Opinnäytetyö YAMK

Kyberturvallisuuden koulutusohjelma

2025

Petri Tähtinen

Organisaation tietoturvatietoisuuden kehittäminen

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö YAMK | Tiivistelmä

Turun ammattikorkeakoulu

Kyberturvallisuuden koulutusohjelma

2025 | 76 sivua

Petri Tähtinen

Organisaation tietoturvatietoisuuden kehittäminen

Tämän opinnäytetyön tavoitteena oli selvittää organisaation tietoturva-tietoisuuden tasoa ja sen kehittämismahdollisuuksia. Työssä tutkittiin henkilöstön osaamista, asenteita ja käyttäytymistä tietoturvaan liittyen sekä näiden vaikutusta organisaation turvallisuuskulttuuriin. Tietoturvatietoisuus on keskeinen osa kokonaisturvallisuutta, sillä ihmiset ovat yhä merkittävämpi kyberuhkien kohde.

Tutkimus toteutettiin kvantitatiivisena kyselytutkimuksena hyödyntäen *Human Aspects of Information Security Questionnaire* (HAIS-Q) -mittaristoa, joka perustuu *Knowledge–Attitude–Behaviour* (KAB) -malliin. Mallin avulla tarkastellaan tietoturvaan liittyvän osaamisen, asenteiden ja käyttäytymisen yhteyksiä. Kyselylomake mukautettiin organisaation tarpeisiin, ja tulokset analysoitiin tilastollisesti.

Tulokset osoittivat, että henkilöstön osaaminen ja asenteet olivat hyvällä tasolla, mutta parhaiden käytäntöjen noudattaminen ei aina ollut systemaattista. Tämä havainto on linjassa aiempien tutkimusten kanssa, joissa on todettu, ettei tietoisuus ja asenteet yksinään riitä turvallisen käyttäytymisen varmistamiseksi. Johtopäätöksenä voidaan todeta, että tietoturvatietoisuuden vahvistaminen edellyttää jatkuvaa kehittämistä, selkeää viestintää ja tietoturvakulttuurin vahvistamista. Tutkimus tarjoaa käytännön suosituksia organisaation tietoturvakäytäntöjen kehittämiseksi.

Asiasanat:

Tietoturvatietoisuus, tietoturva, kyberturvallisuus, KAB, HAIS-Q,

Master’s Thesis | Abstract

Turku University of Applied Sciences

Degree programme in Cyber Security

2025 | 76 pages

Petri Tähtinen

Developing Information Security Awareness in the Organization

This thesis investigates the level of organizational information security awareness and identifies potential areas for enhancement. The study examines employee’s knowledge, attitudes, and behaviors regarding information security, as well as their influence on the overall security culture within the organization. Given the increasing targeting of individuals by cyber threats, elevating awareness is an essential aspect of comprehensive security measures.

For this research, a quantitative survey was conducted utilizing the *Human Aspects of Information Security Questionnaire* (HAIS-Q), which is grounded in the *Knowledge–Attitude–Behavior* (KAB) model. The survey was tailored to address the specific requirements of the organization, and the findings were subjected to statistical analysis.

The results indicated that while employees demonstrate strong knowledge and favorable attitudes towards information security, their adherence to established best practices remains inconsistent. This finding aligns with previous research suggesting that awareness and positive attitudes alone do not ensure secure behavior. To enhance information security awareness, it is imperative to emphasize continuous development, effective communication, and the cultivation of a robust security culture. The study concludes with practical recommendations aimed at improving security practices within the organization.

Keywords:

Security awareness, information security, cyber security, KAB, HAIS-Q,

Sisältö

Liitteet

Kuvat

Taulukot

Käytetyt lyhenteet

AI	Tekoäly, eli koneen kyky jäljitellä inhimillistä päättelyä (Artificial Intelligence)
BCP	Liiketoiminnan jatkuvuussuunnitelma (Business Continuity Plan)
C&C	Hyökkääjän hallintajärjestelmä (Command and Control)
CIA	Tietoturvallisuuden peruspilarit (Confidentiality, Integrity, Availability)
CISO	Organisaation tietoturvajohtaja (Chief Information Security Officer
COBIT	ISACA:n luoma tietohallinnon hallintaviitekehys (Control Objectives for Information and Related Technologies)
CSF	NIST:n luoma kyberturvallisuuden Viitekehys (NIST Cybersecurity Framework)
CVE	Järjestelmä, joka antaa yksilölliset tunnisteet julkisille tietoturvahaavoittuvuuksille (Common Vulnerabilities and Exposures)
DP	Tietosuoja (Data Protection)
DPO	Tietosuojavastaava (Data Protection Officer)
DRP	Toipumissuunnitelma (Disaster Recovery Plan)
ENISA	EU Kyberturvallisuusvirasto (European Union Agency for Cybersecurity)
GDPR	EU:n tietosuoja-asetus, joka säätelee henkilötietojen käsittelyä ja suojaa yksilöiden yksityisyyttä (General Data Protection Regulation)

HAIS-Q	Kyselyjärjestelmä tietoturvatietoisuuden arviointiin (Human Aspects of Information Security Questionnaire)
InfoSec	Tietoturva; käytännöt ja toimenpiteet, joilla suojataan tietoja (Information Security)
ISA	Tietoturvatietoisuus (Information Security Awareness)
ISACA	Järjestö, joka keskittyy tietohallintoon, tietoturvaan, riskienhallintaan, auditointiin ja IT-hallintoon (Information Systems Audit and Control Association)
ISO	Tietoturvavastaava (Information Security Officer)
ISO/IEC	Kansainvälinen standardointiorganisaatio (Organization for Standardization sekä International Electrotechnical Commission)
ISMS	Tietoturvan hallintajärjestelmä (Information Security Management System)
KAB	Tietoturvatietoisuuden kolmea ulottuvuutta mittaava malli (Knowledge, Attitude, Behaviour)
MITRE	Yhdysvaltalainen organisaatio, joka tunnetaan erityisesti kyberturvallisuuteen liittyvistä hankkeista, kuten ATT&CK-viitekehyksestä ja CVE-tietokannasta.
NIS2	EU:n verkkoturvadirektiivin toinen versio (Network and Information Security 2)
NIST	Yhdysvaltalainen standardointijärjestö (National Institute of Standards and Technology)
OPS	Organisaation operatiivisista ICT-toiminnoista, kuten IT-infrastruktuurista ja toimintavarmuudesta, vastaava tiimi (Operations Team)

OSINT	Avointen lähteiden tiedustelu (Open-source Intelligence)
OWASP	Järjestö, jonka tavoitteena on edesauttaa ohjelmistojen turvallisuutta (Open Web Application Security Project)
PCI-DSS	Maksukorttialan tietoturvastandardi (Payment Card Industry Data Security Standard)
PDCA	Jatkuvan parantamisen malli (Plan-Do-Check-Act)
SaaS	Ohjelmistopalvelumalli, jossa ohjelmistoa käytetään pilvipalvelun kautta ilman paikallista asennusta (Software as an Service)
SANS	Kyberturvallisuuden koulutusorganisaatio (System Administration, Networking, and Security)
SP	NIST:n nimeämistapa teknisille dokumenteille (Special Publication)
SLA	Palvelutasosopimus (Service Level Agreement)
WEF	Maailman talousfoorumi (World Economic Forum)

1 Johdanto

Ihmisistä on tullut globaalisti kyberuhkatoimijoiden ensisijainen hyökkäysvektori, ja teknologian sijasta, ihmiset edustavatkin nykyään suurinta tietoturvariskiä organisaatioille. Viimeisimpien tutkimusten mukaan inhimillinen tekijä on osallisena vähintään 68 %:ssa onnistuneista tietomurroista. [1]

Sosiaalinen manipulointi ja erityisesti tietojenkalastelu ovat lisääntyneet ja tekoälyavusteiset kalasteluhyökkäykset ovat laadukkaita sekä rikollisille helppoja ja nopeita toteuttaa. Kyberturvallisuuskeskus arvioi, että uhkataso tulee pysymään jatkossakin kohonneena, ja tietoturvataitojen merkitys korostuu entisestään. Yhteiskunnan digitalisoituessa näiden taitojen hallinta ja jatkuva kehittäminen ovat osa tärkeitä kansalaistaitoja. [2]

Nykyään on yhä selvempää, että pelkät teknologiset ratkaisut eivät riitä takaamaan riittävää tietoturvan tasoa. Vaikka kehittyneet ohjelmistot ja laitteistot ovat tärkeitä suojautumistapoja, ne eivät yksinään pysty vastaamaan kaikkiin modernien kyberuhkien asettamiin haasteisiin. Henkilöstön tietoturvaosaaminen ja valmius reagoida nopeasti ja oikein, erilaisiin uhkatilanteisiin ovat ratkaisevan tärkeitä organisaation turvallisuuden ylläpitämisessä. Vain yhdistämällä sopivat teknologiat ja hyvin koulutettu henkilöstö voidaan saavuttaa kattava ja kestävä tietoturva, joka pystyy vastaamaan jatkuvasti kehittyviin uhkiin. Tietoturvatietoisuuden kasvattaminen tuleekin olla osa organisaation kokonaisvaltaista tietoturvastrategiaa.

Opinnäytetyön tavoitteena oli arvioida henkilöstön tietoturvatietoisuuden tasoa, sekä arvioinnin jälkeen kehittää yritykselle tarkoituksenmukainen ja mitattava kehityssuunnitelma, jolla tietoisuutta voidaan parantaa. Tason tulee vastata työtehtävien edellyttämää osaamista ja arvioinnissa onkin otettava huomioon yrityksen henkilökunnan erilaiset tehtävät; esimerkiksi turvallisen ohjelmistokehityksen osaamista ei ole tarkoituksenmukaista arvioida myyntitehtävissä olevilta työntekijöiltä. Toisaalta henkilöstön valmiudet tunnistaa mahdollisimman tehokkaasti tietojenkalasteluviestejä ovat välttämättömiä kaikille yrityksen työntekijöille, riippumatta heidän työtehtävistään.

Organisaatioiden tietoturvatietoisuuden kehittämiseen on tarjolla erilaisia viitekehyksiä ja tietoisuusohjelmia, joita voidaan hyödyntää pohjana omalle kehitystyölle. Monet näistä ovat kuitenkin maksullisia ja laajoina kokonaisuuksina kalliita. Lisäksi valmiiden ohjelmien soveltaminen suoraan oman organisaation tarpeisiin voi olla haastavaa, sillä eri toimialoilla voi olla hyvin erilaisia vaatimuksia ohjelmien laajuudelle ja sisällölle.

Tämän tutkimuksen teoriaosuudessa käsitellään tietoturvatietoisuuden muodostumista ja siihen vaikuttavia tekijöitä sekä esitellään tutkimuksen kohdeorganisaatio. Lisäksi tarkastellaan tietoturvatietoisuuden nykytilaa ja ennusteita sekä perehdytään menetelmiin, joilla tietoisuutta voidaan kehittää. Empiirisessä osuudessa esitellään tutkimusmenetelmät, mittausjärjestelmät ja tulokset. Tulosten raportoinnissa on huomioitu organisaation tietoturvakäytännöt sekä vaatimukset luottamuksellisuuden suhteen.

Tietoturvatietoisuuteen liittyvä tutkimus on keskittynyt paljon yleisten mallien ja viitekehysten kehittämiseen, mutta niiden käytännön soveltuvuus eri organisaatioihin vaihtelee. Esimerkiksi HAIS-Q-malli on laajasti käytetty mittari tietoturvatietoisuuden arviointiin [3], mutta sen alkuperäisessä muodossa keskitytään yleisiin turvallisuusperiaatteisiin, eikä malli sopinut alkuperäisessä muodossaan suoraan kohdeorganisaation tarpeeseen.

Yhtenä tutkimuksen keskeisistä lähteistä on käytetty Petri Puhakaisen väitöskirjaa *A Design Theory for Information Security Awareness*, joka tarkastelee tietoturvatietoisuuden muodostumista sekä sen yhteyttä käyttäjien toimintaan, kognitiivisiin prosesseihin ja käytännön ratkaisuihin [4]. Puhakaisen käyttämä Design Theory -lähestymistapa tarjoaa arvokkaan viitekehyksen tietoturvakäyttäytymisen parantamiseen, mutta kuten monet teoreettiset mallit, se ei anna suoria ohjeita organisaatiokohtaisen tietoisuusohjelman toteutukseen. Lisäksi mallin sovellettavuus riippuu organisaation rakenteesta ja tietoturvakulttuurista, eikä se huomioi kaikkia käytännön haasteita, kuten rajallisia resursseja tai organisaation sisäisiä rajoitteita tietoisuuden kehittämisessä. Tämä korostaa tarvetta soveltaa teoreettisia malleja joustavasti ja yhdistää niitä organisaatiokohtaiseen arviointiin ja kehitystyöhön.

2 Tutkimuksen tausta ja metodologiat

Nykyään ihmisen roolia organisaation tietoturvan toteuttajana korostetaan lähteestä riippumatta. Inhimillisen tekijän osuus tietomurroissa vaihtelee käytettävien lähteiden mukaan, mutta on erittäin merkittävä tutkimuksesta riippumatta [1] [5] [6].

Kohdeorganisaation riskienhallintaprosesseissa on tunnistettu riskejä, joita voidaan vähentää henkilöstön tietoisuusohjelman avulla. Lisäksi asiakkaiden suorittamissa tietoturva-auditoinneissa sekä tarjouspyyntöihin liittyvissä tietoturvakyselyissä korostuu nykyään henkilöstön osaamisen kehittäminen, sen jatkuva seuranta ja parantaminen.

2.1 Tutkimuksen taustaa

Tutkimukset osoittavat, että inhimillinen tekijä pysyy edelleen organisaatioiden suurimpana riskinä, eikä tämän odoteta muuttuvan lähitulevaisuudessa [7]. Henkilöstön osaamista kehittämällä voidaan pienilläkin investoinneilla parantaa huomattavasti organisaation kokonaisturvallisuutta.

Myös oma kiinnostus ihmisten tietoturvakäyttäytymisen parempaan ymmärtämiseen, oli merkittävä tekijä tutkimuksen aiheen valinnassa. Ihmisten tietoturvaan liittyvää käyttäytymistä on tutkittu erilaisten teoriasuuntausten ja teoreettisten lähtökohtien kautta, joiden avulla on pyritty ymmärtämään ja selittämään, mikä ohjaa työntekijöiden tietoturvakäyttäytymistä. Tunnetussa tietoturvakäyttäytymiseen liittyvässä tutkimuksessa, *Kriittinen analyysi neutralisoimisteorian soveltamisesta tietojärjestelmätieteessä*, Tiina Vestman esimerkiksi kirjoittaa, että seurausten tai rangaistuksen pelko ei ohjaa työntekijöiden tietoturvakäyttäytymistä, ja esittää näkemyksen siitä, kuinka työntekijät oikeuttavat tietoturvarikkomuksiaan erilaisten neutralisoimistekniikoiden avulla ja järkeilevät niiden avulla toimintaansa, jolloin seurauksetkin menettävät merkityksensä [8].

2.2 Tutkimuksen metodologiat

Opinnäytetyö on luonteeltaan tutkimuksellinen kehittämistyö. Tutkimukselliselle kehittämistyölle on ominaista käytännöstä nousseiden ongelmien ratkaiseminen tai käytäntöjen uudistaminen. Tällaisessa työssä kerätään systemaattisesti tietoa sekä käytännöistä että teoriasta, ja hyödynnetään monipuolisesti erilaisia menetelmiä [9].

Tutkimuksen metodologinen lähestymistapa perustuu määrälliseen analyysiin, jossa hyödynnetään olemassa olevia teorioita sekä tunnettuja malleja tietoturvatietoisuuden käsitteen ja sen muodostumisen ymmärtämiseen. Tutkimustavaksi valikoitui kvalitatiivinen tutkimus, joka hyödyntää myös useita kvantitatiivisen tutkimuksen käytäntöjä.

Tutkimuksen tavoitteena on tuottaa konkreettinen malli, jolla organisaation tietoisuuden tasoa parannetaan ja seurataan, eli tutkimusstrategiaksi valikoitui konstruktiivinen menetelmä. Tämä menetelmä sopii hyvin tietoturvatietoisuuden kehittämiseen, koska se keskittyy tarpeeseen ratkaista konkreettisia ongelmia, ja se yhdistää tarpeen käytännön ongelman ratkaisemiseen sekä tieteellisen tiedon.

Tutkimuksen tieteellisinä lähteinä on aiemmin mainittujen väitöstutkimusten lisäksi [4] [8] muun muassa Parsons, ym. tutkimusryhmän useat julkaisut, jotka lähestyvät työntekijöiden tietoisuuden tason arvioinnin aihetta inhimillisten tekijöiden kautta [10] [11].

Varsinkin Puhakaisen tutkimus on alalla merkittävä, koska siinä painotetaan, että tietoisuus ei rajoitu pelkästään työntekijöiden tiedolliseen ymmärrykseen tietoturvakäytännöistä, vaan ulottuu myös käytännön toimintaan ja sitoutumiseen organisaation asettamiin tietoturvatavoitteisiin. Metodologisesti Puhakaisen lähestymistapa tarjoaa mahdollisuuden tarkastella tietoturvatietoisuutta kokonaisvaltaisena prosessina, joka huomioi sekä työntekijöiden kognitiivisen ymmärryksen että käytännön toimet. Tätä kaksiosaista lähestymistapaa hyödynnetään myös tässä tutkimuksessa, jossa tavoitteena on saada laajempaa ymmärrystä tietoturvatietoisuuden kehittämiseen liittyvistä tekijöistä.

2.3 Tiedonkeruumenetelmät

Tiedonkeruumenetelmänä käytetään kyselytutkimusta. Kyselytutkimuksen etuna on se, että sen avulla saadaan kerättyä laaja aineisto ja siinä voidaan kysyä suurelta määrältä ihmisiä useita kysymyksiä. Menetelmänä kysely on tehokas ja nopea, ja ne tuottavat tyypillisesti suuren määrän numeroihin perustuvia tuloksia, joita voidaan käsitellä tilastollisesti. Kyselytutkimus on kvantitatiivinen menetelmä ja perusvaatimuksena kyselyn käyttämiseen on, että aiempaa tietoa tutkittavasta aiheesta on riittävästi. Onkin huomattavaa, että ellei kyselylomakkeen luomisen pohjaksi ole riittävästi aiempaa tietoa, kannattaa tutkimusmenetelmäksi valita kvalitatiivinen tutkimusmenetelmä [9].

