepiirin sensitiivisyyden takia, ja mahdollisimman suorien sekä avoimien vastausten saamiseksi pitkästä työhistoriasta, suuri osa haastatteluista ja niiden dokumentoinnista on salassa pidettävää. Ensimmäisten haastattelupyyntöjen myötä tämä rajoitus osoittautui parhaaksi tavaksi saada haastatteluja sovittua. Haastattelut pidetiin Teamsin yli ja olivat jokainen kestoltaan noin tunnin.

Haastattelukysymykset jaoteltiin tutkimusongelman pohjalta kahteen pääosaan.

Tutkimusongelma*:* Voiko muutosjohtamisen ja sen käytännönläheiset työkalut olla työväline laajentaa olemassa oleva organisaatiokulttuuri kyberturvallisuuden huomioivaksi kulttuuriksi, jossa myös ajattelutavat muuttuvat kyberturvallisemmaksi?

Päätutkimuskysymyksenä halutaan tutkia, voiko muutosjohtaminen olla avain kyberturvallisuuskulttuurin vahvistamiselle, jossa myös ajattelutavat muuttuvat kyberturvallisemmiksi. Haastattelujen ensimmäisessä osiossa perehdyttiin kyberturvallisuuteen ja sitä tukevaan kulttuuriin. Asiantuntijoilta kysyttiin heidän kokemuksiaan ja mielipiteitään, miten he kokevat kyberturvallisuuden ja siihen liittyvän kulttuurin, ja mikä heidän mielestään tekee sen tunnistettavaksi. Muutosjohtajilta kysyttiin lisäksi organisaatiokulttuurin ja sen kehittämisen ympäriltä ja muutosjohtamisen roolista kehittämisessä.

Tukikysymykset*:* Mitkä ovat keskeiset kulttuuriset haasteet ja menestystekijät kyberturvallisuuskulttuurin kehittämisessä? Miten toimiala vaikuttaa kyberturvallisuuskulttuuriin?

Tutkimuksen tukikysymykset keskittyvät toimialanäkökulmaan, sekä kyberturvallisuuskulttuurin tunnistettaviin haasteisiin ja menestystekijöihin. Näitä asiantuntijoilta kysyttiin omien toimialakokemusten kautta. Mitä he itse ovat tunnistaneet eri toimialoilla, mitä itse pitävät kyberturvallisuuskulttuurin parhaina edistäjinä ja toisaalta pahimpina sudenkuoppina. Lisäksi perehdyttiin vielä asiantuntijan kokemuksiin organisaatioiden toteutuneista uhkatilanteista tai läheltä piti -tilanteista. Miten ne ovat vaikuttaneet organisaatioon ja mitä niistä on opittu, mitä mahdollisesti toiminnassa muutettu.

Haastattelujen löydökset dokumentoitiin Wordilla ja luokiteltiin datarakenteeseen Exceliin yhteisten teemojen tunnistamiseksi. Haastattelumateriaali analysoitiin sisältöanalyysin menetelmillä, eli koko dokumentaatio käytiin läpi järjestelmällisesti tutkimusongelman sekä keskeisten käsitteiden ja teemojen kautta (Ruusuvuori ym., 2010).

3 Teoreettinen viitekehys

3.1 Keskeiset käsitteet

Kyberturvallisuus määritellään tietoturvariskien hallinnaksi, kun tieto on digitaalisessa muodossa erilaisissa tallennusvälineissä, tietokoneissa ja verkossa. Tieto liikkuu kuitenkin eri toimijoiden välillä yli organisaatiorajojen, toimijat ovat vuorovaikutuksessa digitaalisesti verkkojen välityksellä ja fyysisesti. Toimijat ovat ihmisiä ja erilaisia digitaalisia järjestelmiä. Kyberturvallisuus näkyy voimakkaasti teknisissä kontrolleissa, mutta sen merkitys on jatkuvasti kasvava niin organisatoristen kuin henkilöstöönkin liittyvien kontrollien kautta kyberuhkien hallinnassa. Kyberturvallisuuden uhkien ilmentyminä henkilöstön näkökulmasta voidaan mainita huijausviestit ja tiedonkalastelu, käyttäjätunnusten väärinkäyttö ja tilien kaappaaminen, erilaiset haittaohjelmat tai suojaton toimiminen verkossa. Yhteistä näille tapahtumille on inhimillinen virhe, tahallaan harhaan johtaminen tai riittämättömät suojaukset. (ISO/IEC 27002, 2022.)

Organisaatiokulttuuri toistaa yrityksen ja sen työntekijöiden arvoja ja asenteita. Sen sanotaan olevan yrityksen kaikki, se mitä tapahtuu, kun kukaan ei katso. Hyvä organisaatiokulttuuri on aina sidottu yrityksen isoon kuvaan, yrityksen visioon ja tavoitteisiin. Kulttuuri on elementti, jota voi kehittää ja vahvistaa. (Luukka, 2019.)

Muutosjohtamisen malleja on useita, alkaen Lewinin 3-portaisesta jo 1947 julkaistusta mallista, Kotterin 8-portaiseen malliin (Tienari ym., 2012). Mallit syntyivät havainnosta, että muutos ei tapahdu itsestään. Muutos vaatii aktiivista työtä vanhojen tapojen murtamiseksi, uuden työskentelytavan omaksumiseksi ja juurruttamiseksi. Proscin tekemän tutkimuksen pohjalta tunnistettiin, että muutos onnistuu, kun muutos tapahtuu yksilötasolla. (Prosci, 2025.)

Kyberturvallisuuskulttuurilla tarkoitetaan kulttuuria, jossa turvallisuuden elementit on rakentuneet osaksi organisaatiokulttuuria. Ne ovat yrityksen

DNA:ssa. Kulttuurin pohja syntyy siitä, kun ihmiset ymmärtävät oman vastuunsa ja roolinsa turvallisuudessa. Kyberturvallisuustietoisuus ja sitä vahvistava kulttuuri syntyy jatkuvasta vuorovaikutuksesta, motivaation löytämisestä ja oikeanlaisen toiminnan tunnustamisesta. Johdon näkyvällä tuella, ja myös seurannalla vahvistetaan kyberturvallista kulttuuria. (Wright, 2019.)

3.2 Kyberturvallisuuskulttuuri tutkimuskohteena

Turvallisuus ja kyberturvallisuus ovat monitulkintaisia termejä. Laajemmassa kontekstissa turvallisuus voi olla valtiotasoista, missä tehtävänä on valtiotasolla varautua erilaisiin globaaleihinkin häiriötilanteisiin (VM, 2017). Turvallisuudesta voidaan puhua myös esimerkiksi puhuttaessa auton ihmistä turvaavista ratkaisuista kuten turvavyöstä. Kyberturvallisuus on osa informaatiotekniikan turvallisuutta (ISO 27002, 2022). Se kulttuurillisesti sitoutuu organisaation laajempaan kulttuuriin, organisaation tavoitteisiin, arvoihin ja asenteisiin. Myös Suomen valtiolla on kyberturvallisuusstrategia, jonka tavoitteena on määritellä keskeiset tavoitteet ja menetelmät, jolla valtion toimijat voivat hallita valtion kybertoimintaympäristöön kohdistuvia haittoja (VM, 2024).

Tässä työssä keskitytään informaatiotekniikan turvallisuuteen, ja erityisesti kyberturvallisuuteen.

3.2.1 Informaatiotekniikan turvallisuus ja kyberturvallisuus sen osana

International Organization of Standardization (ISO) on kansainvälinen voittoa tavoittelematon standardointijärjestö. Sen ylläpitämä, ISO 27001, on kansainvälisesti tunnustettu tietoturvallisuuden hallintamalli. Malli ohjaa organisaatioita huomioimaan turvallisuuden teknisissä ratkaisuissaan ja prosesseissaan. ISO 27001 -sertifiointi vahvistaa myös muille, että organisaatio on asianmukaisesti turvannut toimintansa. Standardin vie käytännön tasolle ISO 27002, joka kuvaa tietoturvastandardissa ISO 27001 tunnistetut kontrollit

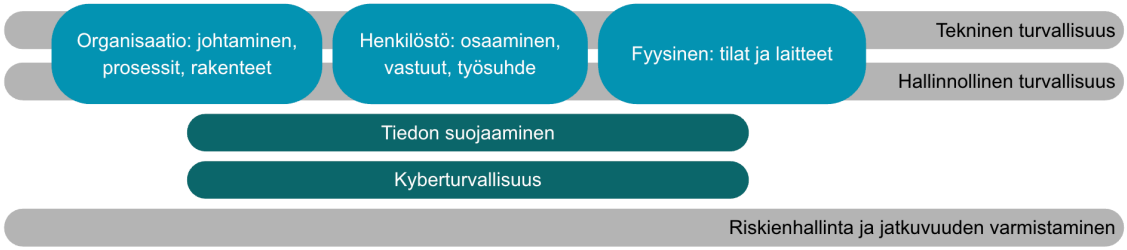
parhaiksi käytännöiksi. ISO 27002 mukaan keskeiset tieto- ja informaatiotekniikan turvallisuuden osa-alueet ovat (ISO/IEC 27002, 2022):

- Organisaatio: Johtaminen, politiikat, prosessit ja rakenteet.
- Henkilöstö: Ihmisiin liittyvät toimet, kuten koulutus, vastuut, sopimukset ja toimiminen työsuhteessa.
- Fyysinen: Toimitilat, pääsynvalvonta, laitteiden suojaus, siisteys.
- Tekniset: Pääsynhallinta, verkkojen suojaus, salaukset, valvonta.

Määritelmässä tieto sisältyy kaikkiin osa-alueisiin, tiedon ollessa eri tilanteissa eri muotoista: puheena, paperilla tai digitaalisessa muodossa. Kyberturvallisuus määritellään tietoturvariskien hallinnaksi, kun tieto on digitaalisessa muodossa erilaisissa tallennusvälineissä, tietokoneissa ja verkossa. Tieto liikkuu kuitenkin eri toimijoiden välillä yli organisaatiorajojen, toimijat ovat vuorovaikutuksessa niin digitaalisesti verkkojen välityksellä ja kuin fyysisestikin. Toimijat ovat ihmisiä ja erilaisia digitaalisia järjestelmiä. Kyberturvallisuus näkyy voimakkaasti teknisissä kontrolleissa, mutta sen merkitys on jatkuvasti kasvava niin organisatoristen kuin henkilöstöön liittyvienkin kontrollien kautta kyberuhkien hallinnassa (ISO/IEC 27002, 2022).

Informaatiotekniikan turvallisuuden osa-alueita ohjataan riskienhallintaprosessilla. Riski on tunnistettu poikkeama, jonka toteutumista prosessilla pyritään estämään, minimoimaan, tai sen realisoituessa tekemään tarvittavat toimenpiteet liiketoiminnan jatkuvuuden säilyttämiseksi. (Juvonen ym., 2023). Riskienhallintaprosessin käytännön ohjeita ja parhaita käytänteitä kuvaa ISO/IEC 27005, joka on tietoturvastandardin ISO 27001 tarkentava ohje. Turvallisuuden osa-alueita suojataan *teknisin ja hallinnollisin* keinoin. Tekninen turvallisuus luo suojausmenetelmät, hallinnollinen turvallisuus määrittelee säännöt ja ohjeet, joilla mahdollistetaan turvallinen toimiminen. Turvallisuutta hallitaan *riskienhallinnan ja jatkuvuuden varmistamisen* näkökulmasta, riskiperusteisesti todennäköisyyksiä hyödyntäen. (ISO/IEC 27002, 2022; ISO/IEC 27005, 2022.)

Kyberturvallisuus ISO:n määritelmässä tunnistetaan informaatiotekniikan turvallisuuden eri osa-alueita poikkileikkaavana teemana, linkittyneenä tiedon suojaamiseen. Informaatiotekniikan turvallisuuden osa-alueet on kuvattu kuvassa 2.



Kuva 2. Informaatiotekniikan turvallisuuden osa-alueet (mukaillen: ISO 27002, 2022)

Kyberturvallisuus on laajimmassa katsantokannassaan globaalia ja osa kokonaisturvallisuutta valtioiden strategioissa, kattaen myös valtiollisen puolustuksen, varautumisen ja suojautumisen. Suomen valtio uusi kyberturvallisuusstrategiansa vuonna 2024. Sitä ohjaa niin Euroopan digitavoitteet (EU, 2025), kuin maailmantilanteen murroksetkin. Suomen kyberturvallisuustavoitteet ovat kunnianhimoisia, mutta myös välttämättömiä kokonaisturvallisuuden näkökulmasta. Mallissa korostetaan, miten paras lopputulos saavutetaan julkisten ja yksityisten toimijoiden yhteistyöllä sekä yksilön kautta, kyberturvallisuus on kansalaistaito. Strategian tavoitteet keskittyvät neljään pääkohtaan: Osaamisen kehittyminen, varautumisen suunnittelu ja toteutus, yhteistoiminta, sekä toteutuneisiin uhkiin reagointi ja vastatoimet. (VM, 2024.)

Ihmiskeskeisen kyberturvallisuuden tutkijat Anne Adams ja Martina Angela Sasse (Adams & Sasse, 1999) esittivät raportissaan jo vuonna 1999, että turvallisuutta ei suunnitella käyttäjälähtöisesti, ihmistä ajatellen. He tunnistivat, että esimerkiksi salasanatekniikat ja -prosessit ovat monimutkaisia, eivätkä tuo käyttäjille tarvittavaa ymmärrystä tai motivaatiota toimia niiden mukaisesti. Sasse jatkoi uudemmassa tutkimuksessaan (Sasse, 2015), että ihmisen pakottaminen tai jopa käskeminen valitsemaan turvallinen tie ei auta. Ihmisen

perimmäinen motivaatio tulee tunnistaa ja hyödyntää sitä mahdollisimman kitkattomassa prosessissa. Esimerkkinä Sasse nostaa pankin tai verkko-ostokset, jossa tänä päivänä on jo huomioitu yksilön kyvyt ja tahtotila. Ihminen toimii motivaatioperusteisesti ja tekniikan tulee tukea tätä, ei päinvastoin. (Adams & Sasse, 1999; Sasse, 2015.)

3.2.2 Organisaatiokulttuuri ja sen kehittäminen

Panu Luukka (2019) kuvaa yrityksen kulttuuria yrityksen kaikeksi. ”Kulttuuri erottaa organisaation muista organisaatioista, se on yhdistelmä tiedostettuja ja tiedostamattomia arvoja, toimintatapoja ja rakenteita. Nämä yhdessä ohjaavat työntekijöiden ajattelua ja käyttäytymistä.” (Luukka, 2019.)

Kulttuuri on tunnistettava osa yritystä, se muuttuu hitaasti ja omaksutaan kun liitytään osaksi organisaatiota. Kulttuurin rakenne voidaan nähdä kolmiosaisena (Schein & Schein, 2017):

1. Ulospäin näkyvät ilmentymät: mitä kohtaat, kun tapaat kulttuurin edustuksen, vaatteet, tapa kohdata, kieli, ilmapiiri
2. Sisällä olevat arvot ja asenteet: ajan saatossa muodostuneet, sosiaalisesti yhdessä tunnistetut arvot ja asenteet, esimerkiksi laatuajattelu, myyntiasenne
3. Perusolettamukset, jotka otetaan itsestään selvyytenä: esimerkiksi tiimityö yksilön edun sijaan, avoimuus, rehellisyys

Organisaatiokulttuuri toistaa yrityksen ja sen työntekijöiden arvoja ja asenteita. Sen sanotaan olevan sitä mikä tapahtuu, kun kukaan ei katso. Hyvä organisaatiokulttuuri on aina sidottu yrityksen isoon kuvaan, yrityksen visioon ja tavoitteisiin (Luukka, 2019; Piha, 2017). Luukka kuvaa, että kulttuuri on elementti, jota voi kehittää ja vahvistaa. Piha nostaa esiin, että syyn tulee kuitenkin olla selvillä, miksi kulttuuria halutaan kehittää. Jos joku kulttuurissa estää tavoitteiden toteutumisen, silloin kulttuuria on katsottava uusin silmin. Organisaatiokulttuurilla tulee olla omistaja, joku, joka vaalii sen olemassaoloa ja sen henkilön tulee olla yrityksen toimitusjohtaja ja muu johto. Yrityksen koko

johto toimitusjohtajista esihenkilöihin toistaa yrityksen kulttuuria omana itsenään ja on näin vahva esimerkki koko organisaatiolle. (Luukka, 2019; Piha, 2017.)

Kun kulttuuria muutetaan, on ensimmäinen askel määrittää muutos: Mitä halutaan muuttaa ja miksi. Muutettaessa jotain kulttuurillista, todellisuudessa etsitään syytä, miksi joku ei-haluttu tapahtuma toteutuu, ja miten organisaation prosessien, toimintatapojen tai muun pitäisi muuttua, jotta niin ei tapahtuisi jatkossa. Organisaatiokulttuurin muuttaminen on pitkäjänteistä ja sitkeää työtä. Onnistunut muutos vaatii johtamista, strukturoitua ja fokusoitua muutosprosessia. (Piha, 2017; Schein & Schein, 2017.)

3.2.3 Kyberturvallisuuskulttuuri

Aiemmin kuvattiin, miten turvallisuutta luodaan riskejä hallitsemalla, estämällä, minimoimalla riskiä tai turvaamalla toteutuneen uhan jälkeen jatkuvuutta (Juvonen ym., 2023). Turvallisuudentunne syntyy luottamuksesta, että tiedetään ja tunnetaan riskit, ja uskotaan että ne ovat hallinnassa. Turvallisuudentunne on inhimillinen tuntemus. Kyberturvallisuuden uhat ovat kuitenkin usein tuntemattomia tai liian abstrakteja ymmärrettäväksi, ja sen korostaminen lisää jo sanan ”kyberuhka” tai vain ”kyber” pelkoa. Kyberuhista puhuttaessa mediassa jo kuvituksessa näyttäytyy huppupäinen hahmo, binäärilukuja, väritys on mustaa. Pelottelu on vallitseva tapa puhua. Pelon sijaan tulisi nostaa esiin mahdollisuuksia, arkipäiväistää uhat ja vahvistaa yksilön valppautta ja kykyä tunnistaa uhat. (Juvonen ym., 2023; Järvinen, 2025.)

Organisaatiokulttuuri on sitä mitä tapahtuu, kun kukaan ei katso (Luukka, 2019). Kyberturvallisuuskulttuurissa tämä korostuu. Jos joku aihe tuntuu pelottavalta tai hankalalta, ihmiset herkästi ohittavat sen, jopa toimivat ohjetta vasten. Kyberturvallisuuskulttuurilla tarkoitetaan kulttuuria, jossa turvallisuuden elementit on rakentuneet osaksi organisaatiokulttuuria. Kulttuurin pohja syntyy siitä, kun ihmiset ymmärtävät oman vastuunsa ja roolinsa turvallisuudessa. Kyberturvallisuustietoisuus ja sitä vahvistava kulttuuri syntyy jatkuvasta

toiminnasta, motivaation löytämisestä ja oikeanlaisen toiminnan tunnustamisesta. Johdon näkyvällä tuella, ja myös seurannalla vahvistetaan kulttuuria. Kyberturvallisuuskulttuuria johdetaan organisaatioissa kyberturvallisuustietoisuutena ja sen tasoa nostavilla ohjelmilla. Ohjelmat pohjautuvat tietoiskuihin, kampanjoihin ja koulutuksiin ja taustalla toimivaan hallinnolliseen tietoturvaan, joka luo säännöt ja ohjeistukset. (Luukka, 2019; Wright, 2019.)

Euroopan unionin kyberturvallisuusvirasto ENISA (European Union Agency for Cybersecurity) edistää Euroopan kyberpolitiikkaa ja tukee maita valmistautumaan kyberturvallisuuden haasteisiin. ENISA on luonut kyberturvallisuustietoisuuden ohjelmamallin yrityksille. Ohjelman materiaali on julkisesti saatavilla ja organisaatioiden hyödynnettävissä omiin tarkoituksiinsa. Ohjelma on yrityksen aloituspaketti, jolla kyberturvallisuustietoisuuden ohjelman voi omassa organisaatiossaan luoda ja käynnistää. Se sisältää ehdotuksen suunnitelmaksi, ja erilaisia kampanjoita ja tehtäviä hyödynnettäväksi. Ohjelma alkaa tavoitteiden, rahoituksen ja työryhmän valitsemisella, sekä johdon tuen varmistamisella. Kohderyhmäajattelun kautta tunnistetaan mitä erilaisia rooleja organisaatiossa on. Valitaan kohdennetusti oikeanlaiset toimenpiteet ja suunnitellaan käytännön toteutus. Ohjelma kehittyy arvioinnin myötä. Kyberturvallisuustietoisuuden ohjelma on luonteeltaan pitkäkestoinen. Kyberturvallisuustietoisuuden suunnittelu on esitelty kuvassa 3. (ENISA, 2023.)

Kuva 3. Kyberturvallisuustietoisuuden ohjelma (ENISA, 2023)

ENISAn mallin pohjalta, yrityksen kyberturvallisuustietoisuuden ohjelma voisi näyttää ylätasolla esimerkiksi tältä (ENISA, 2023):

1. Lisää tietoisuutta tietojenkalastuksesta: Koulutusta, informatiivista materiaalia esimerkein sekä edistymistä seuraava kysely. Sekä yleistä tietoutta, että kohdennettua viestintää ja koulutusta. Kohdennettu viestintä korostaa erityisesti roolikohtaisuutta, ja miten eri tavoin kyberturvallisuus eri rooleille näyttäytyy.
2. Nosta kyberturvallisuuskulttuuria ja -koulutusta: Kohdennettua koulutusta, häiriön ilmoitusprosessi, kokemusten kautta oppiminen. Hyvä taustaprosessit parantavat kyberturvallisuuskulttuuria.
3. Paranna valmiuskykyä: Häiriön käsittelyprosessin parantaminen, koulutusta ja teknisiä harjoituksia arvioinniksi, eskalaatioprosessin luominen.

Tietoisuuden tulee olla kohdennettua suoraan yksilölle kiinnostavaksi, muuten se ei muuta ihmisten käyttäytymistä. Ihmisten käytöksen muutoksen motivaattorit ovat ympäristösidonnaisia, kulttuurillisia ja henkilökohtaisia (Bada ym., 2015). Roolien ja vastuiden tulee olla selviä, johtajien tulee johtaa omalla esimerkillään. Kun tietoisuudessa huomioidaan roolit, vastuut, motivaatio ja prosessit, voidaan todella muuttaa ihmisten käyttäytymistä kohti kyberturvallisuuskulttuuria (Wright, 2019).

Kyberresilienssi

Resilienssi on dynaaminen oppimiseen perustuva prosessi. Erica Seville (2017) kuvaa sen organisaation kykynä ennakoida, varautua, vastata ja mukautua muutokseen ja yllättäviin häiriöihin, jotta organisaatio voi selvitä ja menestyä. Resilientti organisaatio tarvitsee sekä kykyä suunnitella, että mukautua. Resilientti organisaatio on valmis muutokseen ja yllättävän tilanteen tapahtuessa, yrityksen säilyttävä resilienssi palauttaa toiminnot nopeasti normaalille tasolle. Arjen resilienssi on sitkeyttä ja toimintaa, muutosjoustavuutta, sosiaalista kyvykkyyttä, sekä merkityksellisyyden kokemusta. (Seville, 2017.)

Kyberturvallisuus ja sitä ympäröivän kulttuurin muuttaminen on luonteeltaan sekä systeemistä muutosta että inkrementaalista muutosta. Systeeminen muutos on kokonaisvaltainen, monimutkainen muutos, vaikuttaa laajalti eri toimintamalleihin ja jossa monet muutostekijät ovat vaikeasti ennakoitavia. Resilienssikäsityksen mukaisesti siinä on useita samanaikaisia tasapainotiloja. Säilyttävä resilienssi palauttaa nykyiset toiminnot häiriötilan jälkeen, uuden systeemisen tasapainon hakeminen on uudistavaa resilienssiä. Strateginen kyberturvallisuuskulttuurin edistäminen on systeemistä muutosta, siihen liittyvät pienet jokapäiväiset muutokset inkrementaalista muutosta. (Uusikylä & Jalonen, 2023.)

Kyberturvallisuuskulttuurin maturiteetti

SANS Institute on kansainvälinen kyberturvallisuuskoulutuksia ja -sertifiointeja tarjoava yritys. Organisaation tavoitteena on tukea nykyisiä ja tulevia kyberturvallisuuden harjoittajia käytännön taidoilla ja tiedoilla. SANS on kehittänyt kyberturvallisuuskulttuurin maturiteettia mittaavan mallin jo vuonna 2011, jonka käyttö ja jatkokehitys jatkuu edelleen. Maturiteetin ymmärtäminen helpottaa tunnistamaan organisaation tilannetta ja mihin missäkin maturiteetin vaiheessa keskittyä. (SANS, 2026.)

Malli perustuu viiteen tasoon:

1. Kyberturvallisuustietoisuuden mallia ei ole. Työntekijöillä ei ole ymmärrystä tavoitteista, ja siitä että heidän toimillaan on suora vaikutus organisaation turvallisuuteen.
2. Vaatimusten täyttämiseen keskittyvä. Tietoisuuden malli keskittyy siihen, että täytetään lakisääteiset minimivaatimukset tai esimerkiksi sertifioinnin vaatimukset. Työntekijöillä ei ole ymmärrystä omasta roolistaan organisaation tiedon suojaamisessa.
3. Tietoisuuden ja käyttäytymisen muutos. Suurimmat ihmislähtöiset riskit on tunnistettu, ja kypsimmät organisaatiot tarjoavat jo kohdennetusti erilaista koulutusta ja tietoa. Viestinnän sävy on positiivista ja

kannustavaa. Työntekijä ymmärtää oman roolinsa kyberturvallisuudessa ja noudattaa ohjeita suojatakseen organisaatiota.

4. Pitkän ajan kulttuurillinen muutos. Tietoisuuden ohjelmassa ei enää keskitytä pelkästään kouluttamiseen, vaan myös laajemmin toiminnan kehittämiseen turvallisuuden huomioivaksi. Työntekijät ymmärtävät turvallisuuden merkityksen ja oman roolinsa siinä. Kyberturvallisuus ja turvallisuus ovat osa organisaatiokulttuuria.
5. Optimointi ja resilienssi. Tietoisuuden ohjelma on strategisesti tavoitteellinen, sillä on liiketoiminnallisia tavoitteita ja sen toteutumista mitataan. Seurauksena ohjelma kehittyy jatkuvasti ja tuo merkittävää liiketoiminnallista hyötyä. Turvallisuus on liiketoiminnan mitattava mahdollistaja. (SANS, 2026.)

3.2.4 Muutosjohtaminen

Organisaatiokulttuurin kehittäminen tarvitsee tuekseen aktiivista muutosjohtamista, sillä vain johdettu muutos toteutuu (Schein & Schein, 2017). Jokainen muutos tähtää johonkin tarpeeseen ja tavoitteeseen, muutoksella on aina syy miksi se pitää tehdä. Ulkoisia tarpeita voivat olla erilaiset muuttuneet säädökset tai lait, sisäisiä tarpeita esimerkiksi muutokset strategiassa tai keskittymiskohteissa. Muutosjohtaminen kuvaa käsitteenä sitä johtamisen prosessia ja työkaluja mitä tarvitaan, jotta muutos onnistuu. Muutos on onnistunut, kun ihmiset ovat muuttaneet toimintaansa. Muutosjohtamisessa keskitytään erityisesti ihmisten ja yksilön asenteiden ja toiminnan muutokseen. (Murthy, 2007; Prosci, 2025.)

Muutosjohtamisen malleja on useita, alkaen Lewinin 3-portaisesta jo 1947 julkaistusta mallista, Kotterin 8-portaiseen malliin (Tienari & Meriläinen, 2012). Mallit syntyivät havainnosta, että muutos ei tapahdu itsestään. Muutos vaatii aktiivista työtä vanhojen tapojen murtamiseksi, uuden työskentelytavan omaksumiseksi ja juurruttamiseksi. Prosci-yrityksen perustaja Jeffrey M. Hiatt esitteli 1990-luvun lopulla ADKAR-mallin. Proscin tekemän tutkimuksen pohjalta tunnistettiin, että muutos onnistuu, kun muutos tapahtuu yksilötasolla (Prosci,

2025). ADKAR keskittyy erityisesti ihmispuolen muutokseen, arvoihin ja asenteisiin, jotka ovat keskeisiä kulttuurimuutoksissa.

ADKAR-mallin mukaisesti jokaisessa muutoksessa on kaksi puolta: tekninen puoli ja ihmispuoli. Tekninen puoli kattaa muutoksen teknisen toteutuksen, jota ohjataan projektinhallinnan menetelmillä määrittelystä toteutuksen kautta käyttöönottoon. On tyypillistä, että muutoksissa huomioidaan vain tekninen puoli keskittyen projektin tehtävien loppuunsaattamiseen. Ihmispuolella tarkoitetaan kaikkea sitä, millä varmistetaan, että ihmisten käyttäytyminen todella muuttuu ja muutoksesta tulee pysyvä. Muutos on hidasta, ja jokainen yksilö käy jokaisen askeleen omassa tahdissaan. On kuitenkin olennaista, että askeleet tehdään järjestyksessä, jotta mielelle annetaan aikaa muuttua. Liian aikainen kouluttaminen esimerkiksi ei johda toivottuun lopputulokseen. Kouluttaminen on hyvä tehdä vasta sitten, kun tarvittava pohjaymmärrys on saavutettu. ADKAR-malli on saanut nimensä vaiheiden ensimmäisistä kirjaimista. ADKAR: Awareness, Desire, Knowledge, Ability ja Reinforcement:

1. Awareness – tiedostaminen: mikä muuttuu, koska, miten se vaikuttaa minuun. Luodaan pohja muutokselle.
2. Desire – halu: miten hyödyn muutoksesta, muutokseen osallistaminen. Vahvistetaan muutoksen pohjaa, osallistetaan, luodaan kiinnostusta.
3. Knowledge – tiedot: mitä todella pitää tehdä toisin, käytäntö. Pilkotaan muutos käytännöksi, mitä tietoa tullaan tarvitsemaan, koulutetaan, opastetaan.
4. Ability – taidot: miten toimin jatkossa. Vahvistetaan tieto taidoksi, harjoitellaan, kokeillaan, tehdään yhdessä.
5. Reinforcement – vahvistaminen: varmistetaan muutoksen toteutuminen. Muutoksen vahvistaminen esimerkiksi juhlimisella, seurataan muutoksen toteutumista, kysytään kokemuksia, tehdään lisätoimenpiteitä vahvistamiseksi. (Prosci, 2025.)

3.2.5 Keskeiset huomiot

Kyberturvallisuus ja siihen liittyvä kulttuuri tähtäävät siihen, että häiriöt eivät lamauta organisaatiota tai sen yksilöitä. Pitkäjänteinen muutos jatkuvasti muuttuvassa maailmassa sekä organisaation resilienssikyky ovat kriittinen yhdistelmä. Kulttuuri ei muutu hetkessä (Luukka, 2019), jatkuvat häiriöt tai uudet toimintatavat aiheuttavat muutoskriittisyyttä (Prosci, 2025) ja organisaation menestymiseksi organisaation tulee laaja-alaisesti suunnitella tulevan varalle ja mukautua tilanteisiin (Seville, 2017.)

Kyberturvallisuutta tulee suunnitella käyttäjälähtöisesti, ihmislähtöisesti. Toimintatapojen ja tietoteknisten suojausten tulisi olla tarpeeksi yksinkertaisia, jotta ne voidaan ymmärtää. Pakottaminen ja käskeminen ei lähtökohtaisesti tuo sitä ymmärrystä joka käyttäjää motivoi. Ihmisen motivaatiolla on suuri merkitys halutun lopputuloksen saamiseksi. (Adams & Sasse, 1999; Sasse, 2015.)

4 Haastattelututkimuksen tulokset: Kyberturvallisuuskulttuuri

Tässä kappaleessa kuvataan haastattelututkimuksen (Liite 2: Haastatellut, 2025) tuloksia. haastatteluissa nousseita Haastateltaessa tietoturva-asiantuntijoita, kyberturvallisuuden määritelmät poikkeavat hivenen toisistaan asiantuntijoiden taustan ja kokemusten kautta. Toiset asiantuntijat viittaavat kyberturvallisuuteen teknisinä turvallisuuden ratkaisuina, toiset asiantuntijat nostavat ihmisen roolin merkitykselliseksi osaksi kyberturvallisuutta. Kyberturvallisuuden paikka osana tietoturvaa tai kyberturva poikkileikkaavana turvallisuuden osana myös vaihteli kokemusten ja taustojen perusteella. Kyberturvallisuus on nuori ala, ja sen määritelmät eivät ole täysin vakiintuneita, organisaatiolla ja omalla roolilla on myös vaikutusta käytettyihin termeihin.

Useat haastatellut turvallisuusasiantuntijat pitivät sanaa ”kyber” huonona, jopa ”hypenä” ja turhaakin pelkoa ilmentävänä sanana. Asiantuntijat käyttäisivät mieluummin sanaa tietoturva tai eri muotoja sanasta turvallisuus. Haastatteluissa nostettiin tekninen turvallisuus ja hallinnollinen turvallisuus helpommin ymmärrettävinä termeinä. Luottamuksellisuus ja tiedon turvaaminen on niitä asioita, joita kyberturvallisuuden teknisillä ja hallinnollisilla ratkaisuilla pyritään suojaamaan. Kyberturvallisuutta toteutetaan uhkia ja riskejä hallinnoimalla ja niihin varautumalla.

Toimialalla on vaikutus terminologiaan. Haastatteluissa nostettiin esiin korkeimman uhkan tai riskin mukaista terminologiaa. Jos ollaan perinteisen teollisuuden parissa, henkilöstöturvallisuus on merkityksellisin turvallisuuden alue, jolloin sana ”turvallisuus” on se tärkein ja sen alle niputetaan myös muut turvallisuuden osa-alueet. Digitaalisen liiketoiminnan yrityksessä, jossa yrityksen tai sen asiakkaiden tieto on suurin suojattava asia, ”tietoturva” ja ”kyberturva” ovat käytetyimmät termit. Uhka tai riski määrittää myös kyberturvallisuuden paikan organisaatiossa, ja sillä voi olla suora vaikutus kyberturvallisuuden budjettiin ja toimenpiteisiin. Mitä strategisempana ja

tärkeämpänä kyberturvallisuus nähdään, sen näkyvämpi paikka sillä on organisaatiossa.

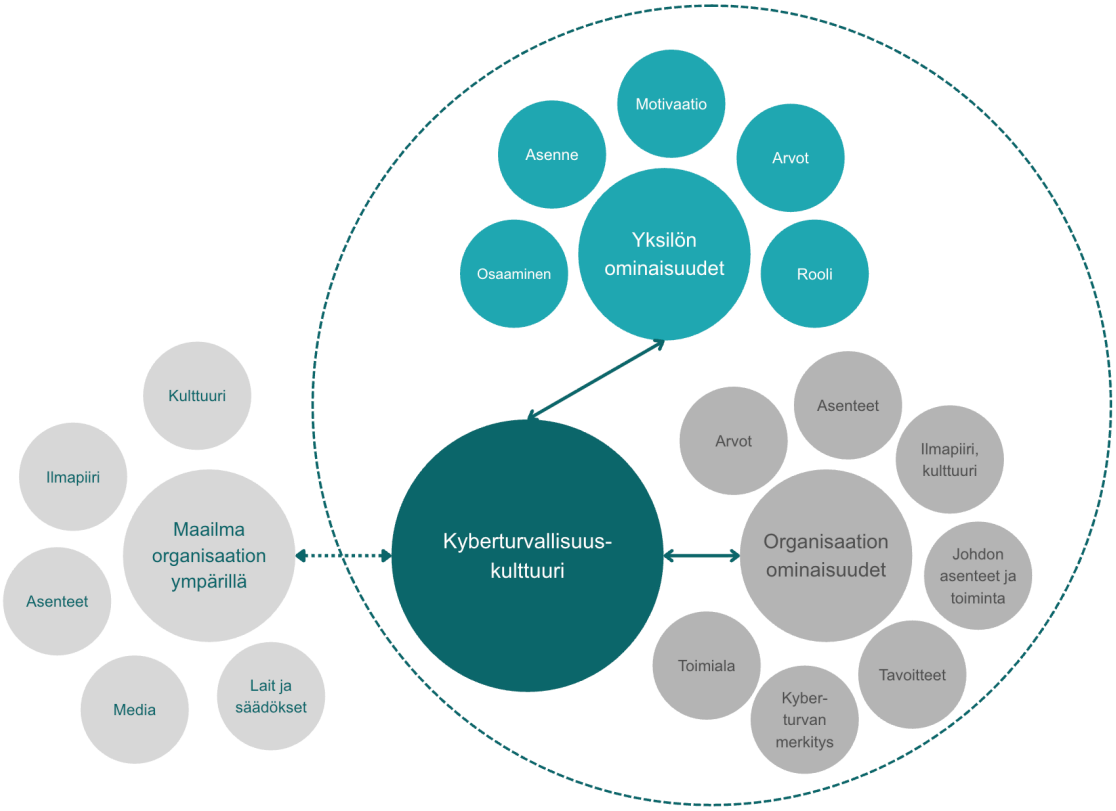
Keskeisenä havaintona voi tunnistaa, että kyberturvallisuuden ja turvallisuuden eri osa-alueiden terminologian ja suhteiden toisiinsa määrittäminen ja kuvaaminen organisaatiokohtaisesti on olennainen osa kulttuurin kehittämistä. Yhtenäinen terminologia luo yhtenäisen kokemuksen. Lisäksi uhka- ja riskitaso ja strateginen merkittävyys määrittelee kyberturvallisuuden paikan organisaatiossa ja siihen käytettävissä olevat resurssit.