Koska kyselytutkimukset perustuvat ennalta määriteltyihin kysymyksiin ja vastausvaihtoehtoihin, tämän tutkimustavan suurimpana heikkoutena pidetään sillä kerätyn tiedon pinnallisuutta. Tutkimusmallin strukturoitu muoto aiheuttaa sen, että se rajoittaa vastaajien mahdollisuutta perustella tarkemmin vastaustaan tai selventää tarkemmin syytä annettuun vastaukseen. Kyselytutkimuksella on myös lähes mahdotonta arvioida vastaajajoukon vastausmotivaatioita, eli sitä kuinka vakavasti vastaajat ovat suhtautuneet tutkimukseen sekä sitä, kuinka hyvin vastausvaihtoehdot ovat onnistuneet. Tutkimusten mukaan kyselytutkimuksissa ongelmaksi saattaa muodostua myös ilmiö nimeltä sosiaalinen toivottavuus, jossa vastaajat pyrkivät antamaan vastauksia, jotka koetaan yleisesti hyväksyttäviksi tai odotettaviksi, sen sijaan että vastaisivat kysymykseen rehellisesti. Tämä luonnollisesti vääristää tutkimuksen tuloksia, ja siihen tulee varautua esimerkiksi tarjoamalla mahdollisuus vastata täysin anonyymisti sekä käyttämällä Likert-tyyppistä vastausskaalaa, jossa vastausvaihtoehto ei ole täysin binäärinen, kyllä tai ei. Kysymysasettelu on myös erittäin tärkeää, jotta ne kuulostavat vastaajille mahdollisimman neutraaleilta, ilman että vastaaja tuntee painetta vastata tietyllä tavalla [12].

Yleisen tulkinnan mukaan kvantitatiivisilla kyselymenetelmillä saadaan pinnallista mutta luotettavaa tietoa, kun taas kvalitatiivisilla menetelmillä syvällistä mutta huonosti yleistettävää tietoa [9].

Kyselytutkimus toteutettiin tässä opinnäytetyössä sähköisenä kyselynä, joka on nopea ja tehokas tapa kerätä tietoa. Kyselylomakkeen suunnittelu perustui tutkimuksen tavoitteisiin, ja lomakkeeseen sisällytettiin vain olennaiset kysymykset. Lomakkeen pituus ja ulkoasun selkeys ovat tärkeitä, sillä liian pitkä kysely voi heikentää vastaushalukkuutta. Lisäksi saatekirjeellä on merkittävä vaikutus vastausprosenttiin. Sen tulee herättää luottamusta ja sisältää tiedot tutkimuksesta, kyselyn tarpeellisuudesta, anonymiteetistä ja vastausajasta [9].

2.4 Tutkimuksen tiedonkeruulomake

Tutkimuksen tiedonkeruumenetelmän pohjana käytettiin myöhemmin työssä esiteltävää tiedonkeruulomaketta. Alkuperäisen lomakkeen kysymykset muokattiin paremmin kohdeorganisaatiolle sopiviksi, ja muokatussa lomakkeessa oli lopulta 69 väittämää, jotka jakautuivat seitsemään eri mitattavaan tietoturvallisuuden osa-alueeseen. Kysymyksistä noin 30 % oli negatiivisesti aseteltuja, jolla pyritään välttämään vastausvinoumaa, ns. Response Bias, jossa vastaajat valitsevat väittämästä riippumatta aina saman vastausvaihtoehdon. Tutkimuksessa käytettiin, alkuperäisen tutkimuslomakkeen tapaan, 5-portaista Likert-asteikkoa vastaajien mielipiteiden arviointiin. 5-portainen asteikko sisältää keskipisteen eli neutraalin vastausvaihtoehdon, mikä mahdollistaa myös vastaajien neutraalin suhtautumisen väittämiin ilman pakkoa valita joko myönteinen tai kielteinen kanta.

Muokattu kyselylomake on liitteenä, Liite 1.

Tutkimuksessa käytetty Likert-asteikko on yksi käytetyimpiä kyselytutkimusasteikkoja, jonka tavoitteena on saada tehokkaasti ja jäsennellysti kerättyä tietoa vastaajien mielipiteistä ja asenteista. Likert-asteikkoa pidetään luotettavana tapana mitata mielipiteitä ja se soveltuu hyvin erilaisiin aihealueisiin ja määrällisiin kyselytutkimuksiin. Asteikon avulla vastaaja ilmaisee olevansa väittämän kanssa täysin samaa mieltä, täysin eri mieltä tai jotain niiden väliltä. Kyselytutkimusasteikkoja käytetään aina suljettujen kysymysten kanssa, eli vastaajille annetaan valmiit vastausvaihtoehdot, mikä vähentää tulosten

subjektiivista tulkintaa ja helpottaa niiden kvantitatiivista analyysiä. [13]. Tässä työssä tärkeä peruste Likert-asteikon valinnalle oli myös sen soveltuvuus toistuviin kyselytutkimuksiin, jossa voidaan jatkossa seurata tietoturvatietoisuuden kehittymistä organisaatiossa jatkuvan parantamisen mallin, Plan-Do-Check-Act (PDCA). mukaisesti.

2.5 Tutkimuksen vastaajajoukko

Koska tutkimuksella haluttiin arvioida organisaation tietoturvatietoisuutta kokonaisvaltaisesti, kyselytutkimuksen vastaajajoukkona olivat kaikki organisaation työntekijät. Kyselyyn osallistuminen oli vapaaehtoista, mutta vastaajamäärä pyrittiin saamaan mahdollisimman suureksi eri keinoin, mm. tiedottamalla. Saateviestissä korostettiin tutkimuksen täydellistä anonymiteettiä, eli vastaajien henkilötietoja ei kerätty eikä käsitelty missään tutkimuksen vaiheessa. Vastaajilta kysyttiin ainoastaan työntekijän osasto, mutta tämän perusteella vastausta ei voinut yksilöidä tiettyyn henkilöön. Lisäksi vastaajille tarjottiin mahdollisuus jättää myös osastotieto ilmoittamatta, mikäli he niin halusivat. Tämä lähestymistapa edesauttoi hyvän vastausprosentin saavuttamista sekä rehellisten ja luotettavien vastausten keräämistä.

3 Tutkimuksen kohdeorganisaatio

Toimeksiantajayritys on suomalainen ohjelmistoalan yritys, jolla on laaja asiakaskunta toimialallaan. Yritys kehittää ja ylläpitää SaaS-ohjelmistotuotetta, jota käytetään maailmanlaajuisesti tapahtumien hallintaan ja osallistujien rekisteröintiin. Ohjelmisto on käännetty 22 eri kielelle, ja sillä on yli 2100 asiakasta. Vuonna 2024 sen kautta luotiin yli 85 000 erilaista tapahtumaa, ja järjestelmään tuotiin lähes 35 miljoonaa ilmoittautumiskontaktia. Yrityksellä on Suomen toimistojen lisäksi toimipisteet myös Ranskassa ja Ruotsissa, mutta kaikki ohjelmiston konesalipalvelut sijaitsevat Suomessa. Tämä varmistaa, että kaikki asiakastiedot ja henkilötiedot säilytetään EU-alueella.

Laajasta asiakaskunnasta ja ohjelmiston suosiosta johtuen, järjestelmän kautta kulkee vuosittain merkittävä määrä erilaisia henkilötietoja, joten henkilötietosuojasäädösten, kuten General Data Protection Regulation (GDPR)-asetuksen, aukoton noudattaminen on välttämätöntä ja ohjelmistossa onkin hyvät työkalut mm. datan anonymisointiin. Yritys toimii tiedon käsittelijänä (Processor) järjestelmään tallennetulle tai siellä prosessoidulle osallistujien henkilötiedolle sekä rekisterinpitäjänä (Controller) asiakkaiden tiedoille ja oman henkilökunnan tiedoille.

Yrityksen ohjelmisto on itse kehitetty, ja kaikki sovelluskehittäjät työskentelevät Suomessa. Suuri osa yhtiön työntekijöistä on ohjelmistokehittäjiä tai työskentelee muuten suoraan ohjelmiston parissa, esimerkiksi infrastruktuurissa, tietoturvassa tai laadunvalvonnassa. Näiden lisäksi yrityksessä on merkittävä asiakastukiosasto, joka hoitaa asiakaspalvelua ympäri maailmaa useilla eri kielillä. Näitä tukevat kaikki muut normaalin yrityksen tukitoiminnot, kuten myynti, talous- ja hallintopalvelut.

Yrityksen työskentelymalli on hybridi, eli osa työviikosta pyritään tekemään toimistoilla ja osa etänä, työntekijän niin halutessa.

3.1 Organisaation tietoturvatietoisuuden nykytilanne

Yrityksen toimialan vuoksi henkilökunta on lähtökohtaisesti hyvin tietoinen erilaisista uhkakuvista, joita he kohtaavat päivittäisissä työtehtävissään. Lisäksi monella työntekijällä on loppututkinto tietotekniikan, tietoliikenteen tai tietoturvallisuuden alalta, tai heillä on pitkä työkokemus ICT-alalta, joten oletuksena osaaminen on suurella osalla henkilökuntaa hyvällä tasolla. Organisaation kulttuuri, mukaan lukien turvallisuuskulttuuri, on myös hyvin avoin ja erilaisilla viestintäratkaisuilla on tehty tietoturvahavainnoista raportoiminen tai niihin liittyvän avun pyytäminen helpoksi.

Kaikilta työntekijöiltä edellytetään myös tietyn tasoista osaamista tietoturvasta sekä tietosuojasta, ja työsuhteen alussa suoritetaan koulutukset molemmista. Näin varmistetaan osaamisen perustaso jo ensimmäisestä työpäivästä alkaen. Suoritetut koulutukset dokumentoidaan myös organisaation koulutusjärjestelmään, josta saadaan tarvittaessa otettua suoritusdokumentit. Jatkossa kertauskoulutuksia kaikille järjestetään vähintään vuosittain sekä sovelluskehittäjät saavat lisäksi erikseen turvalliseen sovelluskehitykseen liittyvää koulutusta, joka perustuu OWASP Top10-julkaisuun. Koulutukset päivitetään vuosittain vastaamaan kulloinkin ajankohtaista uhkakuvaa, ja niiden suorittaminen on pakollista. Vuosittaisten koulutuksen lisäksi käytössä ei ole ollut muita pakollisia tietoturvaan liittyviä koulutuksia.

Poikkeuksellisista tietoturvaan liittyvistä havainnoista, jotka saattavat vaatia käyttäjien välitöntä huomiota tai toimenpiteitä automatisoitujen suojausratkaisujen lisäksi, henkilökuntaa tiedotetaan tähän tarkoitukseen varattuja viestintäkanavia hyödyntäen. Tietoturvaan, tietosuojaan ja erilaisiin käyttäjähuijauksiin liittyviin alueisiin, löytyykin organisaatiosta valmiit, ja aktiivisesti hyödynnetyt viestintäkanavat.

Organisaatiolla on tietoturvan hallintajärjestelmä (ISMS), joka perustuu pitkälle ISO/IEC 27001 sekä ISO/IEC 27002- standardeihin, mutta sitä ei ole sertifioitu. Tieto- ja kyberturvariskien hallinta on sisällytetty kiinteäksi osaksi organisaation normaalia riskienhallintaa.

4 CIA-mallin merkitys organisaatiolle

Alan kirjallisuus ja eri organisaatioiden julkaisemat tietoturvastandardit tarjoavat hieman toisistaan poikkeavia määritelmiä käsitteelle tietoturvallisuus. Kaikki määritelmät kuitenkin perustuvat samaan perusajatukseen; jälkiteollisessa yhteiskunnassa organisaation tärkein resurssi on tieto, joka halutaan pitää luotettavana sekä nopeasti, oikeassa muodossa ja ainoastaan oikeiden henkilöiden saatavilla. Klassisessa tiedon arvoon perustuvassa määritelmässä, jota kutsutaan myös CIA-kolmioksi, tietoturvallisuus koostuu kolmesta osatekijästä, jotka ovat luottamuksellisuus, eheys sekä saatavuus (Kuva 1) [14].

Kuva 1.Tietoturvallisuuden CIA-malli [15].

4.1 Luottamuksellisuus (Confidentiality)

Luottamuksellisuus tarkoittaa tiedon suojaamista siten, että vain valtuutetut henkilöt tai järjestelmät pääsevät siihen käsiksi. Tämä tarkoittaa, että tieto on suojattu luvattomalta käytöltä ja paljastumiselta. Luottamuksellisuus on yksi tietoturvan keskeisistä periaatteista, ja sitä saatetaan joskus virheellisesti käyttää myös synonyyminä tietoturvallisuudelle, vaikka se kattaa myös muita osa-alueita.

Toimeksiantajaorganisaatiolla on useita asiakkuuksia, jotka toimivat mm. finanssialalla, energiasektorilla ja muilla kriittisen infrastruktuurin toimialoilla, ja ovat näin uuden NIS2-direktiivin vaikutuspiirissä. Tästä syystä tiedon luottamuksellisuuden varmistaminen, kaikissa sen elinkaaren vaiheissa, on

ehdottoman tärkeää. Organisaation päivittäisessä tekemisessä se toteutuu esimerkiksi vahvojen salausjärjestelmien hyödyntämisenä sekä toimenpiteillä, joilla rajoitetaan tehokkaasti tietoihin pääsyä vain oikeutetuille henkilöille.

4.2 Eheys (Integrity)

Eheys tarkoittaa tiedon tarkkuuden ja täydellisyyden säilyttämistä siten, että tieto ei muutu luvattomasti tai vahingossa. Eheys varmistaa, että tieto on luotettavaa ja että sitä voidaan käyttää luottamuksella päätöksenteossa ja liiketoiminnassa. Tiedon tulee säilyä muuttumattomana ja aitona koko sen elinkaaren ajan, ja sen muutosten tulee olla seurattavissa ja valtuutettujen henkilöiden tekemiä.

Yrityksen prosessoimien tietojen eheyden varmistaminen on tärkeää ja organisaation järjestelmät varmistavatkin sen useilla eri ratkaisuilla. Lokitietojen turvallinen ja dokumentoitu toteutustapa sekä suunnitelmalliset ja monitasoiset varmuuskopiointiratkaisut varmistavat sekä asiakkaiden, että organisaation omien tietojen eheyden. Suojautuminen tietojen tahattomalta tai tahalliselta muuttumiselta varmistetaan tarkoituksenmukaisilla tehtävien eriyttämisillä (Segregation of Duties) ja kaksoisvalvonnan (Dual Control) -kontrolleilla sekä tehokkailla pääsynhallinnan käytännöillä.

4.3 Saatavuus (Availability)

Saatavuus tietoturvassa tarkoittaa, että tietojärjestelmät ja tiedot ovat käytettävissä silloin, kun valtuutetut käyttäjät niitä tarvitsevat. Saatavuus varmistaa, että tiedot ovat saatavilla ja käytettävissä ilman tarpeetonta viivettä ja että järjestelmät toimivat jatkuvasti, vaikka ne kohtaavat teknisiä ongelmia, hyökkäyksiä tai muita häiriöitä.

SaaS-palveluntarjoajalle järjestelmien saatavuus on hyvin oleellista. Saatavuutta mitataan usein Service Level Agreement, SLA-tasolla, joka määrittää prosenttiosuudella ajasta kuinka paljon järjestelmä on vuositasolla käytettävissä. Tyypillisiä SLA-arvoja on esim. 99,9 % tai 99,99 %, joista jälkimmäinen tarkoittaa

vuositasolla n. 53 minuutin suunnittelemattomia käyttökatkoja. Toimeksiantajan järjestelmien saatavuus on varmistettu mm. erilaisilla teknisillä ratkaisuilla, sopimuksellisilla yksityiskohdilla palveluntarjoajien kanssa, suunnitelmallisilla katastrofi (DRP)- ja jatkuvuussuunnitelmilla (BCP) sekä sisäisellä ja ulkoisella katkottomalla monitoroinnilla ja valvonnalla.

4.4 Laajennettu tietoturvallisuuden määritelmä

Nykyisin tietoturvallisuuden klassista määritelmää saatetaan pitää riittämättömänä, koska se ei huomioi riittävästi tiedon tuottajan identiteettiä, eikä laitteistojen tai tieto- ja tietoliikennejärjestelmien arvoa. Yleisin laajennettu määritelmä käsittää klassisen määritelmän lisäksi kaksi muuta osatekijää, eli kiistämättömyys ja pääsynvalvonta.

Kiistämättömyys (Non-repudiation) tarkoittaa tietojärjestelmän kykyä tunnistaa ja tallentaa luotettavasti järjestelmää käyttävän henkilön tiedot. Pääsynvalvonta (Access control) tarkoittaa menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. Varsinaisiin tietoihin pääsyn rajoittaminen taas kuuluu edellä esiteltyyn luottamuksellisuuden ylläpitoon. [14]

4.5 Kyberturvallisuuden ja tietoturvallisuuden erot

Tietoturvallisuutta ja kyberturvallisuutta käytetään usein synonyymeinä, jopa virallisissa lähteissä, mutta ne tarkoittavat hieman eri asioita. Tietoturvallisuus (Information Security, InfoSec) käsittelee kaikkea organisaation tietoa riippumatta sen muodosta (digitaalinen tai analoginen) tai sijainnista. Sen tavoitteena on turvata tieto koko elinkaaren ajan, mukaan lukien sen luonti, säilytys, käsittely ja hävittäminen, kaikissa mahdollisissa tiedon tiloissa, kuten säilytyksen, siirron ja käsittelyn aikana. Kyberturvallisuus (Cybersecurity) taas keskittyy ainoastaan digitaalisten tietojen ja järjestelmien suojaamiseen verkkoympäristössä.