4.1 Kyberturvallisuuskulttuuri organisaatiokulttuurin osana

Haastateltavat yksimielisesti näkevät kyberturvallisuuden kulttuurillisena asiana. Esiin nousi myös Luukan (2017) nostama teema, miten kulttuuri on sitä mitä tapahtuu, kun kukaan ei katso. Kyberturvallisuuskulttuurin katsotaan toteutuvan, kun se on luontaista toimintaa arjessa, kyberturvalliset toimet ovat sidoksissa arjen rutiineihin, ja kyberturvallisuus on luonteva osa ajattelutapaa. Kyberturvallisuuden ja sitä toistavan kulttuurin tehtävänä on toimia liiketoiminnan tavoitteiden mahdollistajana. Mahdollistavuus tarkoittaa sitä, että turvallisuusajattelu on osa kaikkea toimintaa. Silloin kyberturvallisuuden läsnäolo on jatkuvaa, ja pelkkä viestintää sekä koulutus kerran vuodessa ei riitä. Parhaassa tapauksessa kyberturvallisuuskulttuuri auttaa yksilöä näkemään vaihtoehtoja ja ratkaisumahdollisuuksia riskien välttämiseksi uhkien sijaan. Hyvässä kulttuurissa katse on aina tulevaisuuteen suunnattu. Virheistä opitaan, apua pyydetään ja myös vastaanotetaan.

Organisaation sisäisellä kuin ulkoisellakin asenneilmapiirillä kyberturvallisuutta kohtaan on merkittävä vaikutus. Negatiivisessa ilmapiirissä ihmiset piilottavat virheensä, kun taas positiivisessa niistä uskalletaan puhua ja oppia. Pelolla ja liialla uhkailulla ei kyberturvallisuudessa päästä kannustavaan turvalliseen kulttuuriin, joten arvot, asenteet ja ihmisen arvostus erityisesti johdon suunnalta merkitsevät. Maailman kulloinenkin tilanne ja asenneilmapiiri vaikuttaa niin yksilöihin kuin yrityksiinkin, median tuomalla viestillä ja sen sävyllä on vaikutus.

Yksilö tuo organisaatioon omat arvonsa ja asenteensa ja myös kokemansa motivaation. Organisaation muu toiminta vaikuttaa motivaatioon, epäreiluuden tuntemus yrityksen taholta voi vaikuttaa toimimaan yrityksen ohjeiden mukaisesti. Lisäksi jos oman roolin ja tehtävien vaikutuksia kyberturvallisuuteen on vaikea tunnistaa, on sitä myös vaikea tuoda arkeen luonnolliseksi osaksi. Haastattelujen pohjalta tunnistettiin kyberturvallisuuskulttuuriin vaikuttavat ominaisuudet kuvaan 4.



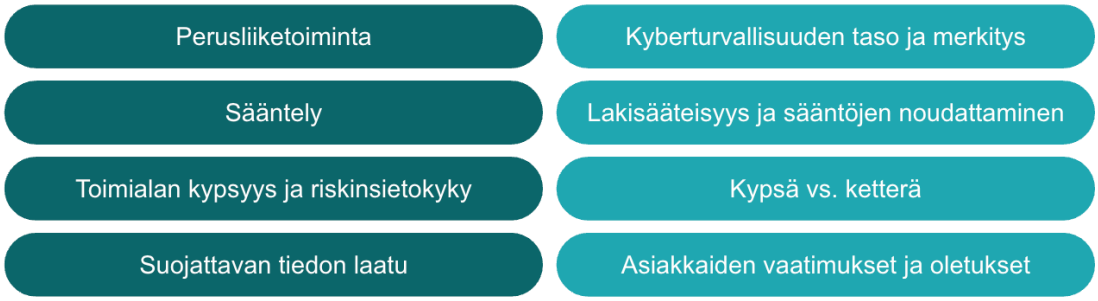
Kuva 4. Kyberturvallisuuskulttuuriin vaikuttavat ominaisuudet

Keskeisenä havaintona voi tunnistaa, että kyberturvallisuuskulttuuri on sellainen kulttuuri, jossa kyberturvallinen toiminta on luonnollinen osa arkea. Tällaiset toimenpiteet voivat olla esimerkiksi laitteiden ja salasanojen suojaaminen, kyberturvallisuuden huomioiminen prosesseissa niin että prosessit huomioivat turvallisen toiminnan. Kyberturvallisuus ei ole irrallinen päälle liimattava osa, eikä sitä voi irrottaa organisaation yrityskulttuurista tai esimerkiksi yrityksen tavoitteista. Johdon asenteilla ja toiminnalla kyberturvallisuutta kohtaan on suuri

merkitys. Kyberturvallisuuskulttuuriin vaikuttaa myös yksilön ja organisaation ominaisuudet sekä organisaation ulkopuolinen maailma ja kulloinkin voimassa oleva ilmapiiri.

4.2 Toimialan vaikutus kyberturvallisuuskulttuuriin

Haastatteluissa havaittiin suuriakin eroja kyberturvallisuuden ja kyberturvallisuuskulttuurin suhteen toimialojen välillä. Perusliiketoiminta ja regulaatiot ohjaavat kyberturvallisuuden tasoa. Toimialan kypsyys, riskinsietokyky sekä suojattavan tiedon laatu vaikuttavat panostuksiin. Toimialavaikutukset on jaoteltu haastattelujen pohjalta kuvaan 5.



Kuva 5. Toimialavaikutus kyberturvallisuuskulttuuriin

4.3 Perusliiketoiminta

Perusliiketoiminta vaikuttaa turvallisuustason valintaan. Miten paljon perusliiketoiminnan vahinkoa voi kyberturvallisuuden riskistä tulla, vaikuttaa tekniseen kyberturvallisuuteen ja siihen, miten paljon kyberturvallisuuskulttuuriin halutaan panostaa. Kun riskin vaikutukset toteutuessaan ovat vakavat, ei suuria riskejä haluta ottaa ja kyberturvallisuuteen halutaan panostaa. Kriittisillä toimialoilla kuten energia, kyberturvallisuuden merkitys on korkeammalla kuin vähemmän kriittisillä aloilla, kuten toteuttava teollisuus (Liite 2: Asiantuntija 6, 2025).

Perusliiketoiminta vaikuttaa myös siltä kulmalta, mikä turvallisuuden osa-alue on toimialalle merkittävin. Valmistavassa teollisuudessa IT toimii usein erillisenä

omana alueenaan, jonka kanssa valmistavalla organisaation osalla ei ole yhteistä rajapintaa. Tässä ympäristössä on helpompi panostaa esimerkiksi henkilöstöturvallisuuteen kuin kyberturvallisuuteen, joka tuntuu irralliselta ja abstraktilta valmistavan organisaationosan arjesta. Kuitenkin tässä ympäristössä kyberturvallisuuden uhkien realisoituessa seurauksetkin ovat vakavat. (Liite 2: Johto 2, 2025; Liite 2: Muutosjohtaja 2, 2025.)

4.3.1 Sääntely

Regulaatio eli sääntely nousi haastatteluissa merkittäväksi tekijäksi toimialoilla. Mitä enemmän säätelyä ja sääntelyä toimialalla on, sitä paremmin kyberturvallisuus on huomioitu ja sitä varmemmin henkilöstö myös noudattaa ohjeita ja sääntöjä. Sääntöjen noudattaminen on silloin rakentunut vahvasti organisaatiokulttuuriin. Sääntelyllä on myös riski, että kyberturvallisuuskulttuurikin on liian säänneltyä. Muutosjohtaja 1 (Liite 2: Haastatellut, 2025) nosti esiin, että sääntely voi johtaa myös kyberturvallisuuskulttuurin sääntelyyn. Hän korosti, että sellaisessa kulttuurissa sääntöjen noudattaminen ei tarkoita, että henkilöstö välttämättä sisäistää miksi joku asia pitää tehdä tietyllä tavalla, sääntöjä vain noudatetaan noudattamisen vuoksi. Toimimattomien ja hankalien prosessien terve kyseenalaistaminen voi jäädä silloin pois (Liite 2: Muutosjohtaja 1, 2025). Sääntelyyn liittyy myös asiakkaiden vaativat sertifikaatit. Kyberturvallisuuden taso voi määräytyä asiakkaiden vaatimusten säätelemänä. EU:n henkilöstösuojadirektiivi toi esimerkiksi henkilötiedoille säännellyn suojan.

4.3.2 Kypsyys ja riskinsietokyky

Toimialoilla on haastattelujen perusteella kypsyyseroja kyberturvallisuuden ja sitä tukevan kulttuurin suhteen. Mitä kypsempi toimialan turvallisuuskäsitys yleisesti on, sitä pidemmällä myös kyberturvallisuus on niin teknisesti kuin kulttuurillisesti (Liite 2: Asiantuntija 6, 2025). Esimerkkinä asiantuntija nosti huoltovarmuuden kannalta merkityksellisen energiasektorin, sekä

lentoliikenteen, missä suurimpana riskinä on ihmishenki. Lentoliikenne nousi toisessakin haastattelussa esimerkiksi siitä toimialasta, missä kyberturvallisuuden takia tietyt toimet tehdään edelleen manuaalisesti, ”kädestä käteen” (Liite 2: Asiantuntija 5, 2025). Tässä mainittuihin toimialoihin liittyy myös korkeat riskit. Jos organisaatio on tottunut käsittelemään suuria riskejä, myös kyberturvallisuus on paremmin huomioitu (Liite 2: Johto 2, 2025). Mitä nuorempi ala on, esimerkiksi startup-kenttä, sitä herkemmin sääntöjä ohitetaan tai teknisen tietoturvan kannalta valitaan nopea ja helppo tie, mikä ei aina ole se turvallisin tie (Liite 2: Muutosjohtaja 2, 2025).

4.3.3 Suojattavan tiedon laatu

Se, minkälaista tietoa yritys käsittelee, vaikuttaa haastattelujen mukaan kyberturvallisuuden tasoon. Kaikki yritykset käsittelevät vähintään henkilöstönsä henkilötietoja, lisäksi asiakkaiden tietoja sekä todennäköisesti asiakkaiden salassa pidettävää tietoa. Julkisella sektorilla on laaja määrä suojattavaa tietoa, ja siellä sen suojaamiseen reagoidaan ja myös panostetaan (Liite 2: Johto 1, 2025). Julkinen sektori on myös vahvasti reguloitua, joka ohjaa panostusta. Sosiaali- ja terveysala käsittelee kriittistä tietoa, mutta siellä kyberturvallisuus ja sitä tukeva kulttuuri ovat vasta rakentumassa. Suojattavana tietona raha on erityisasemassa, finanssiala on tästä syystä panostanut merkittävästi kyberturvallisuuteen (Liite 2: Asiantuntija 2, 2025). Haastatteluissa nousi esiin rahan merkitys. Toimialat, jotka käsittelevät rahaa, suojaavat sitä tehokkaasti ja käyttävät myös rahaa sitä suojaamaan. Asiakkaiden odotukset ja vaatimuksetkin vaikuttavat tämän toteutumiseen.

4.4 Kyberturvallisuuskulttuurin menestystekijät (mahdollistajat)

Haastattelujen mukaan hyvä kyberturvallisuuskulttuuri on sellainen, jossa kyberturvallisuutta toteutetaan oikealla mitoituksella, tavoitteellisesti ja johdon omistamana. Kyberturvallisuus on organisaatiossa tärkeässä asemassa, ja se myös näkyy arjen puheissa ja teoissa. Yleinen asenneilmapiiri organisaatiossa

on avoin, positiivinen ja kannustava, henkilöstöä kannustetaan oppimaan uutta ja myös jakamaan kokemaansa. Tietoa kyberturvallisuudesta on saatavilla ja henkilöstöä palkitaan aktiivisesta turvallisuustoiminnasta. Kyberturvallisuuteen liittyvä koulutus ja viestintä on kohdennettua yksilön arkeen, ja yksilö ymmärtää oman roolinsa merkityksen turvallisuudessa. Prosessit ja yleiset toimintatavat ottavat huomioon kyberturvallisen arjen, ja on luonnollista toimia turvallisesti. Kyberturvallisuus ei ole satunnaista, vaan jatkuvaa toimintaa henkilöstön arjessa niin töissä kuin vapaalla. Yleisesti organisaatiossa on yhteisesti jaettu turvallisuudentunne. Hyvän kyberturvallisuuskulttuurin menestystekijät on jaoteltu haastattelujen analysoinnin perusteella kuvaan 6.

Kuva 6. Kyberturvallisuuskulttuuriin menestystekijät

4.4.1 Johto ja omistajuus

Johdon roolin merkitys esimerkkinä ja kyberturvallisuuden omistajana nousi kaikissa haastatteluissa vahvasti esiin. Kyberturvallisuuden merkityksen ymmärtäminen ja esiin tuominen osana johdon normaalia viestiä, on vahvin kulttuurin vahvistaja (Liite 2: Asiantuntija 4, 2025). Toiselta kulmalta, jos johto ei

seiso viestin takana, on turvallisuustyöllä heikko pohja (Liite 2: Muutosjohtaja 1, 2025). Johdon rooli ei rajoitu pelkästään yrityksen ylimpään johtoon, lähiesihenkilöillä on myös merkittävä rooli esimerkkinä ja tukena. Lähiesihenkilöltä on luontevaa kysyä vaikeitakin kysymyksiä kyberturvallisuuskulttuurista.

Turvallisuuden tavoitetila määräytyy yrityksen tavoitetilan pohjalta, kyberturvallisuus on liiketoiminnan mahdollistaja. Tämä ohjaa suoraan myös valittuihin teknisiin ratkaisuihin. Suojauksen tulee olla sopivalla tasolla suhteessa tavoitetilaan, jatkuvasti kehittyen, moderneja suojaustapoja hyödyntäen. Yrityksen turvallisuussäädökset- ja ohjeistukset tulee sitoa sen toimintaan sopivaksi, oikealle tasolle. Tiukimmat säädökset ei sovellu kaikille, ja taas toisaalta mitä kriittisemmän tiedon parissa työskennellään, sen tiukampaa turvallisuuden tulee olla. Tavoitteen ymmärtäminen yksilötasolla, kohdennetusti vahvistaa kulttuurillista kokemusta. Kun henkilöstö ymmärtää, mitä kyberturvallisuus ja tavoitetila tarkoittaa juuri heidän omassa roolissaan, on todennäköisempää, että ohjeita noudatetaan.

Kyberturvallisuuden roolit ja vastuut tulee olla määritelty. Johdolla on selkeä omistajuus ja niin tekniset kuin tietoisuudenkin roolit on tunnistettu ja kuvattu. Kyberturvallisuuden vastuiden kautta sitä aktiivisesti edistetään organisaation kaikilla tasoilla. Tässä on käytössä erilaisia organisaatiolle luontaisia verkostoja ja tapoja tavoittaa koko henkilöstö.

4.4.2 Organisaatiokulttuuri ja asenneilmapiiri

Olemassa olevan organisaatiokulttuurin ja yleisen asenneilmapiirin merkitys kyberturvallisessa kulttuurissa nousi haastatteluissa esiin. Organisaation arvot, asenteet, toimintaympäristö heijastavat johdon ihmiskäsitystä. Jos ihmisiin ei luoteta ja ilmapiiri on negatiivinen, perustuu kulttuuri valvontaan ja sääntöihin. Positiivinen ihmiskäsitys rakentaa luottamuksen ja avoimuuden ilmapiiriä. Johdolla on esimerkkinä vahva rooli ilmapiirin luomisessa, ja turvallisuuden merkityksen nostamisessa. Organisaation ilmapiiri on kuin johtajansa peili.

Yleisesti koettiin, että positiivisen kautta vahvistaminen on paras tapa kannustaa kyberturvalliseen työskentelyyn. Toisten kautta oppiminen ja hyvien esimerkkien avulla toistaminen on hyvän asenneilmapiirin tulosta. Negatiivinen ilmapiiri taas voi saada ihmiset piilottamaan virheensä, ja kyberturvallisuuden uhkia voi näin realisoitua.

4.4.3 Osaaminen ja tietoisuus

Osaamista voidaan katsoa kahdesta näkökulmasta: teknisten asiantuntijoiden osaaminen ja henkilöstön osaaminen (Liite 2: Johto 1, 2025). Kummallakin on tietoisuudessa tärkeä rooli. Yrityksen toimialasta ja tietoturvakriittisyydestä riippuen, teknisen henkilöstön tarvittava osaamisen taso voi poiketa. Tietoisuuden ohjelmissa tulee siis tunnistaa kyberturvallisuuden tekijöiden tarpeet. Toisaalta myös teknisen henkilöstön kohdalla on olennaista saada heidät mukaan yleiseen viestiin ja koulutuksiin, oman oppimisen ja toisaalta esimerkkinä toimimisen näkökulmasta. (Liite 2: Johto 1, 2025; Liite 2: Johto 2, 2025; Liite 2: Asiantuntija 6, 2025.)

Henkilöstön osaaminen ja tietoisuuden kehittäminen on avainasemassa ja johdolla on merkittävä tehtävä toimia oppimisen mahdollistajana esimerkiksi ajankäytön sallimisen osalta. Osaava ja tiedostava henkilöstö voi pelastaa uhkaavan tilanteen ja olla näin turvallisuuden vahvin lenkki (Liite 2: Johto 1, 2025). Henkilöstön kannalta tiedon tulee olla ymmärrettävää, lähellä omaa roolia ja arkea, ja erityisesti jatkuvaa. Organisaation eri roolien arjen ymmärtäminen on tietoisuuden kasvattamisessa tärkeää. Positiivinen vahvistaminen näkyy arjessa myös kyberturvallisesta toiminnasta palkitsemisella, on se sitten henkilökohtaisesti välitettyä, julkista kiitosta tai esimerkiksi sertifikaatteja.

4.4.4 Prosessit ja toimintatavat

Kyberturvallinen työskentely on mahdollista, kun yrityksen prosessit ja toimintatavat on suunniteltu ne huomioiden. Jos prosessit pakottavat hankaliin toimintatapoihin turvallisuuden takia, on todennäköistä, että henkilöstö valitsee toisen toimintatavan, joka ei välttämättä ole enää turvallinen. Järjestelmällinen ja kyberturvallinen tapa toimia lisää järjestelmällisyyttä, eikä oikomista tapahdu (Liite 2: Johto 2, 2025). Turvallisuus ei saa olla hidaste, tai toimintatavan monimutkaistaja. Millään tietoisuusohjelmalla ei ole merkitystä, jos arki hankaloituu turvallisuuden takia.

4.4.5 Jatkuvuus ja palkitseminen

Kyberturvallisuuskulttuurin edistäminen ja vahvistaminen on jatkuvaa toimintaa. Luontevasti osana normaalia arkena kyberturvallisuus toimii liiketoiminnan mahdollistajana. Tämä tarkoittaa kaikkien aiemmin mainittujen elementtien olemista läsnä kaikessa, kun prosesseja kehitetään, kun organisaatiossa tapahtuu epämiellyttäviä asioita kuten muutosneuvotteluja, johdon puheissa ja toiminnassa. Kyberturvallisuuden tulee olla luonteva osa arkea, jatkuvasti, silloin myös kyberturvallisuuskulttuuri vahvistuu.

4.5 Kyberturvallisuuskulttuurin toteutumisen haasteet

Haasteet kyberturvallisuuskulttuurin toteutumiselle nähtiin voimakkaasti käänteisinä sen mahdollistajille. Jos johto on mukana vain päälle liimattuna tai ei ollenkaan, se ei edesauta kulttuurin toteutumista. Johdon sitoutuneisuus tai sitoutumattomuus aiheuttaa myös muita haasteita kulttuurin toteutumiselle: jos kyberturvallisuus ei ole merkityksellistä yritykselle ja sen tavoitteille, sen kehittämiselle tuskin myöskään on tarjolla resursseja niin henkilöstön kuin budjetin näkökulmasta.

Henkilöstön näkökulmasta kyberturvallisuus voidaan kokea vieraana, kaukaisena. Toimiala ja oma rooli voi vaikuttaa tähän voimakkaasti. Kyberturvallisuuteen tottumattoman organisaation henkilöstö voi keskittyä enemmän fyysisen turvallisuuden asioihin jopa kyberturvallisuuden kustannuksella. Ihmisten suojelemiseksi voidaan hyödyntää suojaamattomia teknisiä ratkaisuja.

Kyberturvallisuustietoisuuden kehittäminen, kun organisaatio ei ole prosessiensa puolesta turvallinen, voi aiheuttaa vieroksumisen ilmiön. On siis hyvin tärkeää katsoa organisaatiota kokonaisuutena. Varmistaa, että turvallisuus on oikein mitoitettu, työtä tehdään tavoitteellisesti ja tämä huomioidaan kaikissa toimintatavoissa.

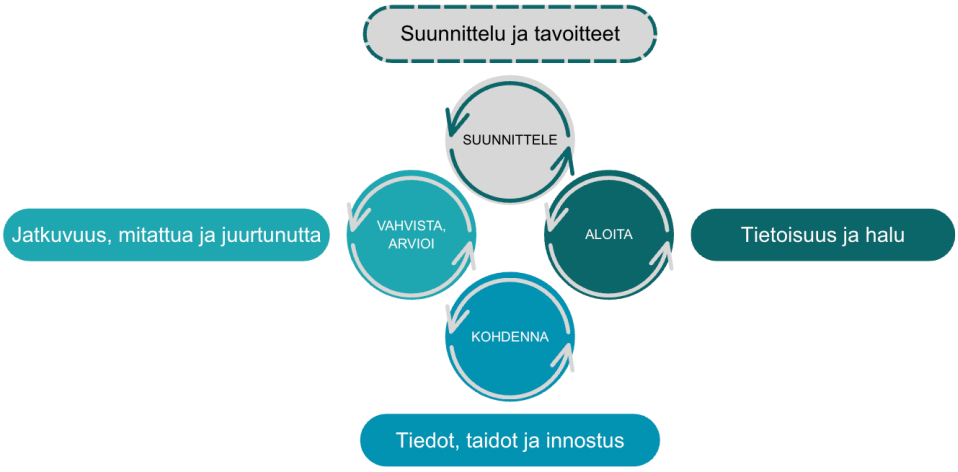
5 Kyberturvallisuuskulttuurin kehittäminen muutosjohtamisen keinoin

Aiemmissa kappaleissa on tutkittu teoreettisen viitekehyksen ja haastattelututkimuksen pohjalta mikä vaikuttaa yrityksen kyberturvallisuuskulttuuriin ja mitä sen kehittämisessä tulisi huomioida. Tässä kappaleessa sovelletaan kerättyä ymmärrystä sekä muutosjohtamisen ja kyberturvallisuustietoisuuden malleja kyberturvallisuuskulttuurin vahvistamiseksi, tietoisuudesta ajatustavan muutokseen. Jokaisessa muutoksessa, myös kyberturvallisuuskulttuurin muutoksessa, on kaksi puolta (Prosci, 2025). Tekninen muutos on tunnistettu muutos, jolla on tavoite, tekniset projektimäärittelyt ja suunnitelmat sekä käyttöönotto. On tyypillistä, että tietoisuuden ohjelmaa katsotaan teknisenä käyttöönottona ja keskitytään ensisijaisesti toteutettaviin toimenpiteisiin, esimerkiksi viestintään sekä vuosittaisiin koulutuksiin (Liite 2: Haastatellut, 2025). Muutoksessa on kuitenkin myös toinen puoli, inhimillinen puoli. Tällä puolella tarkoitetaan ihmisten ajattelutavan ja toiminnan todellista muutosta. Jos tämä puoli jätetään huomioimatta, on todennäköistä, että muutoksen tekninenkään puoli ei onnistu (Prosci, 2025). Inhimillinen puoli vaatii pitkäjänteistä ja suunnitelmallista työtä, paljon yhteistyötä organisaation eri tahojen kanssa ja yhteistä tavoitteellista toteuttamista.

Tutkimuksen lopputuloksena on muodostettu kokonaismalli, miten muutosjohtamisen ja kyberturvallisuustietoisuuden malleja voitaisiin soveltaa yhteen siten, että ne voisivat kulkea rinnakkain, toisiaan tukien panostaen sekä tekniseen että ihmispuolen muutokseen. Kokonaismalli on esitetty kuvassa 7. Kokonaismalli on jaoteltu neljään vaiheeseen: suunnittele, aloita, kohdenna sekä vahvista ja arvioi. Muutosjohtamisen ADKAR-malli sekä ENISAn esimerkki kyberturvallisuustietoisuuden kehittämisestä on esitetty rinnakkain. Kummassakin mallissa nostetaan samoja teemoja, mutta eri kulmalta.

Kuva 7. Kyberturvallisuuskulttuurin kehittäminen kyberturvallisuustietoisuuden ja muutosjohtamisen mallin avulla (Mukaillen: Prosci, 2025; ENISA, 2023)

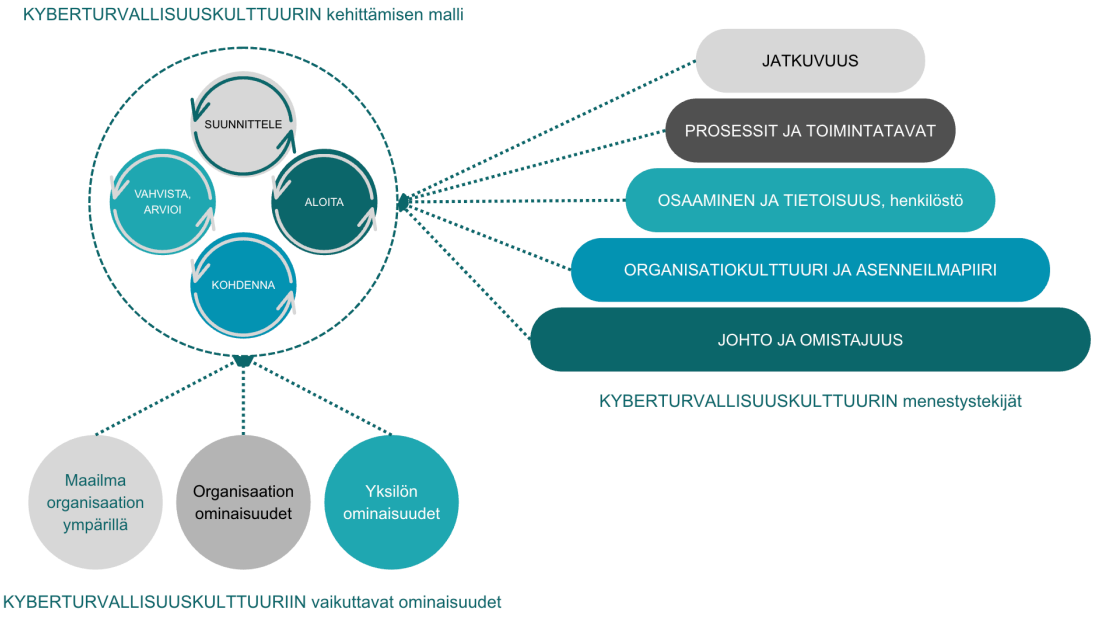
Seuraavassa esitellään tarkemmin tutkimuksen lopputuloksena syntyneet neljä vaihetta, joissa keskitytään nimenomaan siihen mitä mallien lisäksi tai tehostamiseksi tulisi tehdä ja miten, jotta ihmisten ajatustavat ja toiminta saadaan muuttumaan kyberturvalliseksi. Malli jakautuu kuvassa 8 esitetyn mukaisesti neljään osaan: suunnittele, aloita, kohdenna sekä vahvista ja arvioi.



Kuva 8. Kyberturvallisuuskulttuurin kehittäminen muutosjohtamisen menetelmillä, päävaiheet

5.1 Muutosjohtamisen sovellettu malli kyberturvallisuuskulttuurin vahvistamiseksi

Kyberturvallisuuskulttuuriin vaikuttavat menestystekijät ohjaavat mallin soveltamista. Näitä olivat mm. oman organisaatiokulttuurin ja toimialan vaikutus, sekä kyberturvallisuuskulttuurin tunnistetut menestystekijät, kuten johdon aktiivinen rooli (Liite 2: Haastatellut, 2025). Kulttuuriin vaikuttavat aiemmin tunnistetusti myös maailma meidän ympärillämme, sekä yksilön omat ominaisuudet. Kuvassa 9 on vedetty yhteen onnistuneen kyberturvallisuuskulttuurin menestystekijät ja niihin vaikuttavat ominaisuudet (Liite 2: Haastatellut, 2025).



Kuva 9. Kyberturvallisuuskulttuurin kehittämisen mallissa huomioitavat menestystekijät ja ominaisuudet

Ajatusmallien muuttaminen turvallisuusorientoiduksi vaatii runsaasti avointa keskustelua kyberturvallisuudesta suhteessa organisaation tavoitteisiin ja arvoihin, johdon aktiivista osallistumista sekä erilaisten mielipidevaikuttajien aktivointia. Riskien tunnistaminen ohjaa suunnittelua, ja sitä mitä voidaan ratkaista teknisesti, ja missä tarvitaan ihmisten osaamisen ja tietoisuuden kehittämistä. Prosessin aikana tulee olla valmis myös kriittiseen keskusteluun ja

olla avoin muuttamaan tietoisuuden koulutusta, viestintää ja organisaation yleisiäkin toimintatapoja sekä prosesseja. Työ on pitkäjänteistä, ja sen aikana tulee olla valmis muutoksiin. Yhteistyöllä ja aktiivisella osallistamisella voidaan päästä onnistuneeseen lopputulokseen.

Organisaation nykytilaa voi arvioida kyberturvallisuusmaturiteetin kautta. Tässä mallissa oletetaan kyberturvallisuuskulttuurin maturiteetin tason olevan 1-2. Ensimmäisellä tasolla tietoisuuden ohjelmaa ei ole olemassa. Jotain viestintää on voinut olla, mutta työntekijöillä ei ole kattavaa ymmärrystä omasta roolistaan kyberturvallisuudessa tai edes organisaation tietoturvan ohjeistuksista. Maturiteetin tasolla 2 on keskitytty lakisääteisiin minimivaatimuksiin, jolloin silloinkaan työntekijä ei tunne vielä omaa rooliaan turvallisuuden tekijänä. (SANS, 2026.)

Seuraavaksi ja kuvassa 10 on kuvattu, mitä erityisesti olisi hyvä huomioida vaiheittain, jotta kyberturvallisuustietoisuus muuttuisi kyberturvallisuuskulttuuriksi, missä myös ajatusmallit ovat kyberturvallisia ja soveltaminen arjessa voi tapahtua. Vaiheissa on eritelty menestystekijäkohtaisesti mitä erityisesti huomioitava.

Kuva 10. Kyberturvallisuuskulttuurin kehittäminen muutosjohtamisen menetelmillä, vaiheiden kuvaus menestystekijöittäin

5.1.1 Suunnittele: Muutoksen ja tavoitetilan määrittäminen

Hyvä suunnittelu on onnistuneen muutoksen kivijalka. Ihmispuolen muutos keskittyy erityisesti ihmisen toiminnan ja ajatusmallien muutokseen. Osaamisen kehittämisen kannalta on olennaista tuntea oma organisaatio ja sen kohderyhmät. Johdolla ja mielipidevaikuttajilla on vahva rooli positiivisen asenneilmapiirin vahvistamisessa, ja näiden tukiryhmien aktivointi on suunnitteluvaiheen tärkeimpiä tehtäviä (Luukka, 2019). Suunnittelu on vaiheista laajin, sillä siinä perehdytään organisaation erityispiirteisiin laajasti ja dokumentoidaan organisaatiosta paljon sellaista, mitä todennäköisesti ei ole ennen tehty. Harvassa organisaatiossa kohderyhmät on tunnistettu valmiiksi kattavalla tavalla tai pohdittu minkä tukiryhmien kanssa turvallisuutta olisi hyvä edistää. Johdon sitoutuneisuuden vahvistaminen on onnistumisen kannalta kriittistä ja suunnitelma perusteluineen saa herkemmin johdolta täyden tuen. Suunnittelussa erityisesti huomioitavat menestystekijät, ja miten ne olisi hyvä huomioida, on kuvattu kuvaan 11 (Liite 2: Haastatellut, 2025).

Kuva 11. Kyberturvallisuuskulttuurin kehittäminen muutosjohtamisen menetelmillä, vaiheiden kuvaus menestystekijöittäin

Jatkuvuus

Yrityksen toimiala vaikuttaa kyberturvallisuuden tasoon ja organisaatiokulttuuriin ja sen vaikutus on huomioitava suunniteltaessa sopivaa kyberturvallisuustietoisuuden ohjelmaa (Liite 2: Haastatellut, 2025). Yhteisen

terminologian määrittäminen tässä vaiheessa auttaa viestin suunnittelussa ja tiedon omaksumisessa. Turvallisuusratkaisujen tulee olla oikein mitoitettuja suhteessa liiketoimintatavoitteeseen ja riskitasoon, silloin ne otetaan vastaan herkemmin (ENISA, 2023; AlHogail, 2015).

Prosessit ja toimintatavat

Jokaisessa organisaatiossa on omia erityispiirteitä, jotka vaikuttavat toimintatapoihin ja prosesseihin. Suunnitteluvaiheessa ei varsinaisesti lähdetä vielä muokkaamaan prosesseja tai toimintatapoja uusiksi, mutta voi olla hyvä luoda pohjaa niiden keräämiselle. Mitkä organisaatiossa tunnistetaan erityispiirteiksi ja mikä niiden vaikutus kyberturvallisuuteen voi olla (Liite 2: Haastatellut, 2025). Organisaation perustehtävä voi esimerkiksi jo itsessään luoda vaateita turvallisuudelle ja silloin se on hyvä tunnistaa jo alkuvaiheessa, mikä sen vaikutus kyberturvallisuustietoisuuden ohjelmaan on.

Osaaminen ja tietoisuus

Suunnitteluvaiheessa valmistaudutaan kohtaamaan ja osallistamaan henkilöstöä. Tätä tehtävää varten on tarpeen tunnistaa organisaation kannalta kaikki kohderyhmät, joita muutos koskee (Prosci, 2025). Kyberturvallisuustietoisuus ja sitä vahvistava kulttuuri koskee kaikkia, mutta eri tavoin. Tässä vaiheessa myös priorisoidaan, miten ja keitä tullaan tavoittelemaan ensimmäiseksi, mitä ryhmiä pidetään turvallisuuden kannalta kriittisimpinä. Kohderyhmäsuunnittelu on enemmän, kuin vain kohderyhmien tunnistamista, kuten kuvassa 8 on avattu. On tarpeen tunnistaa ne, jotka muutosta tekevät, ja ne, jotka tukevat muutoksen toteutumista (Prosci, 2025).

Kuva 12. Muutoksen roolit (Prosci, 2025)

Muutoksen kohteena on koko organisaatio kohderyhmäkohtaisesti, eli ne keiden tulee muuttaa toimintaansa arjessa. Muutoksen kohderyhmät analysoidaan kattavasti, jotta ymmärretään, miten kyberturvallisuus heidän arjessaan näyttäytyy. Työkaluna voidaan käyttää haastatteluja, joissa kartoitetaan ryhmän arkea, miten heidät tavoittaa ja mikä heitä motivoi, keiden kanssa he keskustelevat, keitä kuuntelevat. Tämän perusteella pystytään vahvistamaan minkälaiset työkalut ja tavat viestiä sekä kouluttaa sopii ryhmälle ja erityisesti sen yksilöille parhaiten.

Muutoksen tekijöiden vastuiden määrittäminen, ei pelkästään projektin kannalta, vaan yleisesti kyberturvallisuuden kannalta, on tärkeä elementti kulttuurin kehittämistä. Kyberturvallisuuden tekniset ja tietoisuuden roolit kuvataan selkeästi, kuka vastaa mistäkin ja millä tavoin. Keneltä voidaan pyytää apua missäkin vaiheessa, kehen toivotaan henkilöstön ottavan yhteyttä ja miten.

Johto, mukaan lukien lähiesihenkilöt, ovat tärkeässä roolissa muutoksen tukijoina. Johto ei kuitenkaan ole ainut, joka voi tukea muutoksen onnistumista. Eri kohderyhmiä pyritään tavoittamaan hyödyntäen jo olemassa olevia tukiverkostoja, kuten lähiesihenkilöitä, sekä luomalla uusia organisaatiolle sopivia verkostoja. Erilaiset muutosagenttiverkostot (Prosci, 2025), esimerkiksi kyberturvallisuusagentit, voivat olla yksilöä lähellä olevia ihmisiä, joilta on helppo kysyä turvallisuudesta ja myös kertoa turvallisuuden huolista. Näitä ryhmiä johdetaan muutoksen tekijöiden toimesta. Ryhmien toiminta on aktiivista ja voi sisältää myös toimintatapojen ja prosessien parantamista. Esimerkki kyberturvallisuuden vastuista on esitelty taulukossa 1.

Taulukko 1. Esimerkki vastuutaulukosta

Rooli muutoksessa	Rooli	Vastuu
Muutoksen tekijä	Kyberturvallisuus-kulttuurin edistäjä	Tietoisuusohjelman ja kulttuurin edistämisen projektipäällikkö. Vastuu kokonaissuunnitelman toteutumisesta. Johtaa muutoksen tukiryhmiä.