F-Securen määritelmän mukaan kyberturvallisuus keskittyy tiedon, tietojärjestelmien ja laitteiden turvallisuuden takaamiseen verkkoympäristössä,

kun taas tietoturvallisuus kattaa tiedon turvaamisen laajemmin. Tietoturvaan kuuluvat myös tiedon fyysinen tallentaminen ja tietoon pääsyn rajoittaminen digitaalisen ympäristön ulkopuolella. Kyberturvallisuuden ja tietoturvallisuuden uhat ovat osin erilaisia. Siinä missä kyberturvallisuus pyrkii estämään haittaohjelmien kaltaisten haittojen aiheuttamia vahinkoja, tietoturvaan kuuluu myös kaikenlaisen tiedon levittämisen sekä väärän tiedon torjunta. Näiden erojen valossa kyberturvallisuutta voi pitää tietoturvallisuuden yhtenä osa-alueena. [16]

4.6 Tietoturvan ja tietosuojan erot

Tietosuoja ja tietoturva liittyvät läheisesti toisiinsa, mutta ovat käsitteinä ja tavoitteiltaan erillisiä. Tietosuoja (Data Protection, DP) keskittyy erityisesti henkilötietojen käsittelyn oikeellisuuteen sekä yksilön oikeuksien turvaamiseen. Tavoitteena on varmistaa, että henkilötietoja käsitellään asianmukaisesti, turvallisesti ja rekisteröityjen oikeuksia kunnioittaen. Tietosuojan keskeinen viitekehys on Euroopan Unionin GDPR-asetus, joka määrittää organisaatioille vaatimukset henkilötietojen keräämiselle, säilyttämiselle ja suojaamiselle. On huomionarvoista, että GDPR-asetus koskee myös EU:n ulkopuolisia yrityksiä ja muita tahoja, jotka käsittelevät EU:n jäsenmaiden asukkaiden tietoja. Tietosuoja kuuluu organisaatioissa tyypillisesti tietosuojavastaavan (Data Protection Officer, DPO) vastuulle, jonka tehtävänä on varmistaa henkilötietojen käsittelyn lainmukaisuus ja rekisteröityjen oikeuksien toteutuminen. [48]

Tietoturva (Information Security) puolestaan kattaa kaiken tiedon suojauksen riippumatta tiedon muodosta tai luonteesta. Tietoturvan tarkoituksena on suojata tiedon luottamuksellisuus, eheys ja saatavuus organisaation tarpeiden mukaisesti. Se keskittyy teknisiin ja hallinnollisiin keinoihin, joilla estetään tiedon luvaton käyttö, muuttaminen tai tuhoaminen. Tietoturvan vastuu kuuluu organisaatioissa usein IT-osastolle tai tietoturvavastaavalle (Information Security Officer, ISO tai CISO). [21]

Tietoturva luo siis tekniset ja hallinnolliset edellytykset tietosuojan toteutumiselle. Ilman vahvoja tietoturvakäytäntöjä, kuten pääsynhallintaa, salauksia ja

valvontamekanismeja, ei henkilötietojen suojaamista voida taata. Näin ollen tietosuoja rakentuu tietoturvan perustalle, mutta sisältää myös juridisen näkökulman henkilötietojen käsittelyyn ja rekisteröityjen oikeuksien toteutumiseen.

Tietoturvan ja tietosuojan hallintaa voidaan osoittaa erilaisilla sertifikaateilla, mutta sertifioinnit ovat huomattavasti yleisempiä tietoturvassa, kun tietosuojassa. Tietoturvan sertifikaatit ovat yleisesti käytössä organisaatioissa, jotka haluavat osoittaa hallintajärjestelmiensä kattavan tiedon suojaamisen kaikki osa-alueet. Tietosuojan sertifikaatit ovat myös yleistyneet, mutta niiden käyttö on edelleen harvinaisempaa.

Tietosuojan sääntely perustuu lakisääteisiin vaatimuksiin, joista keskeisin on GDPR. Se koskee kaikkia organisaatioita, jotka käsittelevät EU-kansalaisten henkilötietoja, ja sen noudattamatta jättämisestä voi seurata merkittäviä sakkoja. GDPR:n noudattaminen ei kuitenkaan edellytä sertifikaattia, mutta sen vaatimukset on täytettävä riippumatta siitä, onko organisaatio hankkinut tietosuojasertifioinnin. Taulukossa 1 on esitelty tarkemmin käsitteiden eroja.

Taulukko 1. Tietoturvan ja tietosuojan keskeisiä eroja

	Tietoturva	**Tietosuoja**
Suojattava tieto	Kaikki organisaation tiedot	Henkilötiedot
Ohjaava direktiivi	Ei ole, pois lukien esimerkiksi NIS2 piiriin kuuluvat organisaatiot	GDPR
Yleinen viitekehys	ISO/IEC 27001, PCI-DSS	ISO/IEC 27701
Lainsäädännön velvoittavuus	Ei pakollinen, mutta voi olla sopimuksellinen vaatimus	Pakollinen, rikkomuksista voi seurata sakkoja
Sertifioinnit	Vapaaehtoisia, mutta yleisiä	Vapaaehtoisia ja harvinaisia

5 Tietoturvatietoisuuden määritelmät

Tietoturvatietoisuus käsitteenä voidaan jakaa kahteen eri lähestymistapaan käytetyn kirjallisuuslähteen mukaan.

Näkökulmien ero perustuu siihen, nähdäänkö organisaation tietoturvatietoisuus ainoastaan työntekijöiden kykynä ymmärtää yrityksen tietoturvakäytännöt ja tietoturvan merkitys päivittäisessä työssä, vai laajeneeko käsite myös työntekijöiden konkreettiseen käyttäytymiseen, ohjeistettujen käytäntöjen noudattamiseen sekä heidän sitoutumiseensa tietoturvatavoitteiden saavuttamiseksi. Jälkimmäisessä näkemyksessä korostuvat myös työntekijöiden aikomukset ja valmiudet toimia tietoturvan periaatteiden mukaisesti, ei vain kyky ymmärtää niitä. Näin ollen tietoturvatietoisuus voi pitää sisällään sekä kognitiivisen ulottuvuuden (tiedon ja ymmärryksen), että käytännön toimintaa ja sitoutumista kuvaavan ulottuvuuden.

Tämä laajennettu tietoisuuden käsite pohjautuu myös sosiaalipsykologisiin näkemyksiin, joissa huomioidaan tietoturvatietoisuuden yksilölliset ja yhteisölliset ulottuvuudet. Laajennetussa määritelmässä tietoturvatietoisuus kattaa työntekijöiden kyvyn ymmärtää tietoturvakäytännöt, mutta lisäksi myös heidän aikomuksensa ja kykynsä noudattaa niitä aktiivisesti osana organisaation päivittäistä toimintaa. Tällöin tietoturvatietoisuus ulottuu tiedollisen ymmärryksen lisäksi myös käytännön sitoutumiseen toimia oikein. Laajennetun määritelmän mukaan tietoturvatietoisuus ei ole vain ohjeiden noudattamista, vaan sen tulee sisältää työntekijöiden sisäinen motivaatio ja vastuu toimia tietoturvallisesti, jolla voidaan vahvistaa organisaation kokonaisvaltaista riskienhallintaa ja turvallisuuskulttuuria [17].

Työntekijän tietoturvatietoisuus muodostuu kahdesta eri osaamisen kategoriasta: yleisestä tietoturvatietoisuudesta sekä tietoisuudesta organisaation omista tietoturvakäytännöistä. Näillä molemmilla on vaikutus työntekijän ja siten myös organisaation tietoturvatietoisuuteen.

Oleellista toimivassa tietoisuusohjelmassa on myös kyky ja aikomus toimia oikein, ei pelkkä osaaminen, joten tässä opinnäytetyössä tietoturvatietoisuus käsitetään jälkimmäisen, laajennetun määritelmän mukaan, eli käsitteessä on mukana oleellisena tekijänä myös työntekijöiden käyttäytyminen.

5.1 Viitekehysten määritelmät tietoisuudelle

National Institute of Standards and Technology, NIST, kuvaa *julkaisussaan SP 800-50, Building an Information Technology Security Awareness and Training Program*, tietoturvatietoisuutta prosessiksi, joka pyrkii lisäämään organisaation henkilöstön tietämystä tietoturvauhista ja haavoittuvuuksista sekä edistämään hyviä tietoturvakäytäntöjä [18].

Riskien tunnistamiseen perustuva lähestymistapa on myös yleinen ja tietoturvatietoisuus voidaan määritellä tietoisuutena tietoturvariskeistä sekä niihin liittyvien torjuntatoimien tuntemisena, joiden avulla organisaatio voi vähentää riskiä tietoturvaloukkauksille. European Union Agency for Cybersecurity, ENISA:n mukaan tietoturvatietoisuus ei ole pelkkää ohjeiden tuntemista, vaan sen tulisi kattaa myös työntekijöiden taidot havaita uhkia ja toimia oikein niitä vastaan. Näin tietoturvatietoisuus tukee aktiivisesti organisaation riskienhallintastrategiaa [19].

ENISA:n *Behavioural Aspects of Cybersecurity*-tutkimus korostaa, että tietoturvatietoisuus on keskeinen osa riskienhallintaa. Tietoturvatietoisuus ei ole pelkkää sääntöjen noudattamista, vaan se on aktiivinen strategia, jolla organisaatio hallitsee riskejään. Dokumentti painottaa, että tietoturvatietoisuus tarkoittaa työntekijöiden varustamista tiedoilla ja taidoilla, joiden avulla he tunnistavat mahdollisia uhkia ja toimivat tavoilla, jotka minimoivat riskejä. Tällainen lähestymistapa sisältää muun muassa organisaation tietoturvapolitiikan tuntemisen ja erilaisia taitoja, kuten tietojenkalastelun havaitsemisen tai arkaluontoisten tietojen turvallisen käsittelyn [19].

ENISA painottaa myös, että toimiva tietoturvakulttuuri ei keskity pelkästään teknisiin toimenpiteisiin, vaan siihen kuuluu myös tietoisuusohjelmia, jotka

hyödyntävät käyttäytymistieteiden oppeja ja strategioita. Tämä kokonaisvaltainen näkökulma liittää tietoturvatietoisuuden riskienhallintaan tukemalla sekä yksilön että koko organisaation vastuuta turvallisuusriskien minimoimiseksi [19].

Tietoturvatietoisuuden kolmantena määritelmänä voidaan ajatella laajasti koko organisaation tietoturvakulttuuria, jonka tulisi olla keskeinen osa koko yrityksen turvallisuusstrategiaa. Tietoturvakulttuuri viittaa organisaation yhteiseen vastuuseen, jossa jokainen työntekijä on osallisena hyvän tietoturvan ylläpitämisessä. Tämä lähestymistapa kattaa enemmän kuin vain tiedon ja käyttäytymisen ja se painottaa yhteisön normeja, asenteita ja käytännön päivittäisiä toimia, jotka tukevat tietoturvaprosesseja ja vähentävät riskejä. Esimerkiksi Control Objectives for Information and Related Technologies-organisaation (ISACA), raportit korostavat, että hyvä tietoturvakulttuuri voi merkittävästi vähentää tietoturvariskejä ja toimia tehokkaana suojakeinona inhimillisiä virheitä vastaan, jotka usein aiheuttavatkin suurimman osan tietoturvaloukkauksista. [20]

Lisäksi voidaan ajatella vaatimustenmukaisuuksien kautta tulevan erilaisia vaatimuksia myös tietoisuudelle. Yleinen tietoturvallisuuden standardi ISO/IEC 27001:2023, sanoo yhtenä henkilöstöön liittyvänä hallintakeinona, että ”Organisaation ja tärkeimpien sidosryhmien henkilöstön on saatava tietoturvaopastusta ja -koulutusta, ja heidän tietojaan organisaation tietoturvapolitiikan, kohdennettujen toimintaperiaatteiden ja menettelyjen muutoksista on päivitettävä säännöllisesti, siinä laajuudessa kuin se on heidän toimenkuvansa kannalta merkityksellistä”. [21] Organisaatioiden tuleekin ottaa vaatimukset tietoisuusohjelmille huomioon, jos lähtevät tavoittelemaan johonkin standardiin perustuvaa sertifiointia, kuten ISO/IEC 27001 tai PCI-DSS.

5.2 Tietoturvakulttuurin muodostuminen

Turvallisuuskulttuuri on tärkeä osa organisaatiokulttuuria. Tyypillisesti organisaatiokulttuuri määrittää laajasti koko organisaation arvot, normit ja toimintatavat, kun taas turvallisuuskulttuuri keskittyy tarkemmin turvallisuuteen

liittyviin alueisiin. Turvallisuuskulttuuri on siis organisaatiossa valitseva käsitys siitä, millaista on turvallinen toiminta, millaisia riskejä toimintaan liittyy ja miten tunnistettuja riskejä voidaan ehkäistä. Turvallisuuskulttuuriin liittyy sekä kyky että tahto toimia turvallisesti ja niin ehkäistä riskien toteutumista. ISACA:n mukaan turvallisuuskulttuurissa turvallisuusajattelu sulautetaan osaksi päivittäisiä käytäntöjä ja se edellyttää johdon vahvaa tukea ja esimerkkiä, työntekijöiden sitouttamista sekä tietoisuuden muuttamista konkreettiseksi toiminnaksi. Turvallisuuskulttuurin kehittäminen on jatkuva prosessi, jossa arviointi ja parantaminen ovat keskeisessä roolissa, jotta turvallisuuskäytännöt pysyvät tehokkaina ja merkityksellisinä [20]. Turvallisuuskulttuuri on avainasemassa organisaation riskienhallinnassa, sillä se ohjaa työntekijöiden käyttäytymistä ja suhtautumista riskeihin.

Tietoturvakulttuuri on osa turvallisuuskulttuuria, mutta se keskittyy erityisesti tietojen, digitaalisten järjestelmien ja verkkojen turvallisuuteen. Siinä painotetaan inhimillisiä, mutta myös teknisiä näkökulmia, jotka liittyvät tiedon suojaamiseen. On siis huomionarvoista, että hyvä turvallisuuskulttuuri tai tietoturvakulttuuri ei muodostu ainoastaan ihmisiä johtamalla ja kouluttamalla, vaan kokonaisvaltainen kulttuuri vaatii muodostuakseen niiden lisäksi osaavia asiantuntijoita ja hyvää teknologiaa, jotta käytännön turvallisuus toteutuu. Tämä tarkoittaa esimerkiksi sitä, että jos organisaatiolla on haavoittuvainen verkkoarkkitehtuuri, sen on vaikea myöskään saavuttaa kokonaisvaltaista turvallisuuskulttuuria.

Usein kirjallisuudessa tai esityksissä tulee vastaan sanonta ”Change the Behaviour, not security awareness”. Tämä kuvaakin hyvin tilaa, johon organisaatioiden tulisikin pyrkiä, eli tietoisuusohjelmien ei tulisi keskittyä ainoastaan osaamisen kasvattamiseen, vaan niillä tulisi olla konkreettinen tavoite työntekijöiden käyttäytymisen pysyvään muutokseen. Tämä saavutetaan vain kulttuurin kehittämisen kautta.

6 Tietoturvatietoisuuden nykytilanne ja näkymät

Nykyään sanotaan, että tieto on organisaation tärkein omaisuus ja yritykset ovatkin investoineet vuosittain miljardeja erilaisiin teknisiin tietoturvatuotteisiin, mutta usein laiminlyöneet panostukset tärkeimpään resurssiin, eli työntekijöihin. Yrityksen tietoturvakoulutus on ollut usein vain kerran vuodessa järjestettävä irrallinen tapahtuma, jossa on saatettu käyttää vanhentunutta tai muuten mielenkiinnotonta materiaalia. Tämän seurauksena työntekijöillä ei välttämättä ole ollut riittävää ymmärrystä nykypäivän hyökkäyksistä ja niiden seurauksista. [22].

Jos halutaan että tietoturvakoulutuksella ja ohjeistuksella on vaikutusta toimintaan, sen tulee olla oikein segmentoitua ja kohdistettu juuri tietylle työntekijäryhmälle, liittyen hänen päivittäisiin työtehtäviinsä. Huonoilla ohjeilla tai huonolla koulutuksella, voi olla jopa turvallisuuskulttuuria rapauttava vaikutus**.** [23]

Gartner on ennustanut, että teknisiin suojausratkaisuihin käytetään vuonna 2025 yli 212 miljardia dollaria. Tämä on 15 % enemmän kuin vuonna 2024 ja jopa 30 % enemmän kuin vuonna 2023 [24]. Vastaavasti tietoturvatietoisuuden kehittämiseen käytettiin vuonna 2023 ainoastaan 5,6 miljardia dollaria, joten ero teknisen suojauksen ja ihmisiin keskittyvän ennaltaehkäisevän suojauksen välillä on merkittävä [25]. Tämä on ristiriitaista, koska useat tutkimukset toteavat, että kuitenkin ihminen aiheuttaa toiminnallaan suurimmat riskit yritysten tietoturvallisuudelle [7] [1].

Tietoisuuden osalta tilanne näyttää olevan paranemassa, ja ennusteen mukaan tietoturvatietoisuuden markkinoiden ennustetaankin kasvavan yli 10 miljardiin dollariin jo vuoteen 2027 mennessä [25].

Samaa kehitystä ennustaa myös World Economic Forumin (WEF) vuosittainen raportti, Global Cybersecurity Outlook 2025, joka toteaa uusimmassa julkaisussaan, että yritykset tunnistavat kyberturvallisuuden kriittisen merkityksen liiketoiminnalle yhä paremmin ja että kyberturvallisuus nähdään keskeisenä

liiketoiminnan mahdollistajana ja resilienssin edellytyksenä. Tieto- ja kyberturvallisuus sisällytetäänkin nykyään usein osaksi yrityksen riskienhallintastrategiaa ja tietoturvatietoisuuden kehittämien on oleellinen osa sitä [26].

Nykyään organisaatioiden käyttäjiltä odotetaankin yhä parempaa tietoturvatietoisuutta. Tietotekniikan kiihtyvä kehittyminen, verkkopalvelujen monipuolistuminen ja toimintaympäristön monimutkaistuminen aiheuttavat sen, että pelkät tekniset tietoturvaratkaisut eivät pysy vauhdissa mukana. Tämä aiheuttaa muutoksia myös yritysten tietoturvaosastoilla koska teknologialähtöisestä turvallisuudesta on siirrytty pikkuhiljaa enemmän ihmisläheiseen, ennalta ehkäisevään ja opastavaan tietoturvallisuuteen. Tämä on tuonut mukanaan myös uusia, tietoturva-ammattilaisille asetettavia henkilökohtaisia vaatimuksia, joissa viestinnälliset ja sosiaaliset kommunikaatiotaidot nousevat esille tietoturvan toteutumisessa. [27].

6.1 Tekoälyn vaikutukset

World Economic Forumin raportin mukaan ainoastaan 10 % yrityksistä luottaa siihen, että tekoälyratkaisut parantavat suojautumista hyökkäyksiä vastaan. [26].

Tekoälyn nopea kehitys ja uudet sovelluskohteet viittaavat siihen, että tekoälyä tullaan pian hyödyntämään vaiheissa, jotka kyberhyökkäyksissä on aiemmin tehty manuaalisesti. Siksi tekoälyn rooli kyberhyökkäyksissä on viime aikoina saanut enemmän huomiota sekä tiedemaailmassa että teollisuudessa. Vaikka tällä hetkellä on epätodennäköistä, että tekoäly loisi täysin uusia hyökkäystapoja, näemme jatkuvasti enemmän tutkimusta siitä, miten tekoälyä voitaisiin käyttää kyberhyökkäyksien radikaaliinkin tehostamiseen ja skaalaamiseen [28].

Nykyiset tekoälytekniikat tukevat jo monia tyypillisen hyökkäysketjun alkuvaiheita. Kehittynyt käyttäjän manipulointi sekä nopeat ja monipuoliset tiedonkeruutekniikat ovat tällaisia esimerkkejä. Tekoälyn tukemat kyberhyökkäykset ovat jo uhka, josta monet organisaatiot eivät pysty selviytymään ja tämä turvallisuusuhka vain kasvaa, kun näemme uusia

edistysaskeleita tekoälymenetelmissä ja kun asiantuntemus tekoälystä tulee laajemmin saataville. [28]

6.1.1 Tekoälyn tuomat hyödyt ja parannukset

Tekoälyn tuoma automaatio tehostaa perinteisiä kyberhyökkäyksiä lisäämällä niiden nopeutta, laajuutta, kattavuutta ja monimutkaisuutta, mikä parantaa hyökkäysten onnistumismahdollisuuksia. Perinteiset hyökkääjät käyttävät paljon manuaalista työtä, asiantuntijaosaamista ja perustason hyökkäystyökaluja toteuttaakseen kyberhyökkäyksiä. Tekoälypohjaiset hyökkäykset mullistavat toteutukset kolmella tavalla. Ensinnäkin tekoäly voi automatisoida manuaaliset hyökkäystehtävät tehokkaammin. Toiseksi tekoäly parantaa perinteisten hyökkäystyökalujen suorituskykyä. Kolmanneksi tekoäly tuo hyökkääjille täysin uusia kykyjä, joita heillä ei ole aiemmin ollut.

Nopeus: Tekoäly voi automatisoida manuaaliset tehtävät, kuten tunnistetietojen keräämisen, haavoittuvuuksien löytämisen ja salasanojen arvailun. Koneet hoitavat nämä tehtävät nopeammin, mikä auttaa hyökkääjiä saavuttamaan tavoitteensa lyhyemmässä ajassa ja vähentää kiinni jäämisen riskiä.

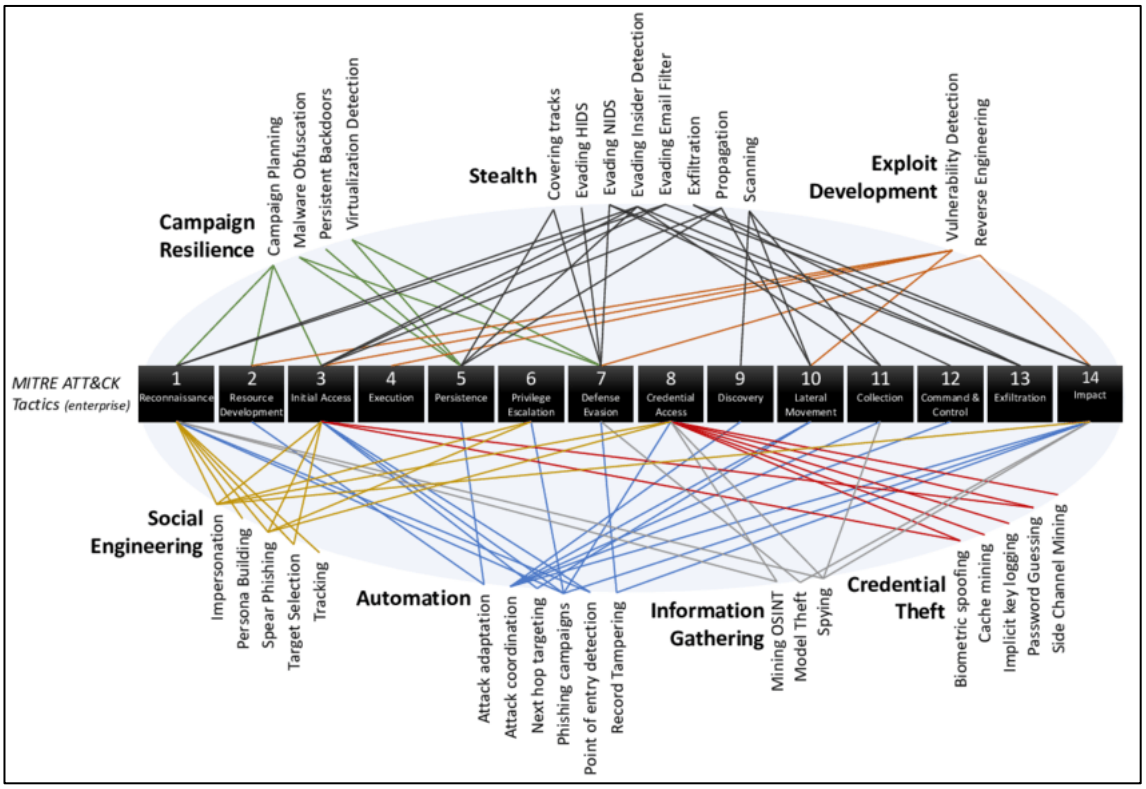
Laajuus: Tekoälyä voidaan käyttää laajentamaan hyökkäyksiä käynnistämällä automatisoituja hyökkäyksiä useisiin kohteisiin samanaikaisesti. Tekoäly on erityisen hyödyllinen kohdennetuissa hyökkäyksissä, kuten spear phishing -hyökkäyksissä, joita voidaan personoida suurelle määrälle uhreja. Tekoäly mahdollistaa tarkemman kohdentamisen ja vaatii vähemmän manuaalista työtä.

Kattavuus: Tekoäly tekee hyökkäyksistä laajempia ja kattavampia. Tekoälyllä varustetut kyberhyökkäykset voivat käsitellä suurempia määriä avointen lähteiden dataa (Open Source Intelligence OSINT), tutkia useampia hyökkäysvektoreita ja tavoittaa enemmän kohteita. Tekoäly varmistaa, että haavoittuvuudet löydetään aukottomasti ja niitä hyödynnetään tarkasti, ilman että mikään jää huomaamatta. [28]

6.1.2 MITRE ATT&CK-viitekehys

Yksi tapa ymmärtää, miten tekoäly voi parantaa hyökkääjien taktiikoita, on jakaa tekoälyn hyökkäyskäyttö kyvykkyyksiin ja sitten tunnistaa, miten ne tehostavat kyberhyökkäysketjua. MITREn ATT&CK-viitekehys jakaa kyberhyökkäyksen vaiheet ja hyökkääjän tavoitteet 14 erilliseen taktiikkaan. Nämä taktiikat kattavat kaikki kyberhyökkäyksissä käytetyt tekniikat. Esimerkkejä taktiikoista ovat tiedustelu (reconnaissance), tiedonkeruu (collection), hallintajärjestelmä (command and control, C&C) ja sivuttaisliike (lateral movement) [29]. Tutkimuksen mukaan tekoäly voi tukea jo nyt monia näistä taktiikoista ja tarjota uusia keinoja hyökkääjien tavoitteiden saavuttamiseksi. Tutkimus listaa jopa 33, seitsemään eri ryhmään kategorisoitua tekoälypohjaista hyökkäyskykyä, joita hyökkääjät voivat käyttää tehostaakseen toimintaansa [30]. (Kuva 2).

Monet kuvan kyvykkyyksistä liittyvät suoraan hyökkäystaktiikoihin, joilta suojautuminen edellyttää ihmisen hyvää ja ajantasaista tietoturvatietoisuutta.



Kuva 2. MITRE ATT&CK mukaiset AI-pohjaiset hyökkäyskyvyt [30].

7 Tietoturvatietoisuuden muodostumiseen vaikuttavat tekijät

Työntekijän tietoturvatietoisuuteen vaikuttavat tekijät voidaan jakaa kolmeen kategoriaan: organisatorisiin, yksilöllisiin ja välillisiin tekijöihin. Nämä kaikki vaikuttavat työntekijän tietoon, asenteisiin ja käyttäytymiseen tietoturvan osalta.

Organisatorisiin tekijöihin kuuluvat organisaation tietoturvakulttuuri, sosiaaliset normit sekä johdon tuki ja vuorovaikutus työntekijöiden kanssa. Yksilöllisiä tekijöitä ovat demografiset ja psykologiset ominaisuudet, kuten työntekijän persoonallisuus ja hänen aiemmat kokemuksensa erilaisista tietojärjestelmistä. Välillisiin tekijöihin kuuluvat tietoturvakoulutus, viestintä ja tietoturvaharjoitukset, jotka tukevat tietoturvatietoisuuden kehitystä organisaation arjessa [10]. (Kuva 3). Näitä tekijöitä ja niiden merkitystä tietoturvatietoisuuden kehittämisessä tarkastellaan tarkemmin seuraavissa alaluvuissa, 7.1–7.3.

Kuva 3. Yksilön tietoturvatietoisuuteen vaikuttavat tekijät [11].

7.1 Organisatoriset tekijät

Tutkimusten mukaan tietoturvallisuuden hallinnalla on merkittävä vaikutus tietoturvatietoisuuden kehittämiseen. Organisaation kulttuuri ja sosiaaliset normit ovat keskeisiä tekijöitä, jotka voivat joko vahvistaa tai heikentää työntekijöiden tietoturvatietoisuutta. Näihin tekijöihin kuuluvat tietoturvakulttuuri, kollektiiviset arvot ja uskomukset sekä normit, kuten työntekijöiden keskuudessa vallitsevat käsitykset hyväksyttävästä ja ei-hyväksyttävästä toiminnasta [10].

Tietoturvakulttuuri on osa organisaatiokulttuuria ja sillä on osoitettu olevan vaikutus työntekijöiden tietoturvatietoisuuteen [23] [31]. Vahvan positiivisen tietoturvakulttuurin omaavassa organisaatiossa työntekijöiden näkemys tietoturvasta onkin yhtenevä organisaation tietoturvakäytäntöjen kanssa. Myös palkitsemis- ja rankaisujärjestelmät, kuten tunnustukset hyvistä tietoturvakäytännöistä tai sanktiot niiden laiminlyönnistä, kuuluvat tähän ryhmään ja voivat motivoida työntekijöitä toimimaan tietoturvakäytäntöjen mukaisesti. Organisatorisiin tekijöihin kuuluu myös organisaation ylimmän johdon tuki. Jos tietoturva nähdään johdossa ainoastaan teknisenä kysymyksenä tai jopa liiketoimintaa rajoittavana tekijänä, tietoturvatietoisuuden kehittäminen ja turvallisen organisaatiokulttuurin luominen on hyvin vaikeaa. Esimerkiksi johdon sitoutuminen resursoimaan tietoturvakoulutuksia ja tukemaan organisaation tietoturvapolitiikkoja ovat keskeisiä tietoturvakulttuurin vahvistamisessa.

7.2 Yksilölliset tekijät

Yksilöllisiin tekijöihin kuuluvat työntekijän henkilökohtaiset piirteet, kuten persoonallisuus ja psykologiset ominaisuudet.

Tietyt ominaisuudet, kuten riskitietoisuus ja kyky hallita stressiä, sekä aiemmat kokemukset ja asenteet tietoturvaan vaikuttavat siihen, kuinka vakavasti työntekijä suhtautuu tietoturvaan ja miten hän toimii mahdollisissa riskitilanteissa.

Demografiset tekijät, kuten ikä ja koulutustausta, voivat lisäksi vaikuttaa siihen, miten työntekijät omaksuvat tietoturvakäytäntöjä. Tutkimuksissa on havaittu, että

esimerkiksi korkea ikä vaikuttaa positiivisesti työntekijän tietoturvatietoisuuden [32]. Hyvä ymmärrys eri tietojärjestelmistä sekä yleinen tietotekniikan osaaminen ovat myös merkittäviä tekijöitä. On osoitettu, että hyvä yleinen tietotekninen osaaminen parantaa työntekijän luottamusta omiin kykyihinsä ja vähentää tietojärjestelmiin liittyviä tietoturvariskejä [33]. Tämä luottamus omaan osaamiseen vahvistaa työntekijöiden valmiutta toimia tietoturvakäytäntöjen mukaisesti sekä auttaa tekemään oikeita päätöksiä rauhallisesti yllättävissä tilanteissa [33].

7.3 Välilliset tekijät

Välillisiin tekijöihin kuuluvat erilaiset toimet ja ohjelmat, kuten tietoturvakoulutus ja harjoitukset, jotka tukevat tietoturvatietoisuuden kehittymistä epäsuorasti. Näiden tekijöiden tarkoituksena on parantaa työntekijöiden tietämystä, asenteita ja käyttäytymistä tietoturvakäytäntöjen mukaisesti.

Tutkimusten mukaan välilliset tekijät voivat merkittävästi parantaa työntekijöiden tietoturvatietoisuutta ja -käyttäytymistä. Ne ovat osoittaneet, että tietoturvakoulutus, joka suunnitellaan organisaation ja yksilön tarpeiden mukaisesti, voi lisätä työntekijöiden ymmärrystä tietoturvasta, parantaa asenteita tietoturvakäytäntöjä kohtaan sekä vähentää inhimillisten virheiden riskiä [11].

Tietoturvaviestintä on toinen keskeinen välillinen tekijä, sillä säännöllinen ja selkeä tiedottaminen muistuttaa työntekijöitä tietoturvakäytäntöjen merkityksestä. Viestintä voi sisältää esimerkiksi muistutuksia, ohjeistuksia tai konkreettisia esimerkkejä mahdollisista uhkista.

Ollakseen mahdollisimman tehokkaita, koulutusten tulisi huomioida työntekijöiden erilaiset persoonallisuustekijät sekä erilaiset oppimistarpeet [32]. Koulutusten tuleekin olla segmentoitu, ja toteutettu kohdennetusti juuri tietylle työntekijäryhmälle, käsittelemään heidän työnsä tekemisen haasteita ja sen syitä ja seurauksia. Jos organisaatiolla on ohjeet, joita ei voi noudattaa tai koulutus, joka ei ole riittävästi kohdennettua, niillä on jopa turvallisuuskulttuuria heikentävä vaikutus [23].

8 Tietoturvatietoisuuden kehittäminen

Tietoturvatietoisuuden kehittämisen tulee olla keskeinen osa organisaation turvallisuuskulttuuria ja jokapäiväistä riskienhallintaa. Sen merkitys on korostunut entisestään verkkorikollisten siirrettyä fokustaan pilviratkaisuihin, mikä on seurausta organisaatioiden viime vuosina kiihtyneestä pilvimigraatiosta. Tilastokeskus arvioi, että vuonna 2022 Suomessa 81 % yrityksistä käytti kaupallisia pilvipalveluita ja määrä oli kasvanut vuodesta 2020 30 prosenttiyksiköllä. Suurista, yli 100 työntekijän yrityksistä, peräti 97 % hyödynsi kaupallisia pilvipalveluita liiketoiminnassaan ja arvioiden mukaan pilvipalveluihin onkin tallennutettu nykyään jo 60 % yritysten datoista [34] [35]. Tällaisessa ICT-ympäristössä yksittäisen työntekijän rooli korostuu, sillä hänen toimintansa voi joko tukea organisaation tietoturvaa tai pahimmillaan altistaa sen merkittäville riskeille.

Tietoturvatietoisuus ei synny hetkessä, vaan sen rakentaminen vaatii jatkuvaa ja määrätietoista työtä. Turvallisuuskulttuuri muotoutuu usein arjen käytäntöjen kautta, kun työntekijät omaksuvat tapoja toisiltaan. Turvallisen toiminnan tavat periytyvät organisaatiossa usein työntekijältä toiselle, ja riippumatta siitä mitä organisaation ohjeissa lukee, yhteisön jäsenet alkavat ajan mittaan toimimaan kuten muutkin yhteisön jäsenet.

Tietoisuuden alin taso voi olla saavutettavissa nopeasti esimerkiksi lainsäädännön tai asiakkaiden vaatimusten täyttämiseksi. Kuitenkin todellinen hyöty ohjelmista saadaan, kun lähdetään kehittämään käyttäytymismalleja ja koko organisaation tietoturvakulttuuria. Tämän saavuttaminen ei tapahdu hetkessä, vaan vaatii jatkuvaa ja määrätietoista työtä ja sen saavuttaminen vie vuosia.