Taulukko 1 (jatkuu)

Rooli muutoksessa	Rooli	Vastuu
Muutoksen tekijä	Muutosjohtamisen asiantuntija	Projektipäällikön tuki huomioimassa ihmispuolen muutosta.
Muutoksen tekijä	Kyberturvallisuus-kulttuurin edistäjä	Tietoisuusohjelman ja kulttuurin edistämisen projektipäällikkö. Vastuu kokonaissuunnitelman toteutumisesta. Johtaa muutoksen tukiryhmiä.
Muutoksen tekijä	Muutosjohtamisen asiantuntija	Projektipäällikön tuki huomioimassa ihmispuolen muutosta.
Muutoksen tukija	Johto	Johto omistaa kyberturvallisuuskulttuurin ja tuo sen esiin omana itsenään, korostaen sen merkitystä. Johdon rooli esimerkkinä on vahva, jos johto itse toimii turvallisesti, on todennäköisempää, että myös henkilöstö toimii niin.
Muutoksen tukija	Kyberturvallisuus-agentit	Kyberturvallisuusagentit ovat mielipidevaikuttajia ja aktiivisia tekijöitä organisaation eri puolilla, joiden avulla päästää lähemmäs yksilön arkea. Heidän tehtäväänsä kuuluu muutoksen tekijöiden tuottaman materiaalin ja viestin edistäminen, ja lisäksi vastavuoroisesti viestin välittäminen muutoksen tekijöille organisaation sisältä. Kyberturvallisuusagentit valitaan olemassa olevista tukiryhmistä, mielipidevaikuttajien joukosta tai vapaaehtoisuuteen sekä kiinnostukseen perustuen, huomioiden keitä eri kohderyhmät kuuntelevat.

Taulukko 1 (jatkuu)

Rooli muutoksessa	Rooli	Vastuu
Muutoksen tukija	Lähiesihenkilöt	Useissa organisaatiossa luontevin henkilö kysymyksille on oma lähiesihenkilö. Tästä syystä heidän roolinsa kulttuurimuutoksessa on merkittävä. Rooli on kuin muutosagentin, sovittua viestiä viedään omalle tiimille eteenpäin ja vastavuoroisesti tuodaan muutoksen tekijöille ymmärrystä organisaation henkilöstöltä. Esihenkilö on myös esimerkki, ja kulttuuri vahvistuu parhaiten esimerkkien kautta.
Muutoksen tukija	Teknisen kyberturvallisuuden asiantuntijat	Kyberturvallisuus on myös teknisiä ratkaisuja, ja tässä teknisillä asiantuntijoilla on suuri merkitys. Ei pelkästään teknisen turvan tuottamisessa, vaan myös sen puolestapuhujina, positiivisina äänitorvina turvallisen toiminnan edistämiseksi.
Muutoksen kohde	Koko henkilöstö jaoteltuna kohderyhmiin	Kohderyhmittäin turvallisuus on erilaista eri rooleille. Henkilöstön tehtävänä on omaksua ja myös itse varmistaa, mikä on olennaista oman roolin kannalta. Yrityksessä tehdään töitä yhteisen tavoitteen eteen, ja jokaisen vastuuna on tehdä oma tehtävänsä niin turvallisesti kuin pystyy yrityksen tietoa vaarantamatta.

Organisaatiokulttuuri ja asenneilmapiiri

Yhteisön asenneilmapiiri luo ympäristön, jossa keskustelua käydään. Luukka puhuu ”meidän jutuista”, pienistä yhteisistä tekijöistä, jotka rakentavat yhteisen kulttuurin. Hänen mukaansa uudet jäsenet aina adaptoituvat vallitsevaan kulttuuriin ja tapoihin toimia (2019). Tästä syystä ajatusmallit ja niiden kautta

toimintatavat muuttuvat vain yhteisön kautta. Jotta kriittistäkin keskustelua voidaan käydä rakentavasti, tulee johto ja organisaation mielipidevaikuttajat tunnistaa ja aktivoida kyberturvallisuuskulttuurityöhön. Ennen viestintää ja koulutusta, on hyvä varmistaa, että mahdollisimman positiivinen asenneilmapiiri on olemassa hankkeen suhteen. Mielipidevaikuttajat pyritään saamaan mukaan ohjelman tukiryhmätyöskentelyyn, joten he pääsevät itse vaikuttamaan alusta lähtien sisältöön ja koulutukseen tarvittavalla tasolla.

Johto ja omistajuus

Kuten organisaatiokulttuuri, niin myös kyberturvallisuuskulttuuri tulee sitoa yrityksen syyhyn olla olemassa, visioon ja tavoitetilaan (Luukka, 2019; ENISA, 2023; AlHogail, 2015). Yrityksen visio ja tavoite on yhteinen, ja myös turvallisuusratkaisujen ja sitä seuraavan kyberturvallisuuskulttuurin tehtävä on edesauttaa tavoitteen toteutumista (Liite 2: Haastatellut, 2025). Minkä tahansa muutoksen tavoitetila tulee määritellä yrityksen tavoitetta mukailevaksi, on olennaista perustella ”miksi”, mitä konkreettisesti ollaan tekemässä ja miten (Prosci, 2025).

Johdon roolin merkitys kyberturvallisuuskulttuurissa on suuri niin esimerkkinä kuin turvallisuuden merkityksen vahvistajana (Wright, 2019). Yhteistyö johdon kanssa tulee olla sujuvaa, kyberturvallisuuden tulee olla johdon agendalla ja puheissa, luontevasti. Johdon agendalla oleminen helpottaa resurssien, kuten budjetin ja henkilöstön osallistumisen, mahdollistamista. Miten johto itse haluaa turvallisuutta johtaa? Kyberturvallisuus on liiketoimintaa mahdollistava teema, joten sitä tulee käsitellä strategisena teemana, näin ollen sen omistaa johto (Liite 2: Haastatellut, 2025).

Lopputulos

Suunnitteluvaiheen tuloksena syntyy teknisen kyberturvallisuustietoisuuden suunnitelman lisäksi ihmislähtöisen muutosjohtamisen toimenpiteiden suunnitelma. Suunnitelma keskittyy erityisesti organisaation ihmisiin ja heidän tuntemiseensa. Taustat ja vastaus kysymykseen ”miksi tämä on tärkeää, miksi tätä tehdään” on suunnittelun jälkeen selkeää. Kulttuurin muuttaminen, mitä

kyberturvallisuustietoisuuden ohjelmatkin ovat, on vaikeaa ja hidasta (Luukka, 2019). Sen suunnittelemiseen tulee käyttää aikaa ja resursseja, jotta voidaan varmistua lopputuloksen onnistumisesta. Kyberturvallisuuskulttuuri vahvistuu, kun koko organisaation koko toiminta huomioidaan askel kerrallaan.

5.1.2 Aloita: Tietoisuus ja halu

Ensimmäisessä vaiheessa on tärkeää vain aloittaa, mutta suunnitelmallisesti. Aloittaa voi pienestä, tavoitteena herättää kiinnostusta organisaatiota lähestyttävillä teemoilla. Tukiryhmien ja mielipidevaikuttajien hyödyntäminen alkaa, heidän kauttaan voi herkästi pysyä ajan hermolla organisaation tunnelmasta ja kokemuksesta. Suunniteltua tulee olla valmis muuttamaan kuullun mukaisesti. Koulutusten aika ei ole vielä, liian nopeasti koulutuksiin meneminen ilman ymmärrystä miksi niitä järjestetään, voi aiheuttaa enemmän hämmennystä kuin synnyttää arjen soveltamista (Prosci, 2025). Ajatusmallit muuttuvat hitaasti, ja on olennaista herätellä kiinnostusta ensin, ja kouluttaa vasta sitten kun henkilöstöllä on parempi ymmärrys siitä, miksi heidän tulee joku asia oppia. Yksilöt myös ovat oppimismatkalla eri kohdissa, sisäistäen uutta eri tahdissa, toistaminen on tarpeellista. Kuvassa 13 on nostettu menestystekijöitä ja miten niitä voi huomioida aloita-vaiheessa (Liite 2: Haastatellut, 2025).

Kuva 13. Aloitusvaiheessa huomioitavat menestystekijät

Jatkuvuus

Suunnitelman avaaminen on tärkeässä roolissa, mitä ollaan tekemässä, miten ja miksi. On hyvä nostaa heti esiin, että tämä ei ole yksittäinen harjoitus vaan jatkuvaa toimintaa organisaation perustehtävän saavuttamiseksi. Pakottamisen sijaan hyödynnetään mieluummin positiivisia motivoinnin keinoja, kuten palkitsemista (Prosci, 2025). Palkitseminen on erilaista eri yksilöille. Sitä voi tehdä tiimin sisällä, organisaatiotasolla ja ihan henkilökohtaisesti riippuen mikä juuri tiettyjä yksilöitä motivoi.

Prosessit ja toimintatavat

Aloittamisessa korostuu avoimen keskustelun mahdollistava ilmapiiri. Kysymyksiä toimintatavoista ja prosesseista voi jo nousta, tukiryhmien avustuksella nousseita aiheita kerätään yhteen tulevaisuutta varten. Eri ryhmissä on hyvä käydä jo keskustelua, miten turvallisuus tulee näyttäytymään ryhmän omassa toiminnassa ja minkälaisia muutoksia toimintatapoihin on ehkä edessä.

Osaaminen ja tietoisuus

Aloitusvaiheessa halutaan vastaus kysymykseen ”miten tämä vaikuttaa minuun” (Prosci 2025). Tähän on hyvä pystyä vastaamaan jopa kohderyhmäkohtaisesti, huomioiden roolien toimintatavat ja toimintaympäristö. Kun vastataan kysymyksiin mitä tapahtuu, miten se aiotaan toteuttaa ja miksi näin tehdään, ollaan jo paljon vahvemmalla pohjalla tulevaisuutta varten (Prosci, 2025).

Osaamisen lähtötilanne on hyvä ymmärtää. Tämä voidaan tehdä mittaamalla kokemuksia kohderyhmittäin. Kokemusmittauksella tarkoitetaan yksilön omaa kokemusta aiheen ympäriltä. Kyberturvallisuusagentit voivat olla tässä hyvä tuki lähtötilanteen selvittämiseksi, mutta kyselyn voi tehdä myös kohdennetusti verkkolomakkeilla. Lähtötilanne ja sitä seuraava edistymisen seuranta auttavat suunnittelemaan toimenpiteitä oikein ja kohdennetusti. Mittauksen tulee olla kevyttä, ja mahdollisuus anonyymiyteen annettava. Kokemusväittämien lisäksi annetaan mahdollisuus avoimelle palautteelle yleisesti sekä jokaiselle

väittämälle erikseen. Tärkeintä on tunnistaa mikä tilanne on nyt, mitä henkilöstö on pitänyt hyvänä ja mitä kaivataan lisäksi, sekä osaamisen kehittymisen trendi.

Organisaatiokulttuuri ja asenneilmapiiri

Tukiverkostot on aktivoitu jo suunnitteluvaiheessa, aloita-vaiheessa niiden käyttö alkaa. Käytännön tasolla se tarkoittaa agenttien osallistumista yleiseen keskusteluun, henkilöstön tukemiseen käytäväkeskusteluissa ja toisaalta myös viestin välittämistä muutoksen tekijöiden suuntaan. Tukiverkostoille on annettava riittävä tieto ja ymmärrys tulevasta, jotta he pystyvät vastaamaan henkilöstön kysymyksiin. Aloita-vaiheessa pahin skenaario on se, että asenneilmapiiri kääntyy negatiiviseksi. Sen kääntäminen positiiviseksi vaatii valtavasti toimia ja keskustelua henkilöstön parissa. Tästä syystä kaikki muutoksen roolit ovat aktiivisessa roolissa aloita-vaiheessa, niin johto, teknisen kyberturvallisuuden asiantuntijat, agentit, lähiesihenkilöt kuin muutoksen tekijä -roolitkin. Keskustelulle tulee antaa aikaa. Osallistumalla ja kuultuna henkilöstö on avoimempi muutokselle (Prosci, 2025).

Johto ja omistajuus

Johdon esiintyminen alkuvaiheessa on kriittistä onnistumiselle. Johdon omin sanoin kerrottu tavoite ja toisaalta mandaatti tekemiselle luo ilmapiirin, jossa merkitys ja henkilöstön rooli on helpompi ymmärtää. Ylin johto on antanut lupauksen resurssien käytölle, mutta myös henkilöstön ajankäytölle mitä kyberturvallisuustietoisuuden ohjelma yksilöiltä vaatii. Johdon rooli esimerkkinä on myös merkityksellinen kulttuurimuutoksessa (Luukka, 2019), johdon näkyvyys erityisesti alussa on tärkeää.

Lopputulos

Lopputuloksena on käynnistynyt kyberturvallisuustietoisuuden ohjelma. Tukiryhmien avulla aktiivinen yhteistyö henkilöstön kanssa on alkanut, ja kohdennettuja toimenpiteitä voidaan käynnistää.

5.1.3 Kohdenna: Tiedot, taidot ja innostus

Kohdentamisessa mennään syvemmälle tietoihin ja taitoihin. Kohderyhmillä on erilaisia tarpeita ja kiinnostuksen kohteita, roolit ovat erilaisia ja turvallisuus myös näyttäytyy heille erilaisena. *Kaikki ei kiinnosta kaikkia.* Viesti on hyvä pitää relevanttina, organisaation ja roolin tehtävään sopivana. Kaikki turvallisuustieto ei kosketa juuri tätä organisaatiota, liiallinen ja täysin irrelevantti tieto voi enemmän hämmentää. Ajan hermolla pysyminen on tärkeää, mutta organisaatiota täytyy myös kuunnella ja kuulla. Päivän polttavat asiat eivät välttämättä ole olennaisimpia juuri valitulla hetkellä, organisaatiossa voi olla jotain tärkeämpää menossa. Suunnittelu-vaiheessa sovittu organisaatiolle tuttu terminologia on hyvä pitää mukana kautta linjan. Liian vaikea ja abstrakti sanasto voi johtaa siihen, että viesti ohitetaan. Kohdenna-vaiheessa huomioitavat menestystekijät on avattu taulukkoon 4 (Liite 2: Haastatellut, 2025).

Kuva 14. Kohdenna-vaiheessa huomioitavat menestystekijät

Jatkuvuus

Kyberturvallisuustietoisuuden ohjelma on jatkuva ohjelma ja sitä on hyvä toistaa kautta linjan, sitoa sisältö osaksi kantavaa teemaa, tavoitetta. Pääviestinä voi korostaa mistä ohjelmassa on kyse, miksi sitä tehdään ja miten. Tietoisuuden ohjelman toimenpiteiden kautta herkästi keskustellaan laajemminkin yksittäisestä turvallisuuden aiheesta. Aika ajoin on hyvä muistuttaa, miksi tästä

kaikesta keskustellaan ja mihin juuri tässä organisaatiossa halutaan päästä. Ohjelmalle on määritetty tavoitteet alussa, ja niihin pääsemisestä palkitaan sovituin tavoin.

Prosessit ja toimintatavat

Kun tietoisuuden poluilla päästään pidemmälle, alkaa erilaiset toimimattomat prosessit ja toimintatavat nousta esiin. Kyberturvallisuuden kohdentaminen eri ryhmille tuo nopeasti esiin, että kaikki prosessit eivät tue turvallista toimintaa. Tässä kohden on olennaista kuulla mitä prosesseista ja toimintatavoista kerrotaan, ja olla aktiivisesti valmis muuttamaan niitä oikeiden tahojen kanssa. Ajatusmallit eivät muutu, eikä tietoisuus muutu soveltamiseksi arjessa, jos arki vastustaa niitä.

Osaaminen ja tietoisuus

Ensimmäisessä vaiheessa yleensä aloitetaan yleiskoulutuksilla (ENISA, 2023), mutta kun kohderyhmien arjesta aletaan oppia enemmän ja erilaiset tarpeet nousevat esiin, on myös kohdennetut koulutukset tarpeellisia (Liite 2: Haastatellut, 2025). Kohdennetut koulutukset on suunnattu eri kohderyhmille juuri heidän arkeensa sopivilla teemoilla. Tyypillisesti hyödynnettävät verkkokoulutukset ovat hyviä, mutta yksipuoleisuutensa takia niiden kautta vaikuttaminen pienenee ilman vuorovaikutteisuutta. Hyödyllistä olisi, että vähintään rinnalla olisi mahdollisuus keskustella turvallisuudesta kohdennetusti. Vuorovaikutuksella päästään syvemmälle kohderyhmien arkeen ja turvallisuuden soveltaminen helpottuu. Myös haasteelliset prosessit ja toimintatavat tunnistetaan tätä kautta. Kohdennetut koulutukset luovat huomaamatta turvallisuusmyönteistä henkilöstöä, jotka herkemmin huomaavat turvallisuuspuutteita ja nostavat niitä myös esiin (Liite 2: Haastatellut, 2025).

Vaikuttava toiminta on monipuolista ja monikanavaista, vuorovaikutuksellista. On hyödyllistä hyödyntää eri kanavia, eri tukiryhmiä, ja useita eri ääniä. Vuorovaikutukseen tähtäävä toiminta vahvistaa ymmärtämistä ja soveltamista, kun yhdensuuntainen viesti on helppo ohittaa. Käytettävissä on kattava tukiverkosto johdon edustajia ja tukiryhmiä. Viesti tulee toistaa useita kertoja

ennen kuin se tavoittaa laajasti ja sitä osataan soveltaa arjessa. Pakottaminen harvoin on hyvä tapa tehdä asioita, kannustamalla ja osallistumisesta palkitsemisella pääsee parempiin lopputuloksiin. Lähiesihenkilöt ovat tärkeä kohderyhmä, heillä on yksittäiseen henkilöön luottamussuhde, ja keskustelut käydään luottamuksella.

Mittaamista on hyvä jatkaa ja tehdä tarpeellisia muutoksia palautteen perusteella.

Organisaatiokulttuuri ja asenneilmapiiri

Pääviestin, kaiken toiminnan ja viestinnän tulee olla avointa ja aitoa, näin ollen myös virheistä ja läheltä piti -tilanteista on hyvä kertoa. Syyt ja seuraukset on hyvä avata ketään syyllistämättä. Pelillistäminen on hauskaa, mutta luontaisesti ihmisiä kiinnostaa uusi vain hetken (Liite 2: Haastatellut, 2025). Monipuolisuus ja kohdistuminen omaan arkeen on mielenkiintoisen toiminnan avain. Mitä lähempänä turvallisuusviesti ja -toiminta on omaa arkea ja toimintaa, sen toimivampaa se on. On helpompi muistaa sulkea ovi, kun ymmärtää mitä sen seuraukset voivat olla. Tai muistaa sulkea näyttö, tai kirjautua sovellukseen uudestaan, kun ymmärtää mitä väärinkäytöstä sillä pyritään estämään. Positiivinen ilmapiiri syntyy avoimuudesta, avoimesta keskustelusta ja mahdollisuuksista vaikuttaa.

Johto ja omistajuus

Kyberturvallisuuden edistäminen arjessa, vaaranpaikkojen tunnistaminen ja harjoittelu vie aikaa. Jos sitä ei mahdollisteta ajankäytön puolesta, on todennäköistä, että sitä ei tapahdu. Johdon mandaatilla on tässä suuri merkitys. Kun johto nostaa asian merkittävyyttä ja tärkeyttä, ja myös allokoi aikaa turvallisuuden harjoittelulle, on todennäköisempää, että niin myös tehdään. Johdon toimiminen esimerkkinä ja tukijana vahvistaa turvallisuusmyönteistä ilmapiiriä.

Lopputulos

Kyberturvallisuustietoisuuden koulutukset on alkaneet ja kohdennettuja koulutuksia on voitu jo järjestää kriittisimmille ryhmille. Keskustelu on avointa ja aktiivista turvallisuuden ympärillä, tavoitteet kirkkaasti esitettyjä. Onnistumisista on palkittu henkilöstöä.