8.1 Tunnettuja tietoturvatietoisuuden viitekehyksiä

Tietoturvatietoisuuden kehittämiseen on olemassa useita eri viitekehyksiä. Niiden hyödyntäminen tarjoaa organisaatioille rakenteellisen lähestymistavan, joka

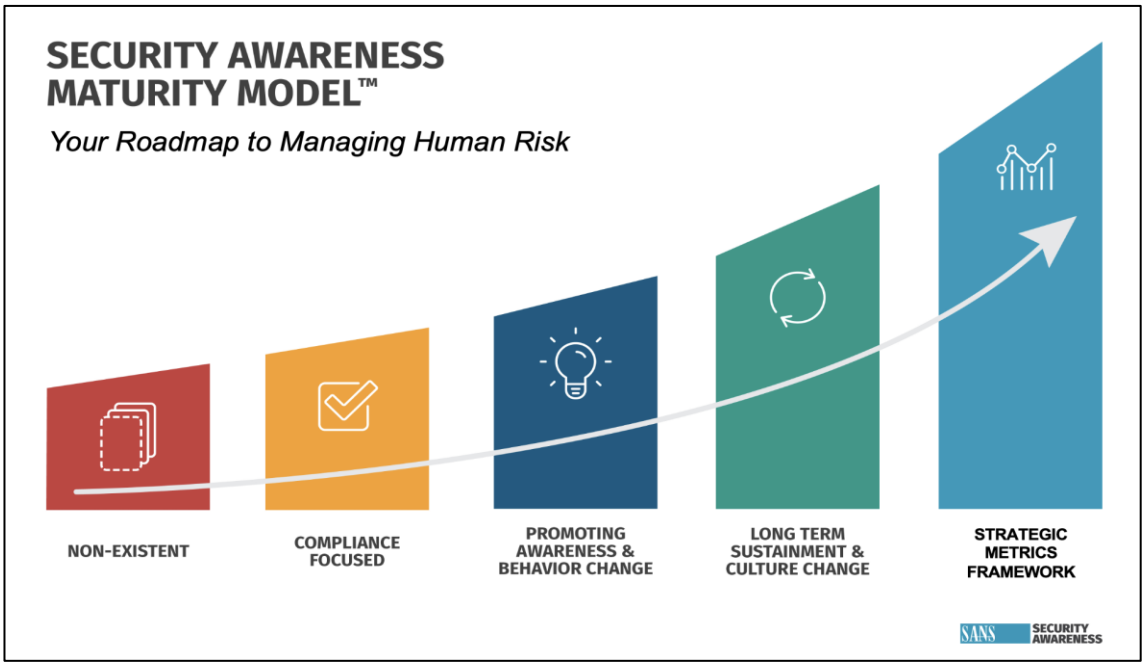
auttaa varmistamaan ohjelmien kattavuuden ja vaikuttavuuden. Viitekehysten hyödyntäminen voi auttaa organisaatioita tunnistamaan omat vahvuutensa ja kehityskohteensa tietoturvatietoisuuden edistämisessä. Esimerkiksi SANS Instituten mallin avulla organisaatiot voivat arvioida tietoturvakulttuurinsa kypsyyttä ja kehittää mittaristoja, joiden avulla voidaan seurata tietoisuusohjelmien vaikutuksia. Tämä systemaattinen lähestymistapa mahdollistaa myös resurssien kohdentamisen tehokkaasti. Taulukossa 1 on esitetty tunnettuja, ja laajalti käytettyä viitekehyksiä tai ohjeistuksia tietoturvatietoisuuden kehittämiseen.

Taulukko 2. Tietoturvatietoisuuden viitekehyksiä

Viitekehys / Malli	Kuvaus
ENISA Cybersecurity Culture Guidelines	Korostaa tietoturvakulttuurin ja tietoisuusohjelmien merkitystä osana laajempaa riskienhallintaa.
NIST SP 800-50	Keskittyy tietoturvatietoisuuden ja -koulutuksen kehittämiseen ja tarjoaa työkaluja organisaation ohjelmien rakentamiseen.
ISACA Security Awareness Model	Painottaa tietoturvatietoisuutta osana organisaation strategiaa ja tietoturvakulttuuria.
SANS Security Awareness Maturity Model	Luokittelee tietoturvatietoisuuden kypsyyden eri tasoihin. Tarjoaa ohjeita tietoisuuden kehittämiseen ja arviointiin vaiheittain, sekä painottaa koulutuksen vaikuttavuuden mittaamista ja jatkuvaa kehittämistä.

8.2 SANS Security Awareness Maturity Model

Yksi käytetympiä viitekehyksiä organisaation tietoturvamaturiteetin mittaamiseen on Yhdysvaltalaisen SANS-instituutin julkaisema tietoisuuden kypsyysmalli, joka jakaa tasot viiteen eri luokkaan. (Kuva 4).



Kuva 4. SANS Maturiteettimalli [7].

Ensimmäisellä tasolla organisaatiolla ei ole lainkaan ohjelmaa tietoisuuden kehittämiseen. Työntekijät eivät ole tietoisia organisaation tietoturvakäytännöistä, eikä tietoturvaa pidetä osana päivittäistä toimintaa

Toisella tasolla tietoturvatietoisuus keskittyy vain välttämättömien viranomaisvaatimusten tai muiden vaatimustenmukaisuuksien täyttämiseen. Tietoisuuskoulutus suoritetaan usein muodollisesti ja pakollisena, esimerkiksi kerran vuodessa, ilman syvempää panostusta tai sitoutumista. Tämä taso on tyypillinen organisaatioille, jotka vasta aloittavat tietoturvatietoisuusohjelmien kehittämisen.

Kolmannella tasolla tietoturvatietoisuutta kehitetään systemaattisesti. Organisaatio hyödyntää erilaisia viestintäkanavia ja järjestää säännöllisiä harjoituksia, joiden tavoitteena on lisätä työntekijöiden ymmärrystä ja sitoutumista tietoturvakäytäntöihin. Tällä tasolla työntekijät tiedostavat organisaation tietoturvakäytännöt, noudattavat niitä ja osallistuvat aktiivisesti esimerkiksi tietoturvatapahtumien raportointiin.

Neljäs taso edustaa jo hyvin korkeaa tietoturvatietoisuuden kypsyysastetta, jossa tietoturva on sisäänrakennettu osa organisaation kulttuuria. Tämä taso ei ainoastaan täytä sääntelyn vaatimuksia ja hallitse riskejä, vaan tukee myös muita organisaation turvallisuusuudistuksia. Turvallisuus on integroitunut kaikkiin organisaation toimintoihin, ja sen saavuttaminen edellyttää pitkäjänteistä työtä. Tyypillisesti tämän tason saavuttaminen vie tyypillisesti 3–10 vuotta.

Viimeisellä tasolla tietoturvatietoisuus on täysin integroitunut organisaation missioon ja strategiaan. Tietoturvatietoisuuden mittarit ovat jatkuvassa kehityksessä ja niitä hyödynnetään aktiivisesti toiminnan vaikutusten arvioinnissa. Mittariston avulla voidaan osoittaa ohjelmaan sijoitetun pääoman tuotto ja sen tuoma lisäarvo organisaatiolle. [7].

Kuvassa 5 on esitetty SANS:n maturiteettimatriisin kolme ensimmäistä tasoa sekä tasojen ohjelma- ja henkilöstöindikaattorit. Stage 1 vastaa edellisen kuvan alinta tasoa (Non-Existing) ja sisältää siihen liittyvät Program ja People-indikaattorit.

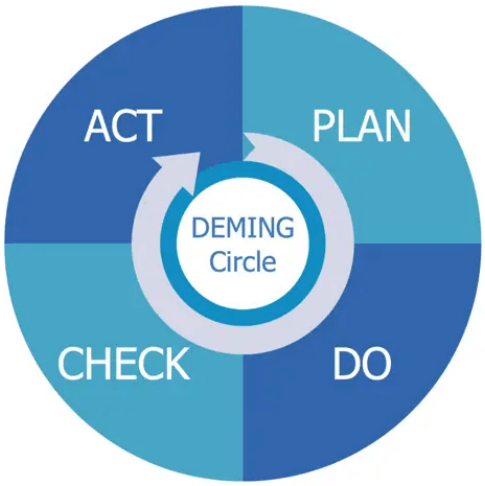
Maturity Level	Description	Program Indicators	People Indicators
STAGE 1 No Security Awareness Program	Program does not exist. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or understand organization policies, and easily fall victim to attacks. **VALUE: None – your organization is at high risk to both failing to meeting any compliance requirements and highly vulnerable to human-driven incidents.**	• There is no security awareness program. • Leadership does not discuss or care about security awareness.	• Employees never discuss security or exhibit secure behaviors.
STAGE 2 Compliance Focused	Program is designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad hoc basis. Employees are unsure of organizational policies and/or their role in protecting their organization's information assets. **VALUE: Your security awareness program meets the legal requirements your organization is required to adhere to. However your organization is not effectively managing it's human risk.**	• There is no strategic plan – training topics are ad hoc and deployed at random times. • Program has limited leadership support – leadership's goal is to maintain compliance at minimum costs. • Security awareness is only considered during audits. • Program lead is a part-time job for one single person, often someone reporting to the compliance, audit or governance teams. • There is little coordination or partnership with other departments, such as communications and human resources. • Leadership perceives security is purely a technical issue. • Training is primarily once a year. • There is little to no communication to the workforce about security beyond the annual training.	• People have a "Let's get this over with" attitude. • People feel security is something that IT takes care of, it's not their problem. • People feel security is something they have to do. • People have a negative perception of security and/or the security team.
STAGE 3 Promoting Awareness and Behavior Change	Program identifies the target groups and training topics that have the greatest impact in supporting the organization's mission and focuses on those key elements. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work and at home. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents. **VALUE: Your organization is not only meeting its compliance requirements, but is able to effectively manage and measure it's human risk.**	• Leadership understands and commits to the need for managing human risk. • There is a strategic plan that has identified the scope of the project, goals, objectives and justification for the program. • Security team has identified and can explain their top human risks and the behaviors that most effectively manage those risks. • Program has sufficient leadership support to provide resources necessary and has an executive champion. • Security awareness is considered part of the organization's overall security effort. • Program lead is dedicated full time to the effort, has a strong communication skills and is a part of the security team. • Program coordinates and collaborates with various departments within organization, including Communications, Human Resources, and Help Desk. Often this coordination is done through an Advisory Board. • Program has gone beyond just annual training and includes continuous reinforcement throughout the year. Usually also includes a phishing program. • Program works to positively engage the workforce.	• Employees understand that security technology alone cannot protect them and they have a responsibility to protect themselves and the organization's assets. • People are reporting incidents or suspected attacks. • When security team pushes out information, people are asking them questions. • Employees are exhibiting the behaviors they are being trained on. • Employees bring strong security behaviors home.

Kuva 5. Maturiteettimallin indikaattorimatriisi [7].

On yleistä, että organisaatiot eivät sijoitu vain yhteen tasoon, vaan niiden kypsyys vaihtelee eri tasojen välillä riippuen siitä, mihin tietoisuuden kehittämisen osa-alueisiin on panostettu.

8.3 Systemaattinen kehittäminen

Tietoturvatietoisuuden kehittämisprosessia voidaan lähestyä tehokkaasti PDCA-mallin (Plan-Do-Check-Act) avulla, joka sisältää neljä keskeistä vaihetta: suunnittele, toteuta, arvioi ja toimi. Tämä malli soveltuu erityisen hyvin jatkuvaan tietoturvatietoisuuden kehittämiseen, sillä useiden muiden ISO-standardien tapaan, myös ISO/IEC 27000 -standardisarja pohjautuu PDCA-malliin. Malli tarjoaa hyödyllisen viitekehyksen, jonka avulla voidaan arvioida ja kehittää tietoturvatietoisuusohjelmien tehokkuutta sekä käytettyjen menetelmien vaikuttavuutta [36]. PDCA-mallia kutsutaan joskus myös Demingin laatuympyräksi sen kehittäjän mukaan (Kuva 6).



Kuva 6. PDCA-malli eli Demingin laatuympyrä [37].

PDCA-mallin ensimmäinen vaihe, suunnitteluvaihe (Plan), keskittyy tietoturvatietoisuuden kehittämisessä nykytilan analysointiin ja kehityskohteiden tunnistamiseen. Tässä vaiheessa esimerkiksi kartoitetaan organisaation

tietoisuusohjelman lähtötaso, määritellään konkreettiset tavoitteet ja suunnitellaan toimenpiteet, joilla parantaa tietoisuutta.

Toisessa vaiheessa, toteutusvaiheessa (Do), suunnitellut ratkaisut viedään käytäntöön. Tämä voi sisältää esimerkiksi tietoturvakoulutusten järjestämistä, viestintäkampanjoiden käynnistämistä tai erilaisten teknisten ratkaisujen käyttöönottoa. Tärkeää on, että toimenpiteet toteutetaan hallitusti ja dokumentoidaan mahdollisia myöhempiä arviointeja varten.

Kolmas vaihe, arviointivaihe (Check), keskittyy tulosten mittaamiseen ja tavoitteiden saavuttamisen arviointiin. Tietoturvatietoisuuden kehittämisessä tämä tarkoittaa esimerkiksi osallistumisasteiden, kyselytulosten tai tietoturvaloukkausten määrän tarkastelua. Tuloksia verrataan suunnitteluvaiheessa asetettuihin tavoitteisiin, jotta voidaan arvioida toimenpiteiden tehokkuutta.

Neljäs vaihe, toimintavaihe (Act), perustuu arviointivaiheessa saatuihin tietoihin. Jos ratkaisut osoittautuivat toimiviksi, ne integroidaan pysyväksi osaksi organisaation toimintaa ja kulttuuria. Jos taas tavoitteita ei saavutettu, PDCA-sykliä jatketaan tekemällä uusia muutoksia ja aloittamalla sykli alusta. Tämä jatkuva kehitysmalli mahdollistaa organisaation sopeutumisen ja parantamisen pitkällä aikavälillä.

Neljäs vaihe, toimintavaihe (Act), perustuu arviointivaiheessa saatuihin havaintoihin. Jos toimenpiteet ovat osoittautuneet tehokkaiksi, ne integroidaan pysyvästi organisaation käytäntöihin ja kulttuuriin. Jos tavoitteita ei saavutettu, sykliä jatketaan uusien kehitystoimenpiteiden avulla. Tämä jatkuva kehitysmalli mahdollistaa organisaation sopeutumisen ja parantamisen pitkällä aikavälillä.

8.4 Arviointi ja mittaaminen

Tietoturvatietoisuuden kehittämisessä on olennaista jatkuva arviointi ja mittaaminen, jotta kehittämistyö tuottaisi lisäarvoa organisaatiolle ja antaisi johdolle selkeän kuvan tietoturvan tilasta. Tietoisuusohjelman luominen ei

itsessään takaa, että kaikki työntekijät ymmärtäisivät ja noudattaisivat organisaation tietoturvakäytäntöjä, minkä vuoksi on tärkeää tarkastella säännöllisesti menetelmien tehokkuutta, onnistumisia sekä tunnistaa tulevaisuuden kehityskohteita. Jatkuva parantaminen edellyttää tietoa siitä, miten nykyiset toimintatavat toimivat käytännössä ja ilman tätä tietoa kehitys voi pysähtyä kokonaan.

Tietoturvatietoisuuden mittaaminen voi olla haastavaa, sillä ihmisten käyttäytymistä on vaikea mitata objektiivisesti ja johdonmukaisesti. Eri kohderyhmillä on erilaiset tarpeet ja taustat, mikä tekee yleispätevien mittareiden käyttämisen haastavaksi. Kehittämiselle on olennaista, että ohjelmalle asetetaan selkeät mittarit, joiden avulla edistystä voidaan seurata ja arvioida. ENISA korostaa, että ennen ohjelman käynnistämistä on tärkeää määrittää organisaation lähtötaso, jotta ohjelman vaikutuksia voidaan mitata konkreettisesti. Lähtötason määrittäminen tarjoaa mahdollisuuden osoittaa tietoisuusohjelman tuomat hyödyt ja kehityksen. Lisäksi selkeiden mittareiden avulla voidaan tarkastella, kuinka hyvin ohjelma saavuttaa tavoitteensa. Näin tietoisuusohjelman vaikutukset voidaan perustella ja ohjelman kehittämistä jatkaa tehokkaaksi. [38]

Usein käytettyjä mittareita ovat esimerkiksi palautekyselyiden tulokset, tietoturvakoulutusten suoritusprosentit ja tietoturvaloukkausten lukumäärä.

ENISA korostaa, että yritysten tietoisuusohjelman onnistumiselle on välttämätöntä, ettei se ole ristiriidassa organisaation kulttuurin kanssa ja sillä on ylimmän johdon tuki. Ohjelmien jatkuvan tuen varmistaminen edellyttää myös, että tietoturvatietoisuuden lisäämisen hyödyt voidaan konkreettisesti osoittaa. [38]. Tässä tutkimuksessa kyselylomakkeen tuloksilla on erittäin suuri merkitys.

8.4.1 HAIS-Q arviointimalli

Tietoturvatietoisuuden arviointiin on olemassa useita erilaisia malleja, jotka painottavat eri osa-alueita, kuten käyttäytymistä, asenteita tai yleistä tietoturvatietoisuuden tasoa. Tämä tutkimus valitsi käytettäväksi HAIS-Q-mallin,

eli *Human Aspects of Information Security Questionnaire* -lomakkeen sen kokonaisvaltaisuuden ja käytännönläheisyyden vuoksi. HAIS-Q, on kyselytyökalu, jonka tarkoituksena on mitata työntekijöiden tietoturvatietoisuutta kolmen keskeisen osa-alueen avulla: tieto, asenne ja käyttäytyminen (Knowledge, Attitude, Behaviour – KAB).

Malli perustuu edellä esitettyyn ajatukseen, että tietoturvatietoisuus ei perustu ainoastaan tietoon organisaation tietoturvakäytännöistä, vaan myös työntekijöiden asenteisiin ja tapoihin toimia tietoturvatilanteissa. HAIS-Q-mallia käytetään myös arvioimaan koulutusten tehokkuutta, ja se auttaa tunnistamaan ne työntekijäryhmät, jotka voivat hyötyä kohdennetusta tietoturvakoulutuksesta

Mallin avulla voidaan tarkastella työntekijöiden tietoturvatietoisuuden eri osa-alueita systemaattisesti, mikä antaa kattavan käsityksen organisaation tietoturvatietoisuuden nykytilasta. Malli tarjoaa selkeitä mittareita, joiden pohjalta voidaan suunnitella kohdennettuja kehittämistoimenpiteitä. Tämä tekee HAIS-Q mallista erityisen hyödyllisen työkalun kohdeorganisaatioille, jossa halutaan arvioinnin lisäksi, myös jatkuvasti kehittää tietoturvatietoisuutta. [3]

Kyseistä mallia on hyödynnetty onnistuneesti myös muissa vastaavissa tutkimuksissa, kuten Tallinnan Yliopiston *Information Security Awareness of Librarians in the Baltic Countries: A Comparative Analysis* [39].

Alkuperäinen HAIS-Q lomake sisältää kysymyksiä seitsemältä eri tietoturvan osa-alueelta, joista esitetään yhteensä 63 kysymystä [11]. Kysymykset kategorisoidaan kolmeen eri KAB-mallin luokkaan kuvan 7 mukaisesti. Alkuperäiset osa-alueet ovat salasanakäytännöt, sähköpostiturvallisuus, Internetin käyttö, sosiaalinen media, mobiililaitteet, tietojen käsittely sekä fyysinen turvallisuus.

Kysymyksissä käytetään yleensä 5-portaista Likert-asteikkoa (esim. 1–5, missä 1 tarkoittaa "täysin eri mieltä" ja 5 "täysin samaa mieltä"). Likert-asteikko mahdollistaa vastaajien suhtautumisen arvioinnin sekä positiiviseen että negatiiviseen suuntaan.

Lomakkeen monipuolinen rakenne antaa siis organisaatiolle mahdollisuuden kartoittaa tietoturvatietoisuutta monista näkökulmista, jolloin saadaan tarkempi ymmärrys työntekijöiden tietoturvakäyttäytymisestä ja mahdollisista kehitystarpeista.

Esimerkki kysymystyypeistä kunkin pääkategorian osalta voisi olla:

- Tieto: "Ymmärrän, miksi salasanojen tulee olla monimutkaisia."
- Asenne: "On tärkeää, että en käytä samaa salasanaa useissa eri palveluissa."
- Käyttäytyminen: "Vaihdan salasanani säännöllisesti."

Table 5 – HAIS-Q items.

	Knowledge	Attitude	Behaviour
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my work accounts. ^	It's safe to use the same password for social media and work accounts. ^	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues. ^	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues. ^
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. ^	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know. ^	It's always safe to click on links in emails from people I know. ^	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender. ^	If an email from an unknown sender looks interesting, I click on a link within it. ^
Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders. ^	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.

Kuva 6. HAIS-Q lomakkeen alkuperäinen versio [11].

Kohdeorganisaation tapauksessa vakiolomakkeeseen tehtiin muutoksia sekä mitattavien osa-alueiden että kysymysten osalta. Kyselyn haluttiin palvelevan parhaalla mahdollisella tavalla juuri tilaajan tarpeita, ja osa vakiolomakkeen kysymyksistä ei ollut siellä relevantteja.

Muokattu kyselylomake on liitteenä, Liite 1.

8.4.2 Knowledge-Attitude-Behaviour -malli

Edellä esitelty HAIS-Q työkalu perustuu KAB-malliin, eli Knowledge-Attitude-Behaviour-malliin. KAB-mallin keskeinen ajatus on, että yksilön tietoturvatietoisuus ei perustu ainoastaan tietoon organisaation tietoturvakäytännöistä, vaan myös siihen, millaiset asenteet ja toimintatavat vaikuttavat henkilön kykyyn toimia tietoturvallisesti arjessa. KAB-malli muodostaa näin perustan monille tietoturvatietoisuuden arviointimenetelmille, kuten HAIS-Q.

Mallin keskeiset elementit ovat:

- Tieto (Knowledge): Työntekijän tietämys tietoturvakäytännöistä ja -riskeistä. Kun työntekijät tietävät, mitä tietoturvaohjeita noudattaa ja miksi, he voivat tunnistaa riskejä paremmin ja tehdä tietoon perustuvia päätöksiä.
- Asenne (Attitude): Tapa, jolla työntekijät suhtautuvat tietoturvaan ja sen käytäntöihin. Positiivinen asenne tietoturvaa kohtaan auttaa sitoutumaan käytäntöihin ja vahvistaa halua toimia oikein.
- Käyttäytyminen (Behaviour): Tapa, miten työntekijät toimivat käytännössä tietoturvatilanteissa. Tämä tarkoittaa esimerkiksi sitä, että työntekijä noudattaa tietoturvaohjeita päivittäisissä tehtävissään ja välttää riskialttiita toimintoja, kuten epäilyttävien linkkien avaamista.

Mallin mukaan yksilön tietoisuus lisää myönteisiä asenteita tietoturvakäytäntöjä kohtaan, ja yhdessä nämä vaikuttavat siihen, että työntekijä toimii tietoturvallisesti. [11].

9 Tutkimuksen toteutus

Vaikka tutkimuksessa pyrittiin säilyttämään alkuperäisen tutkimuslomakkeen rakenne mahdollisuuksien mukaan samana, muutoksia oli tehtävä, jotta kysymykset palvelisivat mahdollisimman hyvin tilaajan tarpeita. Alkuperäisessä versiossa on muun muassa Social Media Use-niminen tutkittava osa-alue, jota ei katsottu tarpeelliseksi tutkia, sekä Mobile Devices-niminen alue joka meidän kielialueellamme mielletään yleensä matkapuhelimiin liittyväksi, vaikka alkuperäisessä versiossa sillä tarkoitetaan kaikkia työntekijöiden käytössä olevia päätelaitteita. Muiden alueiden osalta tehtiin uudelleennimeämisiä, yhdistämisiä tai ne pidettiin ennallaan. Lähes kaikki kysymykset ja väittämät muotoiltiin uudestaan, jotta ne saatiin vastaamaan kohdeorganisaation tarpeita. Myös kieliasua muokattiin helpommin ymmärrettävään muotoon. Lopulliset seitsemän tutkimukseen valittua osa-aluetta esitellään seuraavaksi:

Password Management. Alkuperäinen osa-alue. Muokattiin vastaamaan organisaation tarpeita ja ottamaan huomioon heidän hallintajärjestelmänsä. Sisältää kolme kysymystä.

Phishing Awareness and Email Use. Muokattu osa-alue, alkuperäisessä ainoastaan Email Use. Muokattiin tuomalla mukaan tietojenkalasteluun liittyviä kysymyksiä. Sisältää kolme kysymystä.

Internet Use and Online Behaviour. Muokattu osa-alue, alkuperäisessä ainoastaan Internet Use. Muokattiin organisaation tarpeisiin sopivammaksi. Sisältää kolme kysymystä.

Security Updates and System Maintenance. Uusi osa-alue, joka koettiin tärkeäksi tuoda tutkimukseen mukaan. Sisältää kolme kysymystä.

Secure Data Handling. Muokattu osa-alue, alkuperäisessä Information Handling. Laajennettiin vastaamaan organisaatiolle tärkeitä mitattavia kohteita. Sisältää kolme kysymystä.

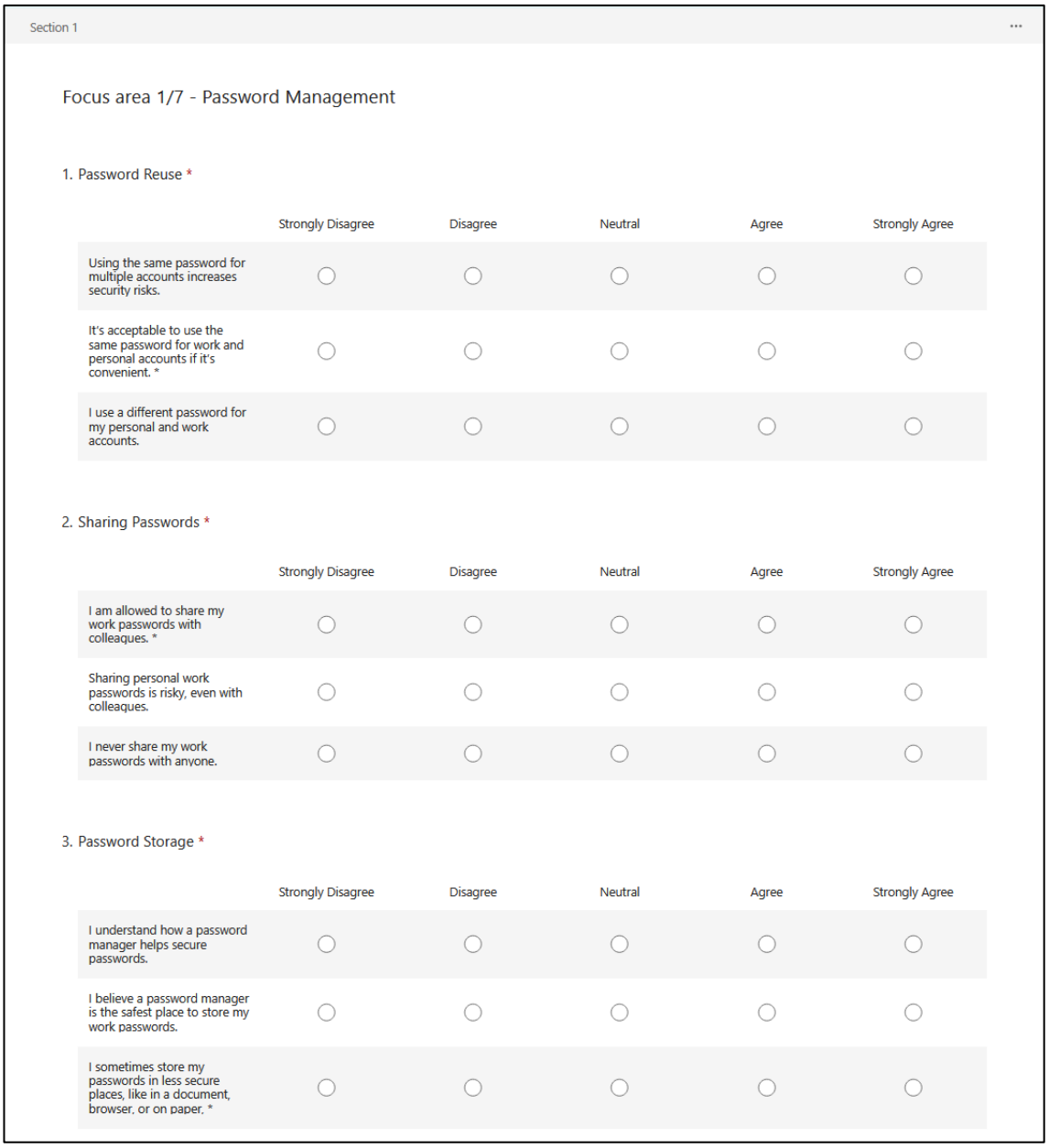
Incident Reporting and Response Guidelines. Muokattu osa-alue, alkuperäisessä Incident Reporting. Laajennettiin koskemaan myös muuta toimintaa, kuin loukkausten raportointia. Sisältää kolme kysymystä.

Company Security Practices. Uusi osa-alue. Keskittyy organisaation omien tietoturvakäytäntöjen ymmärtämiseen ja noudattamiseen. Erittäin oleellinen osa tutkimusta. Sisältää viisi kysymystä.

9.1 Tulosten analysointi

Kysely toteutettiin organisaatiossa sähköisenä verkkokyselynä käyttäen Microsoft Forms-ohjelmaa, ja vastausaikaa annettiin kaksi viikkoa. Kyselyn täyttämiseen ei edellytetty kirjautumista, vaan se oli käytettävissä vastaajan päätelaitteella helposti vain oikean URL-osoitteen tietämällä. Kuvassa 8 on esitetty malli Forms-kyselyn lomakkeesta, jossa mitattiin henkilökunnan toimintaa salasanojen hallinnan osalta.

Henkilökuntaa tiedotettiin kyselystä organisaation sisäisessä viestintäkanavassa, ja osallistumisesta muistutettiin kahdesti. Lopullinen vastaajamäärä oli 35 ja vastausprosentti 67 %, mikä on tämän tyyppisissä tutkimuksissa erittäin hyvä tulos [40]. Ensimmäinen muistutus lähetettiin kymmenen päivää kyselyn avaamisen jälkeen, jolloin vastausprosentti oli 45 %. Muistutuksen jälkeen se nousi 60 prosenttiin, ja viimeisenä vastauspäivänä lähetetyn toisen muistutuksen jälkeen lopullinen vastausprosentti oli 67 %, mikä tarkoittaa 35 vastaajaa. Vastaajista 89 % ilmoitti vapaaehtoisen osastotiedon. Tuloksissa laskettiin jokaisesta mitatusta osa-alueesta aritmeettinen keskiarvo ja keskihajonta sekä Pearsonin korrelaatiot eri K, A ja B-osioiden välillä.


Section 1

Focus area 1/7 - Password Management

1. Password Reuse *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Using the same password for multiple accounts increases security risks.	○	○	○	○	○
It's acceptable to use the same password for work and personal accounts if it's convenient. *	○	○	○	○	○
I use a different password for my personal and work accounts.	○	○	○	○	○

2. Sharing Passwords *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am allowed to share my work passwords with colleagues. *	○	○	○	○	○
Sharing personal work passwords is risky, even with colleagues.	○	○	○	○	○
I never share my work passwords with anyone.	○	○	○	○	○

3. Password Storage *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I understand how a password manager helps secure passwords.	○	○	○	○	○
I believe a password manager is the safest place to store my work passwords.	○	○	○	○	○
I sometimes store my passwords in less secure places, like in a document, browser, or on paper. *	○	○	○	○	○

Kuva 8. Esimerkki Microsoft Forms kyselylomakkeesta

9.1.1 Korrelaatioanalyysi

Korrelaatioanalyysi on keskeinen menetelmä tutkittaessa eri muuttujien välistä yhteyttä ja niiden mahdollisia vaikutussuhteita [41]. Pearsonin korrelaatiokerroin (r) auttaa ymmärtämään, kuinka vahvasti kaksi muuttujaa ovat lineaarisesti yhteydessä toisiinsa. Tässä tutkimuksessa korrelaation tarkastelu on tärkeää erityisesti siksi, että se auttaa arvioimaan KAB-mallin mukaisia suhteita.

Tietoturvatiedon (K) ja asenteiden (A) välinen yhteys kertoo, miten hyvin henkilöstön tietotaso heijastuu heidän asenteisiinsa. Tietoturva-asenteiden (A) ja käyttäytymisen (B) välinen korrelaatio antaa viitteitä siitä, kuinka vahvasti myönteinen suhtautuminen tietoturvaan näkyy käytännön toiminnassa. Tietotason (K) ja käyttäytymisen (B) välinen suhde voi paljastaa, missä määrin tietoturvatietoisuus siirtyy konkreettisiksi toimintatavoiksi.

Korrelaatiota tulkittaessa on tärkeää ymmärtää, mitä eri arvot käytännössä tarkoittavat. Pearsonin r-arvon vaihteluväli on -1 ja +1, jossa esimerkiksi [42]:

- 0,00–0,19 viittaa hyvin heikkoon tai olemattomaan yhteyteen
- 0,20–0,29 tarkoittaa heikkoa positiivista korrelaatiota
- 0,30–0,39 kuvaa kohtalaista korrelaatiota
- 0,40–0,69 osoittaa vahvaa korrelaatiota
- 0,70–1,00 viittaa erittäin vahvaan yhteyteen.

Tulkinnan kannalta erityisesti kohtalainen tai vahva korrelaatio ($r > 0.40$) voidaan nähdä merkittävänä, sillä se kertoo muuttujien välisestä systemaattisesta yhteydestä. Jos korrelaatiot ovat vahvoja, voidaan päätellä, että esimerkiksi korkea tietoturvatietoisuus vaikuttaa suoraan turvallisiin toimintatapoihin. Jos taas yhteys on heikko, se voi viitata siihen, että pelkkä tieto ei riitä muuttamaan käyttäytymistä, vaan sitä tulee vahvistaa esimerkiksi koulutuksella tai ohjeistuksella.

Vaikka korrelaatio on erinomainen tapa ymmärtää muuttujien vaikutussuhteita, se on menetelmänä herkkä yksittäisille poikkeaville arvoille. Siksi tieteellisessä tutkimuksessa voidaan käyttää virheellisten ääriarvojen poistamiseen esimerkiksi Z-Score-nimistä menetelmää, jolla ääriarvot voidaan perustellusti jättää huomiotta [43]. Tässä tutkimuksessa korrelaatiot esitetään sekä raakadataan perustuen, että Z-Score menetelmällä korjattuina.

9.1.2 Keskihajonta

Hajonta (σ) on tilastollinen mittari, joka kuvaa, kuinka paljon yksittäiset vastaukset poikkeavat keskiarvosta [41]. Se antaa lisätietoa vastausjoukon vaihtelusta ja auttaa ymmärtämään, kuinka yhtenäisiä tai hajanaisia vastaajat ovat tietyn muuttujan suhteen. Keskiarvo yksinään voi antaa harhaanjohtavan kuvan tuloksista, sillä se ei kerro, kuinka laajasti vastaukset ovat jakautuneet. Esimerkiksi, jos kahdella eri kysymyksellä on sama keskiarvo, mutta toisessa vastaajien mielipiteet ovat keskittyneet lähelle keskiarvoa ja toisessa ne jakautuvat laajasti, hajonnan avulla tämä ero tulee näkyviin.

Tässä tutkimuksessa hajonta esitetään keskiarvon rinnalla jokaisen fokusalueen osalta, jotta voidaan tunnistaa mahdollisia vaihteluita vastaajien välillä. Suuri hajonta voi viitata esimerkiksi siihen, että vastaajajoukossa on erilaisia käsityksiä tai toimintatapoja, kun taas pieni hajonta osoittaa, että vastaajat ovat vastanneet kysymykseen melko yhtenäisesti. Tämä auttaa arvioimaan, kuinka tasaisesti tietoturvatietoisuus on jakautunut organisaatiossa ja mitkä osa-alueet voivat vaatia lisäkoulutusta tai selkeyttämistä.