5.1.4 Vahvista, arvioi: Jatkuvaa, mitattua ja juurtunutta

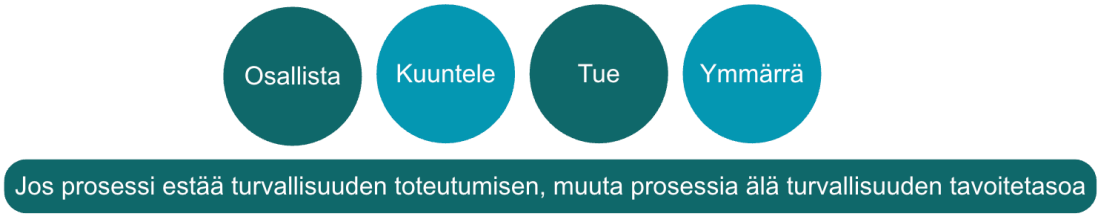
Juurtumisen vaihe on kulttuurimuutoksessa kaikkein olennaisin (Luukka, 2019). Kulttuurimuutos on hidasta ja on luonnollista, että kyllästyminen uusiin teemoihin on mahdollista (Prosci, 2025). Tässä kohdassa alun innostus on laskenut, ja herkästi palataan vanhoihin toimintatapoihin. Lisäkoulutukset ja nostot ovat juurruttamisen vahvistamista. Jo tapahtunutta muutosta on tärkeää juhlia, korostaa miten pitkälle organisaationa on päästy. Viesti ja toimenpiteet on hyvä pitää monipuolisena, kohdaten yksilön edelleen monia eri reittejä, pysyen mielenkiintoisena. Palkitsemisen vaikutus on suuri motivoinnissa, ja kohderyhmäanalyysin perusteella on ymmärrys mitä se eri kohderyhmissä tarkoittaa. Toiselle palkitseminen voi olla oman nimen korostaminen aktiivisena keskustelijana ja turvallisuuden esille nostajana. Toiselle palkitseminen tarkoittaa elokuvalippuja onnistuneen uhan estämisestä. Luukan puhumaan yhteisön merkityksen on pidettävä mielessä myös juurtumisen kohdassa (2019). Positiivisen asenneilmapiirin vahvistaminen turvallisuutta kohtaan on jatkuvasti tärkeässä asemassa.

Vahvista ja arvioi -vaiheessa huomioitavat menestystekijät on kuvattu kuvaan 15 (Liite 2: Haastatellut, 2025). Juurtumisen vaiheessa keskitytään erityisesti onnistumisista juhlimiseen ja toisaalta jatkuvuuden vahvistamiseen.

Kuva 15. Vahvista ja arvioi -vaiheessa huomioitavat menestystekijät

Jatkuvuus

Kyberturvallisuuskulttuurin kehittäminen on jatkuvaa toimintaa. Kyberturvallisuus ja turvallisuuskenttä muuttuu nopeasti, näin ollen myös tietoisuuden ohjelman ja organisaation koko toiminnan täytyy kehittyä ja pysyä ajan hermolla (kuva 16). Turvallisuusorientuneessa organisaatiossa ihmisen rooli ymmärretään turvallisuuden tekijänä ja kyberturvallisuuskulttuurin kehittäminen nähdään strategisena jatkuvana turvallisuuskeskusteluna henkilöstön kanssa. Haasteiden kohdalla on parempi muuttaa prosesseja turvallisemmaksi kuin laskea yhdessä määriteltyä turvallisuuden tavoitetasoa. Onnistumisista tulee juhlia, olla tyytyväinen jo tehdystä, vaikka muutosmatka onkin pitkä.



Kuva 16. Kyberturvallisuuskulttuurin kehittäminen on jatkuvaa

Prosessit ja toimintatavat

Tietoisuuden ohjelmaa laajennetaan pala kerrallaan, aina seuraaviin ja seuraaviin kohderyhmiin ja toimintoihin. Laajentaminen tuo mukanaan uusia prosesseja ja toimintatapoja, joita tulee aktiivisesti tarkastella turvallisuuden näkökulmasta.

Osaaminen ja tietoisuus

Tietoisuuden ohjelman täytyy olla valmis muuttumaan ja muuttamaan organisaatiota sisältäpäin. Kohdennettu mittaaminen on hyvä jatkua säännöllisesti, koska vain sitä kautta voidaan pysyä kartalla koko organisaation toiminnasta ja tehdä tai muuttaa toimenpiteitä siellä missä tarvitaan, palautteen mukaisesti (Liite 2: Haastatellut, 2025).

Organisaatiokulttuuri ja asenneilmapiiri

Kyllästyminen on pitkässä ohjelmassa luonnollista. Jotta keskustelu ja toimenpiteet pysyvät organisaation ajan hermolla, tulee herkästi myös kuunnella organisaation toiveita ja olla valmis muuttumaan. Johdolla on merkityksellinen rooli pitkän ohjelman pysymisessä keskusteluissa mukana.

Johto ja omistajuus

Tavoitteellisuuden muistuttaminen vahvistaa juurtumista. Muistuttaminen siitä, miksi ohjelma on käynnissä ja mikä jokaisen rooli sen onnistumisessa on. Johto korostaa turvallisuuden merkitystä omalla esimerkillään ja pitämällä aihetta aktiivisesti omassa viestinnässään mukana. Onnistumisista juhliminen on myös johdon agendalla. Tällä korostetaan sitä, että vastuu ei ole kyberturvallisuusasiantuntijoiden tai -tietoisuuden asiantuntijoiden tehtävä, vaan kaikkien.

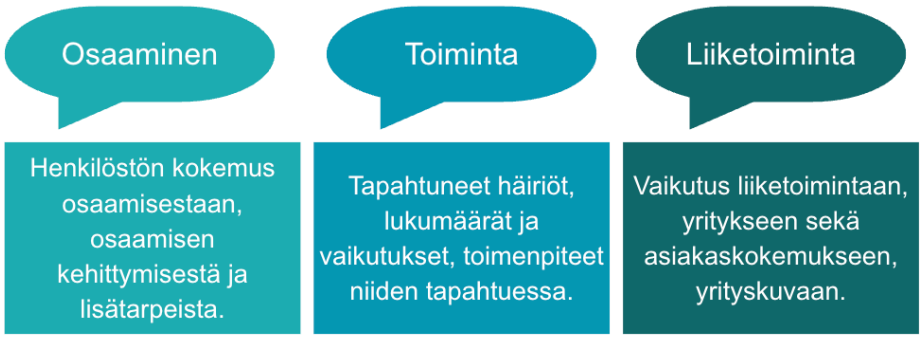
Lopputulos

Kyberturvallisuustietoisuuden ohjelma on käynnissä ja kyberturvallisuuskulttuuri vahvistuu askel kerrallaan. Toimintatavat ja prosessit muuttuvat turvallisemmiksi sitä mukaa, mitä laajemmalle ohjelma leviää. Ohjelma pysyy ajan hermolla ja

muuttuu organisaation mukana. Tietoisuutta ja osaamisen kehittymistä mitataan, ja muutetaan palautteen perusteella. Ohjelman vaikutusta organisaation toimintaan mitataan liiketoiminnan mahdollistajana ja toiminnan muutoksen kautta.

5.2 Kyberturvallisuuskulttuurin mittaaminen

Mittaaminen nostetaan esiin niin muutosjohtamisen kuin kyberturvallisuustietoisuuden ohjelmien toteutumisen kannalta merkityksellisenä seikkana (Prosci, 2025; ENISA, 2023). Vain mittaamalla voi todentaa, että muutosta on tapahtunut. Yrityskulttuurin mittaaminen ei ole yksiselitteistä (Luukka, 2019) ja kyberturvallisuuskulttuurin mittaaminen vielä vähemmän (Liite 2: Haastatellut, 2025). Kokemusta kuitenkin voidaan mitata, toimenpiteiden vaikutusta turvallisuuteen samoin. Mittaaminen lähtee liikkeelle siitä, mitä on tavoiteltu. Jos on tavoiteltu, että tapahtumista (esimerkiksi huijausviesteistä) kuullaan nopeammin, mitataan aikaa, kuinka nopeasti viesti saavuttaa kyberturvallisuuden asiantuntijat. Jos taas sitä, että varkauksia ei tapahdu, tai asiattomia ei löydy käytävistä tai uhkatilanteisiin osataan vastata oikein, mitataan näitä. On hyvä huomioida, että tulokseksi saa juuri sitä mitä mittaa, joten mittaamisen äärelle on hyvä pysähtyä rauhassa ja pohtia mitä todella halutaan saavuttaa, ja millä mittareilla se pystytään todentamaan. Mittaamisen voi jaotella kolmeen osa-alueeseen: osaamiseen, toimintaan ja liiketoimintavaikutukseen (kuva 17). Osaamisen mittarit keskittyvät henkilöstön osaamiseen, toimintamittarit tapahtuneeseen muutokseen toiminnassa ja liiketoimintavaikutusmittarit kahden ensimmäisen vaikutuksesta liiketoimintaan.



Kuva 17. Mittaamisen kolmijaottelu

5.2.1 Osaaminen

Osaamisen mittaamista voidaan toteuttaa erilaisin testein ja kokemusmittauksin. Yrityksen kyberturvallisuustietoisuuden kurssit usein sisältävät lopputentit, joiden onnistumisprosentteja voidaan seurata ja jopa palkita korkeista arvosanoista. Tentit ovat kuitenkin vain yksi ulottuvuus osaamista. Toinen ulottuvuus on kokemus osaamisesta. Kokemusmittauksella voidaan mitata henkilöstön omaa arviota osaamisestaan, sen kehittymistä ja samalla tunnistaa lisätarpeita. Kokonaisuutena tämä on pitkässä matkassa vahvempi trendi. Vaikeiden tai tuntemattomien asioiden, kuten kyberturvallisuuden, osaamisen arvioiminen itse on usein vaikeaa. On luonnollista, että ensivaiheessa oma osaaminen arvioidaan turhan korkeaksi. Vasta opitun myötä ymmärretään, miten vähän vasta tiedetään. Kun mittaamista tehdään säännöllisesti ja pitkäkestoisesti, trendi kuitenkin tulee olemaan ylöspäin.

Kokemusmittaus on arvokas työkalu arvioimaan tarvittavia toimenpiteitä tai lisäkoulutustarpeita. Kokemusmittauksissa on hyvä olla tilaa palautteelle ja toiveille. Mittausta voidaan toistaa esimerkiksi kahden kuukauden välein. Hyviä väittämiä kokemusmittaukseen voi olla esimerkiksi:

- Ymmärrän kyberturvallisuuden merkityksen organisaatiolleni
- Ymmärrän kyberturvallisuuden merkityksen omassa työssäni
- Löydän tarvittavan tiedon, jotta pystyn työskentelemään turvallisesti
- Tiedän keneltä saan apua kyberturvallisuuden kysymyksissä

- Toimintatapamme ja prosessimme tukevat kyberturvallista työskentelyä

Mahdollisia osaamisen mittareita:

- Koulutusten suorittaminen (tavoite 100 %)
- Tenttien arvosanat (tavoite nouseva)
- Kokemusmittaus (tavoite nouseva)

5.2.2 Toiminta

Toiminnan muuttumisen mittaus riippuu suuresti siitä, mitä yrityksen kyberturvallisuuskulttuurilla halutaan tapahtuvan. Jos sillä halutaan lisää ilmoituksia tai kiinnostusta turvallisuuteen, niin silloin haetaan nousevia ilmoituslukuja. Jos taas halutaan vähemmän toteutuneita uhkia, niin silloin seurataan niitä. Yrityksen ja kyberturvallisuustietoisuuden tavoitteet määrittelevät voimakkaasti sen mitä toimintaa halutaan mitata. Turvallisuusviestintää tai toimintaa seuraavien määrää voidaan myös seurata, se toki on toiminnallisesti heikko mittari, vaikka kuvaakin kiinnostuneiden määrää niin seuraaminen ei vielä takaa sisäistämistä. Mahdollisia toiminnan mittareita:

- Häiriöilmoitusten määrä (nouseva tai laskeva tavoitteiden mukaisesti)
- Toteutuneet uhat (tavoite laskeva)
- Toimenpiteiden kesto tapahtuneen jälkeen (laskeva, eri kriittisyyden tasot)
- Viestintää seuraavien määrä (tavoite nouseva)

5.2.3 Liiketoimintavaikutus

Kaikille yrityksille yhteinen mittari on liiketoimintavaikutus. Kyberturvallisuuden häiriöt saattavat aiheuttaa yrityksille mittavia vahinkoja, joita voidaan mitata ajassa ja rahassa. Vaikutusten trendin halutaan olevan laskeva. Liiketoimintavaikutuksiin yhdistyy myös yrityskuvan vaikutukset esimerkiksi

toteutuneiden uhkien seurauksena, miten yritys on käsitellyt toteutuneen uhan jälkitoimet. Samoin asiakaskokemus ja asiakkaiden kiinnostus kyberturvallisuuden toimenpiteitä kohtaan indikoi liiketoimintavaikutusta.

Mahdollisia liiketoimintavaikutuksen mittareita:

- Toteutuneiden uhkien aiheuttamat vahingot, euroissa ja hukatussa ajassa (tavoite laskeva)
- Yrityskuvan muutokset toteutuneen uhan jälkeen (tavoite nouseva)
- Asiakaskokemus, kyberturvaan liittyvät kyselyt (tavoite laskeva)
- Asiakaskokemus, yrityskuva kyberturvallisena yrityksenä (tavoite nouseva)

6 Yhteenveto

Tämän työn tavoite oli keskittyä erityisesti ihmisen rooliin kyberturvallisuudessa. Siihen miten henkilöstön ajatusmallit ja toiminta voidaan muuntaa kyberturvatietoisuudeksi ja vielä pidemmälle, kyberturvallisen arjen teoiksi. Tätä tarkasteltiin siltä kulmalta, miten muutosjohtaminen keinoilla voidaan luoda ja johtaa kyberturvallisuuskulttuuria siten, että tiedon ja organisaation turvaaminen voidaan kääntää innostavaksi ja positiiviseksi mahdollisuudeksi, jossa henkilöstö haluaa toimia turvallisesti. Tätä pohjustaen perehdyttiin myös kyberturvallisuuskulttuurin toteutumisen haasteisiin sekä menestystekijöihin ja toimialan vaikutukseen.

6.1 Kyberturvallisuus ja sitä tukeva kulttuuri

Kyberturvallisuus on kompleksinen ja jopa abstrakti, vaikeasti hahmotettava kokonaisuus. Laajuus ja sisältö vaihtelee sen mukaisesti, keneltä aiheesta kysyy ja missä ympäristössä toimitaan. Tästä syystä kyberturvallisuus myös tuo mukanaan aina uutta ja erilaista tarkasteltavaa. Kyberturvallisuus on kiinteä osa organisaation kokonaisturvallisuutta. Fyysisesti avoin ovi ja esille unohdettu tietokone avaavat aivan liian helposti tietä väärinkäytökselle. Fyysisen uhan torjuminen turvattomalla digitaalisella ratkaisulla vaikuttaa koko organisaation turvallisuuteen. Yksittäisten uhkien listaamisen sijaan yksilön on tärkeä ymmärtää, miksi säännöt ovat olemassa ja mitä varsinaisesti halutaan saavuttaa. Yrityksen tavoitteisiin, arvoihin ja perustehtävään sidottu kyberturvallisuuskulttuuri on aina vahvempi, kuin pakotettu sääntöjen noudattaminen. Johdon vahva esimerkki omana itsenään ja tuki kyberturvallisuudelle sekä sitä tukevalle kulttuurille on avainasemassa. Mikään muutos ei tapahdu, jos on nähtävissä, että johtokaan ei sen takana seiso.

Kyberturvallisuus on kokonaisvaltaista. Jos jokin turvallisuusohjeistus ohitetaan useasti, on syy todennäköisesti prosesseissa ja toimintatavoissa, jotka eivät mahdollista tai monimutkaistavat turvallisen toiminnan. Kun asia on liian

monimutkainen, se herkästi jätetään tekemättä. Kyberturvallisuuden katsominen siis pelkästään teknisestä näkökulmasta on yksipuolista. Tietoisuuden ohjelmat eivät myöskään voi olla vain viestintää ja koulutusta, joissa korostetaan turvallisuuden merkitystä, jos turvallisesti toimiminen arjessa ei ole mahdollista tai on suhteettoman hankalaa.

Kyberturvallisuustietoisuuden malleja on lukuisia, ja niiden hyödyntäminen aktiivista. Kyberturvallisuus tunnistetaan kulttuurisena käsitteenä, sen ymmärretään olevan vahvasti riippuvaa yksilön ja yhteisön toiminnasta. On kuitenkin todettava, että tietoisuus on vasta ensimmäinen askel. Valittu tietoisuuden malli ei siis ole se avain kyberturvallisuuskulttuurin toteutumiseen, vaan se miten sitä mallia sovelletaan käytännössä, miten sillä onnistutaan muuttamaan tapaa ajatella ja toimia. Avoin keskustelu turvallisuudesta ja riskeistä auttaa tunnistamaan, mitä ongelmaa halutaan tosiasiallisesti ratkaista. Ilman avointa keskustelua voidaan helposti kohdistaa toimenpiteet väärin ja päätyä korjaamaan ongelmia, jotka eivät ole ydinhaaste.

Toimialojen välillä ja organisaatioiden välillä on eroja. Perusliiketoiminta ja regulaatiot ohjaavat kyberturvallisuuden tavoitetasoa. Toimialan kypsyys, riskinsietokyky sekä suojattavan tiedon laatu vaikuttavat panostuksiin. Organisaatioissa tulee tunnistaa omalle toimialalle, omaan riskitasoon ja omaan organisaation sopiva kyberturvallisuustietoisuuden malli ja tehdä siitä itselleen sopiva.

6.2 Kyberturvallisuuskulttuurin kehittäminen muutosjohtamisen keinoilla

Kyberturvallisuuskulttuurin kehittäminen on organisaatiokulttuurin kehittämistä. Organisaatiokulttuurilla tarkoitetaan sitä, mitä tapahtuu kuin kukaan ei katso. Hyvä organisaatiokulttuuri on sidottu yrityksen visioon ja tavoitteisiin, se on elementti, jota voi kehittää ja vahvistaa (Luukka, 2019). Kehitys vaatii järjestelmällistä toimintaa, ja muutos onnistuu vasta kun se realisoituu yksilötasolla (Prosci, 2025). Muutos vaatii aktiivista työtä vanhojen tapojen murtamiseksi, uuden työskentelytavan omaksumiseksi ja juurruttamiseksi

(Tienari & Meriläinen, 2012). Muutosjohtamisessa keskitytään erityisesti ihmisten ja yksilön asenteiden ja toiminnan muutokseen (Murthy, 2007).

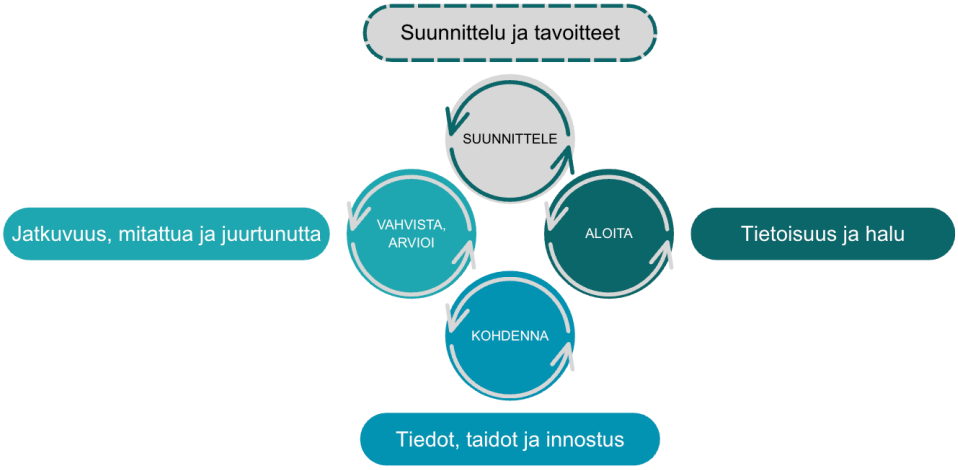
Tässä tutkimuksessa tunnistettiin kyberturvallisuuskulttuurin mahdollistavia tekijöitä sekä yksilön, organisaation kuin ulkopuolisenkin maailman vaikutuksia. Kyberturvallisuuskulttuurin mahdollistavat menestystekijät ovat toimialasta riippumatta samat kaikille:

- Johdon sitoutuneisuus ja omistajuus: Johdon aktiivinen osallistuminen kyberturvallisuuskulttuuriin ja sen merkityksen korostamiseen.
- Positiivinen asenneilmapiiri turvallisuutta kohtaan sekä avoimen keskustelun mahdollistava organisaatiokulttuuri: Ympäristö, jossa saa kysyä ja kysyvää autetaan.
- Henkilöstön osaamisen ja tietoisuuden kehittyminen: Kohdennettua osaamisen ja tietoisuuden kehittämistä, sovellettuna yksilön arkeen.
- Turvallisuuden merkitys jatkuvana toimintana ja liiketoiminnan mahdollistajana: Ei vain kertaluontoinen harjoitus, vaan jatkuvaa toimintaa, strategisesti ja tavoitteellisesti tärkeä liiketoiminnan mahdollistaja.

Ihmislähtöinen muutosjohtaminen keskittyy yksilöön osana yhteisöä ja sen avulla voidaan saada heräteltyä organisaatio yhdestä työntekijästä lähtöisin tunnistamaan oma roolinsa kyberturvallisuudessa. Yksilön ajatusmalleihin ja motivaatioihin keskittymällä voidaan vaikuttaa tapaan toimia ja sitä kautta koko organisaation turvallisuuteen. Erityisesti kulttuurimuutoksessa jokaisella yksittäisellä ihmisellä on suuri merkitys yhteisön osana. Muutosjohtamisen ja kyberturvallisuustietoisuuden ohjelman yhdistämisellä voisi olla positiivinen vaikutus kyberturvallisuustietoisuuden juurtumiseksi kyberturvallisuuskulttuuriksi.

Tässä työssä esitelty soveltava malli on kuin liima muutosjohtamisen ja kyberturvallisuustietoisuuden mallien välissä. Mallissa nostetaan esiin mitä asioita vahvistamalla voi tarttua niihin haasteisiin joihin kyberturvallisuuden

kohdalla usein törmätään (Liite 2: Haastatellut, 2025). Malli koostui neljästä vaiheesta: suunnittele, aloita, kohdenna sekä vahvista ja arvioi (kuva 18).



Kuva 18. Kyberturvallisuuskulttuurin kehittäminen muutosjohtamisen menetelmillä, päävaiheet

6.2.1 Suunnittele

Työ alkaa hyvästä suunnittelusta, jossa johto aktiivisesti sitoutuu yhdessä tekemään töitä kyberturvallisuuden eteen. Yhdessä valitaan toimiala ja organisaation erityispiirteet huomioiden kyberturvallisuustietoisuuden malli sekä määritellään sille tavoitteet organisaation riskikartoitus huomioiden. Vastuut vahvistetaan tietoisuuden ja teknisen kyberturvallisuuden kannalta. Organisaatiosta tunnistetaan ne ryhmät, jotka voivat tukea muutoksessa sekä keitä muutos tulee koskemaan. Kohdennusta tarvitaan kyberturvallisuudessa paljon, jotta arjen soveltaminen on mahdollista, joten kohderyhmien tunnistamiseen ja niiden erityispiirteisiin ja tukiryhmiin on hyvä käyttää aikaa. Suunnitteluvaiheessa käydään aktiivista keskustelua tukiryhmien kanssa kyberturvallisuuden merkityksestä ja mallin jatkuvaluonteisuudesta. Kyberturvallisuustietoisuus ei ole yksi koulutus kerran vuodessa.

6.2.2 Aloita

Paras tietoisuuden ohjelma on aloitettu ohjelma. Mutta sekin on tehtävä suunnitelmallisesti ja perustellusti. Pelkkä tietoisuuskoulutus ei johda vielä mihinkään, jos ei kokonaisuutta ja merkitystä ymmärretä. Ensimmäisessä vaiheessa tärkeää on herättää mielenkiintoa, nostaa esille hyötyjä. Kaikessa keskustelussa nousee esiin mitä ollaan tekemässä ja miksi sekä miten se vaikuttaa yksilöön ja yksilön arkeen. Mitä odotuksia henkilöstölle asetetaan ja miksi. Avoin keskustelu luo positiivista ilmapiiriä, jossa jokaisella on mahdollisuus vaikuttaa. Johto toimii aktiivisesti esimerkkinä ja mahdollistajana. Tukiryhmät ovat yksilöille läsnä, ja toistavat viestiä ja luovat tilaa keskustelulle. Vuorovaikutteisuus on tärkeää, mallia on mahdollista muuttaa palautteen perusteella.

6.2.3 Kohdenna

Kun ymmärrys tietoisuudesta on luotu, voidaan jatkaa kohdennettuun viestintään ja koulutukseen, jossa tarkoituksena on viedä konkretian tasolle se mitä yksilöltä odotetaan. Kaikki toimintatavat ei välttämättä taivu turvalliseen toimintaan, joten kun niitä tunnistetaan, prosessit muuttuvat, turvallisuudentaso ei. Aktiivinen ja avoin keskustelu turvallisuudesta pysyy yllä niin johdon kuin tukiryhmienkin avulla. Johdolla on myös tärkeä rooli ajankäytön mahdollistajana. Harjoittelu ja kouluttautuminen vie henkilöstöltä aikaa. Tavoitteet on alussa määritelty ja kun niitä saavutetaan, onnistumisesta myös palkitaan.

6.2.4 Vahvista ja arvioi

Kulttuurimuutoksessa juurtumisen vaihe on tärkein vaihe. On helppoa siirtyä takaisin vanhoihin tapoihin ja tottumuksiin. Pääviestin korostaminen ja vahvistaminen eri keinoin ja eri henkilöiden sanomana vahvistaa muutoksen toteutumista. Ohjelman aikana henkilöstö on oppinut jo paljon, opitun

vahvistaminen ja arkeen sitominen auttaa juurtumisessa. Johdolla on edelleen tärkeä rooli korostaessa tavoitteiden toteutumista sekä jatkuvuutta, samoin tukiryhmillä. Vuorovaikutteisuus tässäkin vaiheessa auttaa muutoksen aktiivisia tekijöitä tunnistamaan minkälaisia toimenpiteitä tarvitaan ja missä. Muutosta on mitattu läpi ohjelman toteutuksen, niin henkilöstön kokemuksen, toiminnan kuin liiketoimintavaikutusten kautta. Onnistumisesta on tärkeää palkita sekä yksilöitä ja koko organisaatiota.

Kyberturvallisuuskulttuurityö on pitkäkestoista ja jatkuvaa työtä, jossa tulokset voivat tapahtua pitkänkin ajan päästä. Taikatemppuja kyberturvallisuuskulttuuriin luomiseksi ei ole olemassa, hyvällä ja tavoitteisiin perustuvalla mittauksella voidaan seurata kulttuurin toteutumista ja muuttumista ja juhlia onnistumisia.

Ihmisten toiminta ei säännönmukaisesti ole tahallisesti vaarallista, mutta sekin on mahdollista. Hyvällä jatkuvalla muutosjohtamisella ja -viestinnällä kaikessa toiminnassa luodaan organisaatioon luottavainen ja avoin tunnelma, jossa yksilön henkilökohtaiset haasteet tai organisaation vaikeat tilanteet eivät vaikuta negatiivisesti henkilöstön toimintaan. Avoimessa ja yksilöä arvostavassa yleisilmapiirissä yksilö ei haasteellisillakaan hetkillä koe tarvetta haitalliselle toiminnalle.

7 Tutkimuksen arviointi

Kyberturvallisuus on muuttuvassa maailmassa ajankohtainen ja tärkeä aihe. Paljon on kiinni teknisistä ratkaisuista ja teknisistä kykeneväisyyksistä, mutta kyse on myös ihmisestä. Ihmisellä on rooli niin kyberturvallisuusuhan kohteena kuin tekijänä. Ideaalitilanteessa tekniset ratkaisut pystyisivät torjumaan uhan kuin uhan, mutta reaalimaailmassa näin ei ole. Tämän takia kyberturvallisuustietoisuudella ja kyberturvallisuuskulttuurilla globaalilla tasolla on kasvava merkitys. Tekoälyn aikakaudellakin ihmisen toiminta ja ihmisen rooli teknisessä maailmassa nousee ajankohtaiseksi teemaksi. Kyberturvallisuuden ymmärtäminen ja soveltaminen käytännössä kohoaa merkitykselliseksi taidoksi.

7.1 Tutkimuksen luotettavuus

Tutkimuksen luotettavuus laadullisessa tutkimuksessa pohjautuu prosessin luotettavuuteen. Aineistoa voidaan arvioida kolmelta kantilta:

- Merkittävyys
- Aineiston riittävyys ja analyysin kattavuus
- Analyysin arvioitavuus ja toistettavuus

Reliaabeli tulkinta aineistosta tarkoittaa sitä, että aineisto ei sisällä ristiriitaisuuksia. Tätä voidaan saavuttaa kysymällä esimerkiksi samaa asiaa kahdesti, hieman eri sanoin, tai useammalla havainnoijalla. (Eskola & Suoranta, 1998.)

7.1.1 Merkittävyys

Merkittävyys voi olla suhteellinen asia (Eskola & Suoranta, 1998). Tässä tutkimuksessa merkittävyys tarkoitti osaamista, erityistä kiinnostusta ja kokemusta tutkimuskysymysten teemoista. Haastattelukysymykset kirjoitettiin tutkimuskysymysten pohjalta, jotta saavutetaan mahdollisimman merkittävä tulos tavoitteisiin nähden. Lisäksi haastateltavat valittiin laaja-alaista kokemusta

korostaen, eri rooleja ja toimialoja painottaen. Tekninen ja vuosikymmenten aikana kasvanut kokemus saavutettiin tietoturva-asiantuntijoilta ja toisaalta vielä erityisesti ihmispuolen näkemykset muutosjohtajilta. Johdon edustajat eroteltiin vielä asiantuntijoista, jotta eriytyvät näkemykset saadaan tunnistettua ja hyödynnettyä.

Haastattelututkimus perustui etukäteen laadittuun haastattelurunkoon, ja kaikille haastateltaville esitettiin samat kysymykset. Muutosjohtamisen asiantuntijoille oli muutama lisäkysymys ja toisaalta jotain teknisempiä ei kysytty. Englanninkielinen lomake oli haastateltavan (Liite 2: Asiantuntija 6) ajankäytöllisistä syistä lyhyempi. Kysymykset perustuivat kaikissa haastatteluissa tutkimuskysymyksiin.

7.1.2 Aineiston riittävyys ja analyysin kattavuus

Laadullisessa tutkimuksessa aineiston riittävyyttä voi olla haasteellista laskea etukäteen, aineisto enemmän itse kertoo, koska sitä on tarpeeksi (Eskola & Suoranta, 1998). Tässä tutkimuksessa saturaatiopiste oli tunnistettavissa aikaisessa vaiheessa, kun samat teemat alkoivat toistua haastatteluissa. Näin ollen haastateltujen lisääminen olisi voinut tuoda jotain yksittäisiä uusia näkemyksiä, mutta isossa kuvassa tieto oli riittävä tämän työn tuloksia ja rajausta ajatellen.

Vaikka tämän työn edellytykset täyttyivät haastattelujen pohjalta, on otos kuitenkin pieni, ja sillä voi olla vaikutusta yleistettävyyteen. On myös tunnistettava, että muutosjohtamisen ja kyberturvallisuuskulttuurin asiantuntijana kirjoittajalla on voinut olla ennakko-oletuksia, jotka ovat ohjanneet keskusteluita.

Haastatteluja ei saanut tietosuojasyistä tallentaa eikä automaattisesti litteroida, joten käsin dokumentoidessa jotain voi aina jäädä huomioimatta. Haastatteluissa pyrittiin kuitenkin saamaan enemmän laajoja teemoja kuin yksityiskohtia esiin, joten mahdollisuus suurille tulkintavirheille on pieni.

Muutosjohtamisen asiantuntija on validoinut kehitetyn mallin, ja mallia on edelleen kehitetty hänen kommenttiensa pohjalta. Tietoturvanäkemyksen olisi voinut saada vielä valitsemalla lisäksi tietoturva-asiantuntijan validoimaan mallia, mutta keskittyminen muutosjohtajuuteen ja sen menetelmiin ohjasi valintaa.

7.1.3 Analyysin arvioitavuus ja toistettavuus

Arvioitavuudella tarkoitetaan sitä, että tutkijan ajattelua ja päättelyä pystytään seuraamaan työn edetessä. Toistettavuus taas sitä, että toinen tutkija voisi samalla aineistolla päätyä samoihin johtopäätöksiin. (Eskola & Suoranta, 1998.)

Tämä työ on pyritty rakentamaan loogisesti edeten teorian kautta tutkimustuloksiin ja löydöksiin, sekä näitä yhdistelmänä rakennettuun malliin. Tutkimus on rajattu tarkasti, tähdäten koko ajan tutkimuskysymyksissä esiteltyihin lopputuotoksiin. Löydökset ja lopputuotokset on kirjattu mahdollisimman selkeisiin osioihin. Haastattelukysymykset ja tutkimuskysymykset tähtäsivät jo selkeisiin osioihin. Näin ollen tulosten toistettavuus voisi olla mahdollista. Tulkinta ja terminologia perustuu kuitenkin tutkijan subjektiiviseen kokemukseen ja työn aikana kasvaneeseen osaamiseen muutosjohtamisesta kyberturvallisuuskulttuurin alueella.

7.1.4 Eettisyys

Haastattelututkimusta varten jokaiselta haastateltavalta pyydettiin etukäteen suostumus haastatteluun, haastattelupyyntö on avattu liitteessä 3. Taustaksi kerrottiin mihin haastattelujen löydöksiä hyödynnetään ja miten. Opinnäytetyöprosessi avattiin laajemmin, mihin koulutukseen työ liittyy ja miten se julkaistaan. Tallennuksesta ja litteroinnista kysyttiin parilta ensimmäisiltä, ja vastauksen ollessa kielteinen, päädyttiin loppujen osalta siihen, että kerrottiin suoraan, ettei haastatteluja tallennettu eikä automaattisesti litteroitu. Se

osoittautui muutenkin hyväksi ratkaisuksi, koska haastateltavat puhuivat todennäköisesti paljon vapaammin, kun tiesivät ettei heitä tallenneta.

Haastateltaviin viitataan kaikissa kohdissa anonyyminä, erotettuna vain rooleittain ja toimialoittain liitteessä 2. Kaikki dokumentaatio on tallennettu vain tutkijan käyttöön ja anonymisoituna. Nimellä viitatun asiantuntijan kommentit on faktatarkistettu haastateltavalla. Dokumentaatio hävitetään, kun työ on valmis.

7.1.5 Tekoälyn hyödyntäminen

Työn toteutuksessa on hyödynnetty tekoälyä tiedonhaussa ja tiivistelmän tekstinmuotoilussa. Analyysissä ei hyödynnetty tekoälyä. Työkaluina on käytetty työn alkuvaiheessa OpenAI:n ChatGPT:tä ja loppuvaiheessa Anthropicin Claudea.

7.2 Työn arviointi

Tässä työssä keskityttiin erityisesti ihmisen rooliin kyberturvallisuudessa. Siihen miten henkilöstön ajatusmallit ja toiminta voidaan muuntaa kyberturvatietoisuudeksi ja vielä pidemmälle, kyberturvallisen arjen teoiksi. Työssä tutkittiin, miten muutosjohtamisen käytännönläheisillä keinoilla voidaan luoda ja johtaa kyberturvallisuuskulttuuria siten, että tiedon ja organisaation turvaaminen voidaan kääntää innostavaksi ja positiiviseksi mahdollisuudeksi. Tutkimuksessa myös tarkasteltiin toimialoja ja niiden eroavaisuuksia, sekä mitkä menestystekijät onnistuneessa kyberturvallisuuskulttuurissa toteutuu.

Tutkimusongelma oli, voiko muutosjohtamisen ja sen käytännönläheiset työkalut olla työväline laajentaa olemassa oleva organisaatiokulttuuri kyberturvallisuuden huomioivaksi kulttuuriksi, jossa myös ajattelutavat muuttuvat kyberturvallisemmaksi?

Tukevia tutkimuskysymyksiä olivat, mitkä ovat keskeiset kulttuuriset haasteet ja menestystekijät kyberturvallisuuskulttuurin kehittämisessä sekä miten toimiala vaikuttaa kyberturvallisuuskulttuuriin?

Tutkimuksen hypoteesi oli, että vaikka kyberturvallisuustietoisuuden malleja on paljon, niiden käytännön soveltaminen on haasteellista, eikä niiden käyttöönotto takaa onnistunutta kyberturvallisuuskulttuuria. Johdon sitoutuminen, arjen prosessit ja ihmisten asenteet sekä pelot turvallisuutta kohden estävät kyberturvallisuuskulttuurin toteutumisen. Toimialoittain on eroavaisuuksia, toisilla suhtautuminen sääntöihin ja niiden noudattamiseen on luontevampaa kuin toisilla. Muutosjohtamisen ihmislähtöisillä työkaluilla kyberturvallisuusymmärrys voidaan tuoda lähelle yksilöä ja ymmärryksen kautta juurruttaa kyberturvallisuus osaksi organisaatiokulttuuria, ihmisten arvoja ja ajatusmalleja.

7.2.1 Tavoitteiden saavuttaminen

Tavoitteena oli tutkia muutosjohtamisen menetelmien hyödynnettävyyttä kyberturvallisuuskulttuurin vahvistamisessa. Tutkimuskysymyksiin pystyttiin tutkimuksen perusteella vastaamaan ja esitelty malli on hyödynnettävissä hypoteesin mukaisesti.