Vastausten hajonta on laskettu vastaajien Likert-asteikon vastauksista, jossa asteikko oli 1–5, ja arvot kuvaavat vastausten keskihajontaa. Pienempi hajontalukema tarkoittaa, että vastaajien näkemykset ovat yhtenäisiä, kun taas suurempi hajonta viittaa vastaajien mielipiteiden hajanaisuuteen. Hajonnan arvoja voidaan tulkita seuraavasti:

- Alle 0,5: Vastaajat ovat vastanneet hyvin samansuuntaisesti, eli käsitys asiasta on hyvin yhtenäinen
- 0,5–1,0: Vastaajat ovat pääosin samaa mieltä, mutta joukossa on jonkin verran vaihtelua
- 1,0–1,5: Näkemysten välillä on merkittäviä eroja, mikä voi viitata epäselvyyksiin tai eri taustatietoihin.

9.1.3 Cronbachin alfa

Cronbachin alfa (α) on yleisesti käytetty tilastollinen mittari, jolla arvioidaan kyselylomakkeen eri väittämien sisäistä johdonmukaisuutta ja luotettavuutta [41]. Korkea alfa-arvo viittaa siihen, että kyselyn väittämät mittaavat samaa ilmiötä johdonmukaisesti, kun taas matala arvo voi osoittaa epäjohdonmukaisuutta tai sitä, että väittämät eivät mittaa yhtenäistä käsitettä.

Tässä tutkimuksessa Cronbachin alfa laskettiin kaikkien vastausten perusteella, eikä erikseen jokaisen fokusalueen osalta. Alfa-arvon tulkinnassa käytetään yleisesti hyväksyttyjä raja-arvoja, joiden mukaan arvo 0,70 tai suurempi, viittaa jo riittävään johdonmukaisuuteen. Arvoja 0,80–0,89 pidetään hyvinä ja luotettavina, jolloin väittämät mittaavat samaa ilmiötä ilman liiallista päällekkäisyyttä. Arvo 0,90 ja isompi on jo erittäin luotettava, mutta hyvin korkea arvo voi myös viitata siihen, että osa väittämistä on päällekkäisiä tai liian samanlaisia.

Kyselylomakkeen vastaukset muunnettiin numeeriseen muotoon siten, että Strongly Agree sai arvon 5, Agree arvon 4, Neutral säilyi arvossa 3, Disagree sai arvon 2 ja Strongly Disagree arvon 1. Negatiivisesti muotoilluissa kysymyksissä asteikko käännettiin päinvastaiseksi, jolloin esimerkiksi arvo 1 muuttui arvoksi 5 ja arvo 2 muuttui arvoksi 4.

9.2 Tulosten yleiskuvaus

Tässä alaluvussa esitellään yhteenveto kaikista kyselyn vastauksista. Jokaista KAB-arvoa mitattiin kyselyssä 23 kysymyksellä, jotka olivat seitsemästä eri osa-alueesta. Jokainen kysymys koostui kolmesta väittämästä, pois lukien viimeinen osa-alue, Company Security Practices, johon oli määritelty viisi väittämää. Vastaajia oli yhteensä 35 ja koska kaikki kysymykset oli määritelty pakollisiksi vastattaviksi, taulukon 3 tulokset ovat muodostuneet 805 vastauksesta. Taulukossa 3 on esitetty tulokset kaikkien vastaajien osalta, sekä tutkimuksen luotettavuutta mittaava Cronbachin alfa-arvo.

Taulukko 3. Yhteenveto kaikista vastauksista

Kategoria	Keskiarvo	Keskihajonta (σ)	Cronbachin alfa (α)
K (Knowledge)	4,63	0,64	0,86
A (Attitude)	4,56	0,74	0,84
B (Behaviour)	4,30	0,88	0,86

Tutkimuksen K-kategorian vastausten keskiarvo (4,63) osoittaa henkilöstön hyvää kykyä tunnistaa ja ymmärtää tietoturvauhkia. Kategorian vastausten hajonta oli myös vähäistä ja laskettu luotettavuus hyvä, eli voidaan arvioida, että hyvä tietoturvan osaaminen kattaa koko organisaation, riippumatta työntekijän osastosta tai työtehtävästä.

Tutkimuksen A-kategorian tulos on myös hyvä (4,56) eli vastauksista voidaan päätellä pääosin myönteistä suhtautumista kyberuhkien käsittelyyn. Tulosten perusteella työntekijät asennoituvat hyvin tietoturvaan ja suhtautuvat siihen vakavasti, ja näin ymmärtävät sen tärkeyden organisaation liiketoiminnassa.

Tutkimuksen käyttäytymistä mittaavassa B-kategoriassa oli havaittavissa enemmän vaihtelua. Vaikka vastaajat tuntevat ja suhtautuvat myönteisesti tietoturvauhkien käsittelyyn, heidän käytännön toimintansa on jonkin verran epätasaisempaa. On kuitenkin huomionarvoista, että myös Behaviour-kategorian arvosana oli hyvä (4,30), mutta kuitenkin heikoin kaikista mitatuista.

Likert-skaalaa käyttävien kysymysten lisäksi vastaajia pyydettiin arvioimaan asteikolla 1–10 omaa vastaushetken valmiuttaan tunnistaa kyberriskejä, sekä omaa valmiuttaan reagoida niihin oikein. Oikein reagoimista ei kuvattu tarkemmin, ja oikea toiminta jätettiin näin vastaajan itsensä arvioitavaksi. Tulokset myös tästä osuudesta ovat erittäin hyvät, vastausten keskiarvojen ollessa 8,40 ja 8,26. Kuitenkin näissä kahdessa, valmiuksia mittaavassa kysymyksessä, ilmeni erittäin suuria eroja eri osastojen välillä, mikä on luonnollista työtehtävistä johtuvien osaamiserojen vuoksi. Osastokohtaisten erojen esittäminen tässä raportissa ei ole tarkoituksenmukaista, mutta tietoa

tullaan hyödyntämään soveltavasti kuitenkin organisaation omassa koulutussuunnittelussa, jotta voidaan kohdentaa paremmin oikeita koulutuksia oikeille ryhmille.

Sähköisessä Forms-kyselyssä nämä kaksi kysymystä oli aseteltu seuraavasti:

- How confident are you in your ability to recognize a cybersecurity threat, such as a social engineering attack (e.g., phishing, smishing, scam calls)?
- How confident are you in your ability to respond correctly if you are targeted by a cybersecurity threat, such as a social engineering attack (e.g., phishing, smishing, scam calls)?

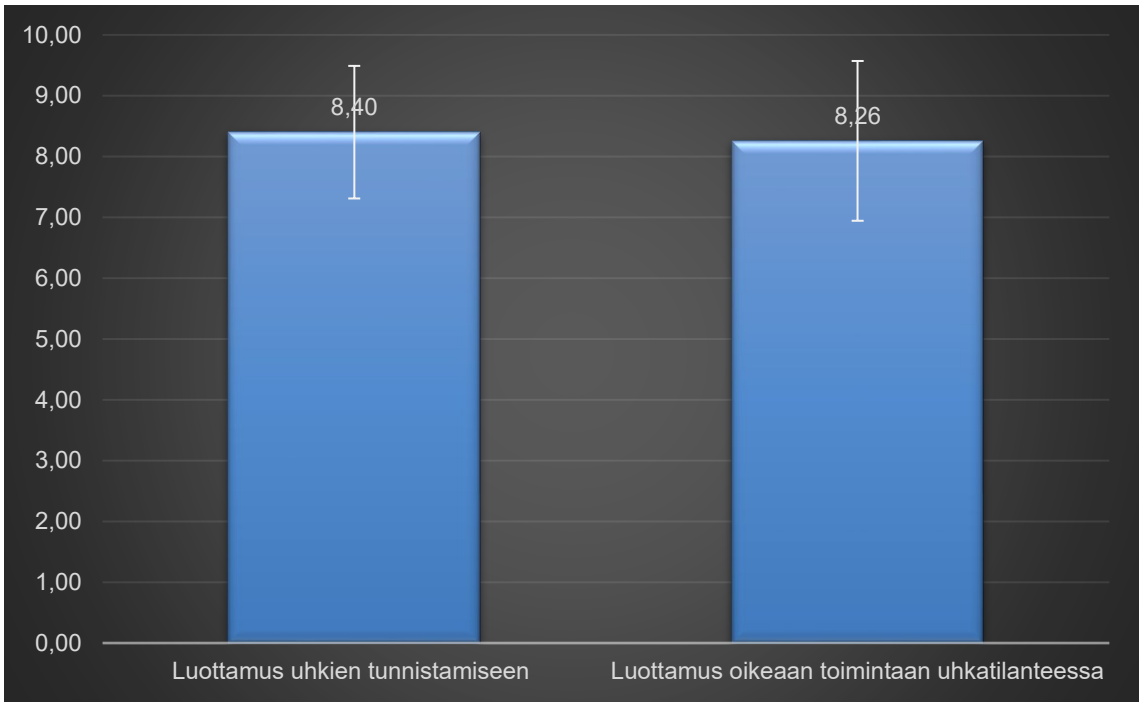
Nämä tulokset ja vastausten hajonnat on esitelty kuvassa 9.

Yhteenvetona kaikkien vastausten perusteella voidaan todeta, että organisaation henkilöstöllä on erinomainen teoreettinen tietoturvaosaaminen ja myönteinen asenne tietoturvallisuutta kohtaan. Tämä näkyy korkeina mittaustuloksina K- (4,63) ja A-kategorioissa (4,56), joiden tulosten hajonta oli vähäistä. Tuloksista voidaan päätellä, että hyvä tietoturvatietoisuus ja asenne eivät ole vain yksittäisten työntekijöiden vahvuuksia, vaan jakautuvat laajasti koko organisaatioon.

Käytännön tietoturvakäyttäytymistä mittaava B-kategoria (4,30) jäi kuitenkin hieman muita alemmaksi, mikä osoittaa, että teoriatieto ja myönteinen asenne eivät kaikissa tapauksissa suoraan johda turvallisiin toimintatapoihin. Tämä on havaittu myös muissa vastaavissa tutkimuksissa, joissa on havaittu, että käyttäytymisen kehittäminen vaatii enemmän kuin pelkästään tietoa ja ohjeistusta. Tätä havaintoa tukee myös aikaisemmin tässä tutkimuksessa mainittu organisaation kokonaisvaltaisen tietoturvakulttuurin kehittäminen. Organisaation turvalliset tavat toimia eivät synny ainoastaan ohjeita kirjoittamalla ja koulutuksia järjestämällä, vaan ne periytyvät organisaatiossa työntekijältä toiselle ja tähän voi vaikuttaa ainoastaan hyvän turvallisuuskulttuurin kautta.

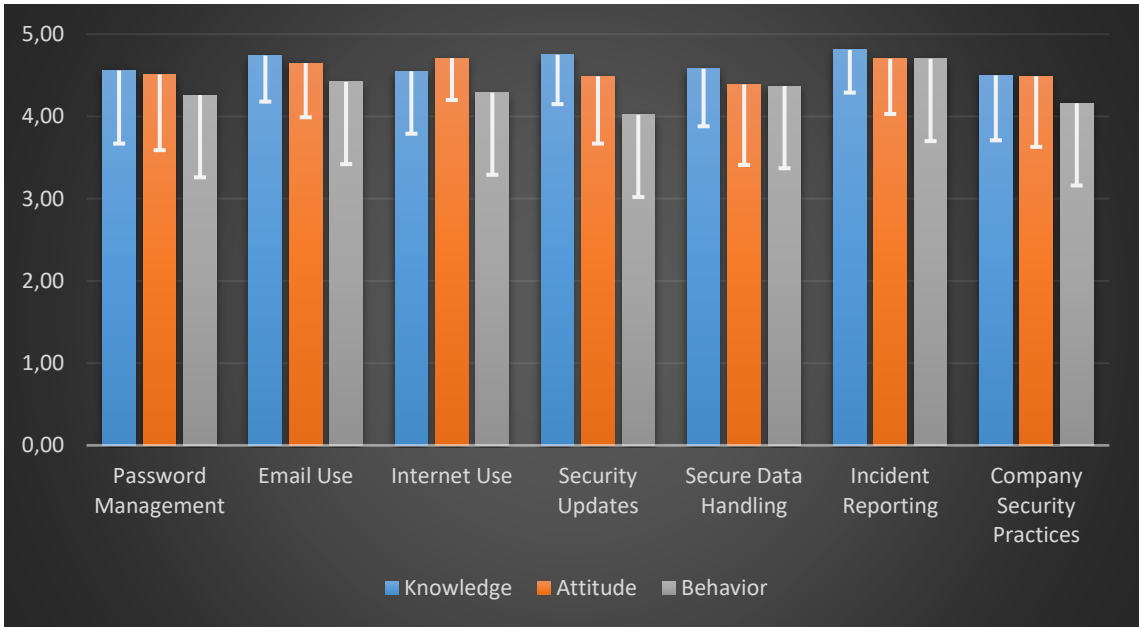
Kyselyn luotettavuutta mittaava Cronbachin alfa oli kaikissa kategorioissa korkealla tasolla (≥ 0,84), mikä osoittaa mittariston sisäisen johdonmukaisuuden

olevan hyvä. Näin ollen kyselystä saatuja havaintoja voidaan pitää luotettavina, ja ne antavat organisaatiolle arvokasta tietoa henkilöstön tietoturvatietoisuuden nykytilasta ja sen kehityskohteista. Tuloksia esitetään graafisesti seuraavissa luvuissa, kuten myös tarkemmat tulokset erikseen vielä jokaisesta tutkimuksen seitsemästä osa-alueesta.



Kuva 7. Vastaajien luottamus uhkiin reagoinnissa asteikolla 1–10

Kuvassa 10 esitetään graafisesti jokaisen mitatun osa-alueen tulokset asteikolla 0–5 sekä niiden hajonnat. Vastuksen hajontaa kuvaa palkin valkoinen viiva, ja viivan pituus korreloi hajonnan suuruuteen, niin että lyhyt viiva kertoo pienestä hajonnasta.



Kuva 8. Kaikkien-osa-alueiden keskiarvot asteikolla 0–5 ja tulosten hajonnat

Taulukossa 4 esitetään tulokset jokaisen yksittäisen kysymyksen osalta. Keskiarvon ja keskihajonnan lisäksi, tässä esitetään vastauksista myös moodi (Mo), joka on aineistossa yleisimmin esiintyvä arvo.

Taulukko 4. Yksittäisten vastausten tulokset

Fokus alue	Kysymys	Keski-arvo	Keski-hajonta	Moodi
Password Management	Password Reuse	4,65	0,87	5
	Sharing Passwords	4,51	0,93	5
	Password Storage	4,17	1,06	5
Phishing Awareness and Email Use	Recognizing Phishing Emails	4,52	0,71	5
	Clicking Links from Unknown Senders	4,74	0,59	5
	Opening Attachments	4,54	0,80	5
Internet Use and Online Behaviour	Downloading Files	4,24	0,95	5
	Accessing Websites from Work Computer	4,63	0,67	5
	Entering Information Online	4,69	0,51	5
Security Updates and System Maintenance	Security updates	4,59	0,66	5
	Security Update Skills	4,32	1,02	5
	Importance of Timely Updates	4,34	0,94	5
Secure Data Handling	Removable Media	4,43	0,96	5
	Ignoring Poor Security Behaviour	4.53	0,82	5
	Handling Classified Information	4,38	0,84	5
Incident Reporting	Reporting Missing Company Property	4,86	0,40	5
	Ignoring Poor Security Behaviour	4,62	0,61	5
	Incident Reporting	4,73	0,74	5
Company Security Practices	Awareness and Usage of Security Policies	4,43	0,77	4
	Security Incident Contacts	4,57	0,69	5
	Safeguarding Company Assets	4,12	1,13	5
	Software Installation Practices	4,19	1,00	5
	Locking Computer	4,60	0,72	5

9.3 Password Management

Tässä osiossa mitattiin henkilöstön käyttäytymistä salasanojen hallinnan osalta. Salasanojen turvallinen käyttö on keskeinen osa tutkimusta, ja kysymyksillä

kartoitettiin, miten hyvin työntekijät tunnistavat salasanojen kierrättämisen riskit, suhtautuvat salasanojen jakamiseen sekä hyödyntävät turvallisia säilytystapoja. Tulokset antoivat käsityksen siitä, missä määrin salasanojen hallintakäytännöt ovat yhdenmukaisia organisaation suositusten ja parhaiden käytäntöjen kanssa. Osa-alueen tulokset on esitetty taulukossa 5 ja kysymyskohtaiset tulokset tarkemmin edellä taulukossa 4.

Taulukko 5. Password Management alueen tulokset

Kategoria	Keskiarvo	Keskihajonta
K (Knowledge)	4,56	0,61
A (Attitude)	4,51	0,54
B (Behaviour)	4,26	0,87
Kategoria	**Korrelaatio**	**Korjattu Korrelaatio**
K -> A	0,49	0,54
K -> B	0,26	0,23
A -> B	0,24	0,14

9.4 Phishing Awareness and Email Use

Tässä osiossa arvioitiin henkilöstön osaamista ja toimintatapoja sosiaalisen manipuloinnin tunnistamisessa sekä turvallisissa sähköpostikäytännöissä. Kysymykset kartoittivat työntekijän kykyä tunnistaa phishing-viestejä, suhtautumista tuntemattomien lähettäjien linkkeihin sekä liitetiedostojen avaamiseen liittyviä käytäntöjä. Näiden osa-alueiden kautta saatiin kokonaiskuva siitä, missä määrin vastaajat tunnistavat sähköpostin tietoturvariskit ja noudattavat turvallisia toimintamalleja. Osa-alueen tulokset on esitetty taulukossa 6 ja kysymyskohtaiset tulokset edellä taulukossa 4.

Taulukko 6. Phishing Awareness and Email Use-alueen tulokset

Kategoria	Keskiarvo	Keskihajonta
K (Knowledge)	4,74	0,28
A (Attitude)	4,65	0,37
B (Behaviour)	4,42	0,56
Kategoria	**Korrelaatio**	**Korjattu Korrelaatio**
K -> A	0,56	0,41
K -> B	0,62	0,43
A -> B	0,52	0,33

9.5 Internet Use and Online Behaviour

Tässä osiossa selvitettiin turvalliseen verkkokäyttäytymiseen ja tuntemattomien tiedostojen lataamiseen ja asentamiseen liittyvää osaamista ja käyttäytymistä. Kysymyksillä kartoitettiin, miten hyvin työntekijät ymmärtävät haitallisten tiedostojen ja vaarallisten verkkosivujen tunnistamisen merkityksen, ja missä määrin he ottavat nämä ne huomioon omassa toiminnassaan. Tulokset on esitetty taulukossa 7.