Asiantuntijahaastattelut toivat avartavia käytännön kokemuksia turvallisuuden kannalta. Haastateltavilla oli niin laaja, monipuolinen kokemus, että materiaalia syntyi työstettäväksi runsaasti. Yhteneväisyyksiä löytyi huomattavan aikaisessa vaiheessa, ja esiin nousi voimakkaasti sellaisia teemoja esiin, joihin muutosjohtamisen ajattelutapa, mallit ja hyödynnettävät menetelmät olisivat avuksi.

Muutosjohtaminen keskittyy ihmisen toiminnan muutokseen ja rooliin usein teknisessäkin maailmassa, hyvin käytännönläheisillä työkaluilla. Työn tuloksena syntynyt malli on sovellettavissa käytännössä, sekä toimeksiantajan käytössä että laajemmin. Malli on kirjoitettu siten, että se on helposti lähestyttävissä eikä

sisällä vaikeasti tulkittavia osioita. Tehtävät on pyritty kuvaamana selkeästi ja siten, että niiden merkitys ja syy tehtävälle on myös korostettu.

Mallin lisäksi lopputuloksena syntyneitä menestystekijöitä ja kyberturvallisuuskulttuuriin vaikuttavia ominaisuuksia voi hyödyntää sellaisenaan tutkiessaan ja kehittäessään organisaation kyberturvallisuuskulttuuria. Työn lopputulokset ovat hyödynnettävissä myös kyberturvallisuustietoisuuden ja kyberturvallisuuskulttuurin koulutuksessa.

Kyberturvallisuus on usein tekninen osaamisalue ja tämä työ vahvistaa, miten ihmisen rooli on merkityksellinen ja miten ihmislähtöinen lähestyminen aiheeseen voi tuoda merkittävää hyötyä. Tutkimuksessa luotu malli on validoitu muutosjohtamisen asiantuntijan toimesta, mutta silti se on vain yksi uusi malli, kunnes sitä hyödynnetään käytännössä. Toimeksiantajan hyödyntäminen ja jatkotutkimuskohteet vasta avaavat mallin todellisen merkityksen.

7.2.2 Prosessi

Tutkimusprosessi jakautui karkeasti neljään vaiheeseen: suunnittelu, tutkimus, kehitys ja finalisointi. Suunnitteluvaiheessa työ haki suuntaa ja rajausta. Nopeasti kulttuurillinen teema nousi kantavaksi ja se vei työtä eteenpäin. Tutkimusvaihe oli yksi laaja kokonaisuus, jonka aikana sekä haastattelututkimus että teoreettinen viitekehys alkoi rakentumaan. Kolmannen vaiheen muodosti kehitysvaihe, jossa teorian ja tutkimusanalyysin perusteella syntyi tutkimuksen lopputulos eli malli muutosjohtamisen menetelmillä rakentuvaan kyberturvallisuuskulttuuriin. Finalisointivaihe sisälsi työn loppuunsaattamisen sekä analysoinnin.

Tutkimuksen konteksti oli laaja, joten rajausta piti tehdä läpi koko prosessin. Punainen lanka kuitenkin matkan aikana löytyi ja vahvistui, mitä pidemmälle prosessi eteni. Jos tutkimus toteutettaisiin uudestaan, rajaukseen voisi vielä enemmän keskittyä ihan ensimmäisessä vaiheessa.

7.2.3 Tulosten merkitys, lisäarvo

Tutkimus vahvisti muutosjohtamisen merkityksen laajoissa ihmisten toimintaa koskevissa muutoksissa. Muutosjohtamisen ja kyberturvallisuuden asiantuntijana toimeksiantaja tulee hyödyntämään tuloksia asiantuntijoiden osaamisen kehittämisessä sekä liiketoiminnassaan.

7.2.4 Rajoitteet

Mallin validointi käytännössä ja käytännön tuomia rajoitteita ei tässä tutkimuksessa voitu tutkia ilman että tutkimus olisi laajentunut merkittävästi. Käytännön soveltaminen on tunnistettu jatkotutkimuskohteena. Lisäksi mallin validoiminen tietoturva-asiantuntijan toimesta olisi ollut ajankäytöllisesti haasteellista ja myös työn fokuksen kannalta ei välttämätöntä.

7.3 Jatkotutkimuskohteet

Tämä tutkimus oli rajattu vastaamaan muutosjohtamisen menetelmien sopivuudesta kyberturvallisuuskulttuurin kehittämiseen. Työn edetessä uusia tutkimuskohteita syntyi uuden tiedon myötä ja niitä oli tiukasti rajattava pois, jotta työ pysyy yhtenä selkeänä kokonaisuutena. Jatkotutkimuskohteet ja avoimet kysymykset on avattu seuraavassa.

- Millainen vaikutus tekoälyllä on kyberturvallisuuskulttuuriin? Tekoälyn hyödyntäminen vaikuttaa laajasti ihmisen tekemään työhön ja ihmiseen rooliin työn tekijänä ja tätä kautta myös kyberturvallisuuteen. Onko jatkossa vielä vaikeampi tunnistaa kyberuhat? Tai ehtiikö kyberturvallisuuskulttuurit edes muodostua, ennen kuin tekoälyn rooli on kasvanut liian räjähdysmäisesti?
- Miten ihmisten motivaatio kehittyy kyberturvallisuuskulttuurissa? Humanistisempi tutkimusaihe olisi ihmisen motivaatiot ja syyt taustalla. Miten motivaatio muuttuu kyberturvallisuuskulttuurin kehittymismatkalla

ja mistä syystä? Mikä alun perin on vaikuttanut motivaatioon nimenomaan turvallisuuden suhteen?

- Miten mallin soveltaminen onnistuu arjessa, mitä siitä opitaan? Luontainen jatkumo olisi soveltaa tässä työssä kehitettyä mallia arjessa, ja kerätä kokemuksia sekä jatkokehitysehdotuksia.
- Miten mittaamisen soveltaminen arjessa toteutuisi? Organisaatiokulttuurin ja kyberturvallisuuskulttuurin muutoksen mittaaminen on haasteellista. Tässä työssä esitetty kolmitasoinen mittaustapa voisi olla yksi mahdollinen malli, jonka toteutumista voisi testata ja tutkia. Mitkä mittarit todella toimivat käytännössä kyberturvallisuuskulttuurin mittareina?

Lähteet

Adams, A., & Sasse, A. (1999). Users Are Not The Enemy. *Communications of the ACM*. *42*(12), 40-46. https://doi.org/10.1145/322796.322806

Alasuutari, P. (2011). *Laadullinen tutkimus 2.0.* Vastapaino.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*. https://doi.org/10.1016/j.cose.2020.102003

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*. https://doi.org/10.48550/arXiv.1901.02672

da Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*. https://doi.org/10.1016/j.cose.2020.101713

ENISA. (2023). *Awareness and cyber hygiene*. Haettu 14.8.2025 osoitteesta https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene

ENISA. (2025). *European Union Agency for Cybersecurity*. Haettu 14.8.2025 osoitteesta https://www.enisa.europa.eu/

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino.

EU. (2025). *Europe's digital decade*. European Commission. Haettu 19.8.2025 osoitteesta https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fi

Haukilehto, T. (2024). *Cybersecurity management in healthcare* (Acta Wasaensia 532) [Väitöskirja, Vaasan yliopisto]. https://urn.fi/URN:ISBN:978-952-395-140-2

IEC. (2026). *International Electrotechnical Commission*. Haettu 24.3.2026 osoitteesta https://www.iec.ch/homepage

ISO. (2026). *ISO: Global standards for trusted goods and services*. Haettu 27.2.2026 osoitteesta https://www.iso.org/home.html

ISO/IEC 27001. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization & International Electrotechnical Commission. Haettu 11.2.2026 osoitteesta https://www.iso.org/standard/27001

ISO/IEC 27002. (2022). *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls*. International Organization for Standardization & International Electrotechnical Commission. Haettu 20.1.2026 osoitteesta https://www.iso.org/standard/75652.html

ISO/IEC 27005. (2022). *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. International Organization for Standardization & International Electrotechnical Commission. Haettu 6.2.2026 osoitteesta https://www.iso.org/standard/80585.html

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P., & Talala, T. (2014). *Yrityksen riskienhallinta*. Finva.

Järvinen, P. (2025). *Yrityksen tietoturvaopas*. Kauppakamari.

Luukka, P. (2019). *Yrityskulttuuri on kuningas*. Alma Talent.

Murthy, C. (2007). *Change management*. Himalaya Publishing House.

Piha, K. (2017). *Konflikti päivässä: Kulttuuri ratkaisee yrityksen kohtalon*. Alma Talent.

Prosci. (2025). *The Prosci ADKAR model*. Haettu 8.1.2026 osoitteesta https://changepartners.fi/wp-content/uploads/2024/03/Prosci-ADKAR-malli-ekirja.pdf

Ruusuvuori, J., Nikander, P., & Hyvärinen, M. (toim.). (2010). *Haastattelun analyysi*. Vastapaino.

SANS. (2026). *SANS security awareness & culture maturity model eBook*. Haettu 20.3.2026 osoitteesta https://www.sans.org/white-papers/security-awareness-maturity-model

Sasse, M. A. (2015). Scaring and bullying people into security won't work. *IEEE Security & Privacy, 13*(3), 80–83. https://doi.org/10.1109/MSP.2015.65

Schein, E. H., & Schein, P. (2017). *Organizational culture and leadership* (5th ed.). Wiley.

Seville, E. (2017). *Resilient organizations: How to survive, thrive and create opportunities through crisis and change*. Kogan Page.

Tienari, J., & Meriläinen, S. (2012). *Johtaminen ja organisointi globaalissa taloudessa*. Alma Talent.

Uusikylä, P., & Jalonen, H. (2023). *Epävarmuuden aika: Kuinka ymmärtää systeemistä muutosta*. Into.

VM. (2017). *Yhteiskunnan turvallisuusstrategia*. Valtiovarainministeriö. Haettu 19.8.2025 osoitteesta https://vm.fi/yhteiskunnan-turvallisuusstrategia

VM. (2024). *Suomen kyberturvallisuusstrategia 2024–2035*. Valtiovarainministeriö. Haettu 19.8.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/fe013d31-1fc0-4d23-b121-9acb09215ec8/content

Verizon. (2024). *2024 data breach investigations report*. Haettu 14.8.2025 osoitteesta https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Wright, C. (2019). *How cyber security can protect your business: A guide for all stakeholders*. IT Governance Publishing.

Haastattelurungot

Taulukko 2. Haastattelurunko suomeksi

KYBERTURVALLISUUS YLEISESTI
Mitä kyberturvallisuus sinulle tarkoittaa? Miten määrittelet sen.
Mitä asioita kyberturvallisuuden piiriin kuuluu?
Miten kuvailet kyberturvallisuuskulttuurin? Onko kyberturvallisuus kulttuurillinen asia? Miksi?
TOIMIALAN VAIKUTUS
Minkä toimialan edustajien parissa olet tehnyt kyberturvallisuuden työtä?
Minkälaista työtä olet eri toimialoilla tehnyt, minkälaisia havaintoja olet tehnyt?
Miten toimiala vaikuttaa kyberturvallisuuteen ja siihen liittyvään kulttuuriin?
Mikä muu vaikuttaa kyberturvallisuuskulttuuriin?
KYBERTURVALLISUUSKULTTUURI, HAASTEET JA MENESTYSTEKIJÄT
Onko nykyisessä tai aiemmassa organisaatiossasi tunnistettava kyberturvallisuuskulttuuri? Mitä se siellä tarkoittaa?
Mitkä elementit rakentavat hyvän kyberturvallisuuskulttuurin?
Mitkä luovat haasteita kulttuurin toteutumiselle?

Taulukko 2. Haastattelurunko suomeksi (jatkuu)

Mikä on kyberturvallisen kulttuurin toteutumisen edellytykset? Mikä edesauttaa sen toteutumista
Mistä tunnistaa kyberturvallisuuskulttuurin arjessa? Mistä tunnistaa sen puuttumisen?
Miten muutosjohtamisen menetelmillä voidaan tukea organisaatiokulttuurin muutosta? Mitä työkaluja käyttäisitte (muutosjohtajille)
Miten mittaisitte kyberturvallisuuskulttuurin muutoksen etenemistä?
TOTEUTUNEET UHAT
Minkälaisia kyberturvallisuuden uhkia olet kohdannut työurasi aikana?
Onko ihmisellä ollut siihen osuutta? Mikä aiheutti toteutuneet uhat?
Miten niistä selvittiin? Mitä opittiin? Mitä tehtiin eri tavoin?

Taulukko 3. Haastattelurunko englanniksi

CYBER SECURITY and CULTURE IN GENERAL
How would you describe cyber security? What falls under its category
INDUSTRY RELATION
In your work past, with which industries have you worked with in cyber security roles? What kind of roles.

Taulukko 3. Haastattelurunko englanniksi (jatkuu)

How would you say industry affects the cyber security culture in an organization?
In addition to industry, what else affects the cyber security culture in an organization?
CYBER SECURITY CULTURE; SUCCESS FACTORS AND CHALLENGES
What are the main characteristics that you recognize that create a cyber security culture?
What in your opinion are the main success factors of forming a good cyber security culture? What helps it bloom
What creates barriers for it to succeed? What kind of pitfalls are there
MEASURING
Which measuring ways do you think are most effective? When focusing on cyber security culture.
What kind of challenges have you faced when measuring? What kind of success stories?
FUTURE
How do you think the for example the use of AI will affect cyber security cultures?
What else do you think will be the most relevant questions in the future related to cyber security?

Haastatellut

Kyberturvallisuuden ja kysymysten laajuuden vuoksi suurin osa haastateltavista ovat anonyymejä, haastattelut dokumentoitiin lokaalisti ja teemoitettiin työn kannalta olennaisten yhteisten teemojen ympärille. Käytön jälkeen dokumentaatio poistettiin. Haastatellut tietoturva-asiantuntijat ovat yksityisen ja julkisen sektorin edustajia, ja heillä on monipuolinen kokemus tietoturvasta kummallakin sektorilla. Muutosjohtajilla on laaja kokemus yksityisestä ja julkisesta sektorista, erityisesti muutosjohtamisen ja organisaatiokulttuurin kehittämisen kuin tietoturvankin näkökulmasta. Kaikkia haastateltavia haastateltiin heidän henkilökohtaisesta näkökulmastaan, ei edustamansa organisaation näkökulmasta. Haastattelut pidettiin Teamsin yli ja jokainen haastattelu kesti noin tunnin. Muutosjohtajien kanssa oli lisäksi ryhmähaastattelu.

Taulukko 4. Haastatellut ja heidän roolinsa

Haastateltu	**Rooli**	**Toimialat**	**Haastattelu**
Johto 1	Tietoturva-asiantuntija, johto	Tietoliikenne, julkishallinto	Toukokuu 2025
Johto 2	Tietoturva-asiantuntija, johto	Energia, tietoliikenne, valmistava teollisuus, kansainväliset organisaatiot	Toukokuu 2025
Asiantuntija 1	Tietoturva-asiantuntija	Julkishallinto, media, energia, teollisuus, laki, palveluntuottaja	Kesäkuu 2025
Asiantuntija 2	Tietoturva-asiantuntija	Ohjelmistokehitys- ja testaus, valmistava teollisuus, tietoliikenne, finanssi, julkishallinto, pelastus, pelit	Kesäkuu 2025

Taulukko 4 (jatkuu)

Haastateltu	**Rooli**	**Toimialat**	**Haastattelu**
Asiantuntija 3	Tietoturva-asiantuntija	Puolustus, teollisuus, kauppa, julkishallinto	Kesäkuu 2025
Asiantuntija 4	Tietoturva-asiantuntija	Finanssi, teollisuus	Kesäkuu 2025
Asiantuntija 5	Tietoturva-asiantuntija	Lentoliikenne	Kesäkuu 2025
Asiantuntija 6	Tietoturva-asiantuntija	Julkishallinto, terveyssektori, valmistava teollisuus, liikenne, lentoliikenne, kansainväliset organisaatiot	Heinäkuu 2025
Muutosjohtaja 1	Muutosjohtaja	Julkishallinto, tietoliikenne, koulutus, valmistava teollisuus	Kesäkuu 2025
Muutosjohtaja 2	Muutosjohtaja	Teollisuus	Kesäkuu 2025

Haastattelupyyntö

Opiskelija tekee opinnäytetyötä liittyen Turun amk:n tutkintoon **tradenomi (ylempi amk), koulutusohjelmana teknologiaosaamisen johtaminen**.

Opinnäytetyön aiheena on (työnimi): *Kyberturvallisuuskulttuuri – Kyberturvallisuuden merkitys kulttuurillisena asiana; haasteet ja menestystekijät; toimialavaikutus.*

Tutkimuskysymykset (työversio): Mitkä ovat keskeiset kulttuurilliset haasteet ja menestystekijät kyberturvallisuuden kehittämisessä? Miten toimiala vaikuttaa kyberturvalliseen kulttuuriin?

Opinnäytetyöllä on toimeksiantaja, (yritys nimetty). Toimeksiantaja tarjoaa ohjausta työhön ja voi halutessaan hyödyntää työn lopputulosta omassa liiketoiminnassaan sekä markkinoinnissa. Opinnäytetyö on lähtökohtaisesti julkinen, työhön ei kerätä luottamuksellista tietoa, ja haastateltavan tai hänen organisaationsa nimeä ei mainita.

Haastateltavat

Haastattelututkimuksessa kerätään ymmärrystä kyberturvallisuudesta kulttuurillisena teemana. Haastateltavat ovat muutosjohtamisen, organisaatiokulttuurin sekä kyberturvallisuuden asiantuntijoita.

Mitä ja miten tietoa kerätään ja käsitellään

Haastattelut suoritetaan kesän 2025 aikana Teamsin yli, ne litteroidaan vain, jos haastateltava erikseen antaa siihen luvan. Haastattelut dokumentoidaan anonymisoituna opiskelijan omalle tietokoneelle. Haastattelukysymykset liittyvät teemoihin: *Kyberturvallisuus ja siihen liittyvä kulttuuri, omat kokemukset sekä kokemus omassa organisaatiossa; kyberturvallisuuskulttuurin elementit, haasteet, menestystekijät, toimialavaikutus.*

Miten tietoa hyödynnetään

Haastatteluilla kerätään ymmärrystä käytännön kulttuurityöstä kyberturvallisuuteen liittyen erilaisissa organisaatioissa. Haastatteluja ei liitetä sellaisenaan opinnäytetyöhön. Ymmärryksen perusteella luodaan kanvas kyberturvakulttuurin visiosta; mitkä elementit muodostavat kyberturvallisen kulttuurin, mitä eroavaisuuksia voi löytyä, tunnistettuja haasteita ja menestystekijöitä, toimialavaikutuksen analysointi. Lopputuloksena muodostuu malli, mitä kyberturvallisuuskulttuuriin liittyy, miten sellainen voidaan luoda ja vahvistaa muutosjohtamisen malleja hyödyntäen.