Taulukko 7. Internet Use and Online Behaviour- alueen tulokset

Kategoria	Keskiarvo	Keskihajonta
K (Knowledge)	4,55	0,53
A (Attitude)	4,71	0,28
B (Behaviour)	4,29	0,42
Kategoria	**Korrelaatio**	**Korjattu Korrelaatio**
K -> A	0,73	0,71
K -> B	0,51	0,47
A -> B	0,68	0,62

9.6 Security Updates and System Maintenance

Tässä osiossa selvitettiin omien päätelaitteiden ohjelmistopäivitysten merkitystä tietoturvan kannalta sekä työntekijöiden valmiuksia huolehtia laitteidensa ajantasaisuudesta. Kysymykset kartoittivat, miten hyvin työntekijät ymmärtävät säännöllisten päivitysten tärkeyden, kuinka hyvät valmiudet heillä on suorittaa ne omatoimisesti sekä kuinka omatoimisesti he huolehtivat päivitysten tarkistamisesta. Tulokset on esitetty taulukossa 8.

Taulukko 8. Security Updates and System Maintenance-osion tulokset

Kategoria	Keskiarvo	Keskihajonta
K (Knowledge)	4,75	0,21
A (Attitude)	4,49	0,42
B (Behaviour)	4,02	0,59
Kategoria	**Korrelaatio**	**Korjattu Korrelaatio**
K -> A	0,88	0,75
K -> B	0,53	0,48
A -> B	0,62	0,56

9.7 Secure Data Handling

Secure Data Handling-osiossa tarkasteltiin tietoturvallisten toimintatapojen noudattamista, erityisesti siirrettävien tallennusvälineiden käyttöä, luottamuksellisen tiedon jakamista ja organisaation tietoluokitusten huomioimista. Kysymykset kartoittivat vastaajien tietoisuutta massamuisteista, suojattujen viestintäkanavien merkityksestä sekä organisaation ohjeiden noudattamisesta luokitellun tiedon käsittelyssä. Lisäksi arvioitiin, missä määrin työntekijät ymmärtävät tietojen suojaamisen tärkeyden osana päivittäisiä työtehtäviä. Tulokset on esitetty taulukossa 9.

Taulukko 9. Secure Data Handling-osion tulokset

Kategoria	Keskiarvo	Keskihajonta
K (Knowledge)	4,58	0,44
A (Attitude)	4,39	0,60
B (Behaviour)	4,37	0,73
Kategoria	**Korrelaatio**	**Korjattu Korrelaatio**
K -> A	0,56	0,46
K -> B	0,45	0,40
A -> B	0,34	0,41

9.8 Incident Reporting and Response Guidelines

Tässä osiossa tutkittiin organisaation tietoturvapoikkeamien ilmoittamiseen liittyviä käytäntöjä ja henkilöstön valmiuksia raportoida havaitsemiaan turvallisuusuhkia. Kysymykset käsittelivät muun muassa varastetun tai kadonneen IT-omaisuuden ilmoittamista, heikon tietoturvakäyttäytymisen tunnistamista ja siihen puuttumista sekä vastaajan kynnystä ilmoittaa tietoturvapoikkeamasta. Tulokset on esitelty taulukossa 10.

Taulukko 10. Incident Reporting and Response Guidelines-osion tulokset

Kategoria	Keskiarvo	Keskihajonta
K (Knowledge)	4,81	0,20
A (Attitude)	4,70	0,36
B (Behaviour)	4,70	0,34
Kategoria	**Korrelaatio**	**Korjattu Korrelaatio**
K -> A	0,36	0,42
K -> B	0,32	0,68
A -> B	0,09	0,21

9.9 Company Security Practices

Tämä osio on erityisen keskeinen, sillä se käsittelee työntekijöiden toimintaa organisaation omien tietoturvakäytäntöjen noudattamisessa. Osiossa esitettiin enemmän kysymyksiä kuin muissa, koska sen käsittelemät aiheet vaikuttavat suoraan työntekijöiden päivittäisiin valintoihin ja toimintatapoihin.

Kysymykset käsittelivät muun muassa organisaation tietoturvapolitiikkojen tuntemusta, oikeiden raportointikanavien hyödyntämistä, yrityksen omaisuuden suojaamista, ohjelmistojen asennuskäytäntöjä sekä työasemien lukitsemiskäytäntöjä. Kysymysten laajempi määrä mahdollisti yksityiskohtaisemman tarkastelun siitä, miten hyvin organisaation omat käytännöt ovat mukana päivittäisessä toiminnassa. Tulokset on esitelty taulukossa 11.

Taulukko 11. Company Security Practices-osion tulokset

Kategoria	Keskiarvo	Keskihajonta
K (Knowledge)	4,50	0,50
A (Attitude)	4,49	0,58
B (Behaviour)	4,16	0,73
Kategoria	**Korrelaatio**	**Korjattu Korrelaatio**
K -> A	0,75	0,70
K -> B	0,71	0,69
A -> B	0,52	0,49

10 Tutkimuksen yhteenveto ja kehitysehdotukset

Tutkimus vastasi tarpeeseen mitata organisaation henkilöstön osaamista tietoturvasta sekä asenteita ja käyttäytymistä erilaisissa tilanteissa.

Tietoturvatietoisuus ei ole vain tekninen kysymys, vaan merkittävä osa organisaation kokonaisturvallisuutta. Henkilöstön sitouttaminen valppauteen ja oikeisiin toimintatapoihin on keskeistä, erityisesti sosiaalisen manipuloinnin ja muiden ihmisiin kohdistuvien hyökkäysten torjumisessa. Näiden uhkien merkitys tulee jatkossa entisestään kasvamaan, mikä korostaa tarvetta jatkuvalle kehittämiselle ja koulutukselle.

Monet toisistaan riippumattomat tutkimukset osoittavat, että haittaohjelmat, kiristyshaittaohjelmahyökkäykset, nollapäivähaavoittuvuudet, sosiaalinen manipulointi, tietojenkalastelu, toimitusketjuhyökkäykset sekä identiteettiin kohdistuvat hyökkäykset tulevat hallitsemaan uhkakenttää myös tulevina vuosina [1] [5] [44] [45] [46] [6] [49]. Vaikka tekniset suojaukset kehittyvät, ihmisiin kohdistuvat hyökkäykset säilyvät tehokkaina, sillä ne hyödyntävät inhimillisiä heikkouksia eikä pelkästään teknisiä haavoittuvuuksia. Sosiaaliseen manipulointiin perustuvat hyökkäykset voivat olla erittäin haastavia torjua jopa kokeneille tietoturvatiimeille. Niiden tunnistaminen on vaikeaa, ja teknisillä ratkaisuilla on haastavaa estää käyttäjiä klikkaamasta haitallista linkkiä tai paljastamasta arkaluonteista tietoa puhelimessa [50].

Kaikkia edellä mainittuja uhkia voidaan kuitenkin joko suoraan tai välillisesti vähentää kehittämällä organisaation henkilöstön osaamista ja turvallisuustietoista käyttäytymistä. Tietoturvakoulutuksen ja jatkuvan tietoisuuden lisäämisen avulla voidaan pienentää riskiä, että työntekijät joutuvat onnistuneen hyökkäysten kohteeksi tai toimivat vahingossa osana hyökkäysketjua.

10.1 Tutkimuksen tulosten yhteenveto

Kuten aiemmin on esitelty, tutkimus mittasi henkilöstön osaamista ja toimintaa KAB-mallin mukaisesti asteikolla 1–5. Tulosten perusteella tietotaso (K) organisaatiossa on poikkeuksellisen korkealla tasolla, ja keskiarvo 4,63 on lähellä kiitettävää. Tämänkaltaista tulosta voisi odottaa työntekijöiltä, joiden päivittäisiin tehtäviin kuuluu tietoturvakriittisiä vastuualueita, kuten tietoturvallinen ohjelmistokehitys tai infrastruktuuri, mutta kyselyssä kerätyn osastotiedon perusteella korkea osaamistaso oli läpileikkaavaa koko organisaatiossa. Tämä viittaa siihen, että koko yrityksen henkilöstöllä on vahva kyky tunnistaa tietoturvauhkia työssään ja erinomainen teoreettinen osaaminen toimia oikein.

Vaikka tietoisuuden taso oli korkea, asenteissa (A) ja käyttäytymisessä (B) havaittiin enemmän vaihtelua. Asenteiden keskiarvo oli 4,56, mikä viittaa yleisesti myönteiseen suhtautumiseen tietoturvaan, mutta yksittäisten osa-alueiden välillä oli hajontaa. Tämä kertoo siitä, että vaikka henkilöstö ymmärtää tietoturvan merkityksen, sen näkyminen käytännön työssä voi vaihdella roolista ja työtehtävistä riippuen.

Käyttäytymisen (B) osalta keskiarvo 4,30 oli selvästi matalampi kuin tietoisuuden ja asenteiden kohdalla, mikä on tyypillinen ilmiö tietoturvatutkimuksissa. Tämä osoittaa, että pelkkä tiedollinen osaaminen ei aina suoraan muutu käytännön toiminnaksi, vaan voi tulla tekijöitä, jotka vaikuttavat turvallisiin toimintatapoihin. Tässä tutkimuksessa havaittiin suurta vaihtelua eri tutkittujen osa-alueiden ja vastaajaryhmien välillä.

Näiden tulosten perusteella voidaan todeta, että kohdeorganisaation vahvuutena on henkilöstön laaja-alainen tietoturvaosaaminen ja myönteinen suhtautuminen tietoturvaan, mutta käytännön toimintatapojen yhdenmukaistaminen ja vahvistaminen tulee olemaan keskeinen kehityskohde.

10.2 Tutkimuksen tulokset osa-alueittain

Osa-aluekohtaisia tuloksia tarkasteltaessa voidaan todeta, että erot eri alueiden välillä ovat erittäin pieniä. Seuraavissa alaluvuissa käsitellään tutkimuksen tuloksia eri osa-alueittain.

10.2.1 Knowledge

Vastaajien osaamista mittaava K-arvo vaihteli välillä 4,50–4,81, eli seitsemän mitattavan osa-alueen välillä ero jäi vain 0,31 yksikköön. Tämä osoittaa, että tietoturvaosaaminen on organisaatiossa tasaisen vahvaa, eikä yksikään osa-alue erottunut merkittävästi muita heikompana tai vahvempana. Knowledge-alueen paras osaaminen löytyy Incident Reporting-osiosta, jossa tulos oli peräti 4,81. Tulos kertoo, että henkilökunta tiedostaa erittäin hyvin, miten toimia tietoturvan poikkeamatilanteissa sekä niihin liittyvissä havainnoissa ja käytännöissä organisaation omistaman IT-omaisuuden osalta. Todella hyvin osattiin myös sähköpostin turvallinen käyttö (4,74) sekä ymmärrettiin päivittämättömien päätelaitteiden vaarat ja ymmärrettiin päivitysten merkitys haavoittuvuuksien poistamisessa (4,75).

Vaikka muidenkin osa-alueiden tulokset olivat hyviä, Company Security Practices -osio jäi hieman muita matalammaksi (4,50). Tämä osio mittasi muun muassa organisaation omien tietoturvakäytäntöjen tuntemusta, tiedon löytämistä sekä kommunikaatioketjuja.

10.2.2 Attitude

Sama trendi jatkuu myös A-kategoriassa, jossa tulokset vaihtelivat välillä 4,39–4,71. Erot eri osa-alueiden välillä olivat jälleen hyvin pieniä, mikä osoittaa, että työntekijöiden asenteet turvalliseen toimintaan ovat varsin yhtenäisiä riippumatta mitattavasta osa-alueesta. Parhaat tulokset saatiin Incident Reporting-osiossa sekä Phishing Awareness and Email Use-osiossa. Jälkimmäisessä A-arvo oli

jopa hieman korkeampi kuin saman osa-alueen osaamista mittaava K-arvo, mikä on poikkeuksellista. Muilla osa-alueilla tulokset noudattivat yleistä suuntausta, jossa pisteet laskivat asteittain siirryttäessä K → A → B.

Heikommat pisteet tässäkin osiossa tuli Secure Data Handling osiosta sekä uudelleen Company Security Practices- osiosta, kuten myös K-kategoriassa.

10.2.3 Behaviour

Käyttäytymistä mittavan B-kategorian tulokset olivat poikkeuksetta heikoimmat kaikista kolmesta mitatusta osa-alueen kategoriasta, pisteiden ollessa 4,70–4,42 välissä. Selkeästi parhaiten osattiin tästäkin kategoriassa Incident Reportin osion kysymykset. Myös Secure Data Handling ja Phishing Awareness and Email Use, saivat hyvät pisteet, kun taas Security Updates and System Maintenance-osio jäi selkeästi koko tutkimuksen huonoimmaksi pisteillä 4,02. Huomionarvoista on, että tässä kategoriassa osaaminen (K) ja käyttäytymisen (B) välinen ero oli peräti 0,73 pistettä, eron ollessa muiden osa-alueiden kohdalla huomattavasti pienempi. Tämä kertoo selvästi, että hyvä ymmärrys laitteiden ja ohjelmistojen päivittämisen tärkeydestä ei toteudu kuitenkaan käytännön tekoina. Tästä erosta huolimatta, myös tämä arvosana (4,02) on hyvä, mutta selkeästi kuitenkin heikoin mitatuista.

10.2.4 Korrelaatioanalyysit

Korrelaatioanalyysi osoitti, että tietoturvaosaamisella (K) on kohtalainen tai vahva yhteys tietoturva-asenteisiin (A) lähes kaikilla osa-alueilla. Pearsonin korrelaatiokertoimet vaihtelivat välillä 0,40–0,75, mikä viittaa siihen, että osaamisen lisääntyminen edistää myönteistä suhtautumista tietoturvaan. Vahvin yhteys havaittiin alueilla Security Updates and System Maintenance sekä Company Security Practices (0,75 ja 0,70), kun taas heikoin yhteys oli Incident Reporting and Response Guidelines-alueella (0,42). Joillain mitatuilla osa-alueilla

on siis selkeästi suorempi vaikutussuhde osaamisen ja asenteiden välillä, kuin toisilla.

Sen sijaan tietoturvaosaamisen ja käyttäytymisen (K → B) välinen yhteys oli heikompi, vaihdellen 0,23–0,73 välillä. Useimmilla osa-alueilla korrelaatio jäi alle 0,50, mikä viittaa siihen, että pelkkä tietoturvaosaaminen ei välttämättä johda suoraan turvallisiin toimintatapoihin. Poikkeuksena oli Incident Reporting and Response Guidelines, jossa yhteys oli huomattavasti vahvempi (0,73). Tämä voi tarkoittaa, että tietyissä tilanteissa tietoturvatieto vaikuttaa suoremmin käytännön toimintaan.

Asenteiden ja käyttäytymisen (A → B) välillä havaittiin hyvin vaihtelevaa yhteyttä, joka oli osassa tapauksista heikko. Korrelaatiokertoimet vaihtelivat välillä 0,14–0,62, mikä tukee aiempaa havaintoa siitä, että myönteinen asenne ei yksinään riitä varmistamaan turvallista toimintaa. Käyttäytymistä ohjaa myös muut tekijät, kuten organisaation laatimat ohjeistukset ja työyhteisön normit.

Korrelaatiotulokset tukevat aiempaa tietoturvakäyttäytymistä koskevaa tutkimusta, jossa on havaittu, että tietoturvaosaaminen yksinään ei riitä varmistamaan turvallista käyttäytymistä, vaan siihen vaikuttavat myös organisatoriset tekijät ja sosiaaliset normit [47]. Havaittu heikko yhteys asenteiden ja käyttäytymisen välillä on linjassa aiempien tulosten kanssa, joissa on korostettu, että pelkkä myönteinen suhtautuminen ei aina johda oikeisiin toimintamalleihin ilman jatkuvaa kehittämistä ja hyvää kommunikointia.

Erityisesti Incident Reporting and Response Guidelines -alueen vahva yhteys käyttäytymiseen viittaa siihen, että konkreettiset ja selkeät käytännöt voivat edistää tietoturvakäytännön noudattamista. Tämä on yhteneväistä aiempien tutkimusten kanssa, joissa on havaittu, että käyttäytymiseen vaikuttavat vahvasti organisaation tietoturvakulttuuri, ohjeistusten selkeys ja valvontamekanismit.

11 Kehitysideat

Tulosten analysoinnin pohjalta tunnistettiin konkreettisia kehitysideoita, jotka esitellään seuraavaksi. Koska millään osa-alueella ei havaittu heikkoja tuloksia, ei kehittämistoimenpiteitä tarvitse kohdistaa priorisoidusti yhteen tiettyyn alueeseen toisten kustannuksella.

11.1 Välittömät toimenpiteet

Nopeimmin kehitettäväksi osa-alueeksi nousee kuitenkin Company Security Practices, sillä kaikki siihen liittyvät käytännöt ovat jo olemassa ja dokumentoitu. Kehityksen painopisteenä tulee siis olla näiden käytäntöjen selkeämpi viestintä henkilöstölle, jotta ohjeistukset ja prosessit tunnistetaan ja niitä osataan hyödyntää päivittäisessä työssä. Tämän alueen osaamisen parantaminen onnistuu yksinkertaisesti jo kertaamalla mistä organisaation järjestelmästä tai dokumentinhallinnasta löytyy tietoturvan politiikat ja toimintaohjeet, sekä painottamalla oikeiden viestintäkanavien käyttöä ja tekemällä yhteystietojen löytämisen selkeämmäksi.

Viestintä toteutetaan käyttämällä organisaation olemassa olevia viestintäkanavia sekä käytössä olevaa koulutusalustaa, jolla voidaan toteuttaa räätälöityä koulutuksia sekä saada niistä myös suoritusraportit. Tulevissa organisaation sisäisissä koulutuksissa tullaan tähän kiinnittämään myös aikaisempaa enemmän huomiota.

11.2 Keskipitkän aikavälin toimenpiteet

Seuraava kehitysalue tulee olemaan Security Updates and System Maintenance-alue, jossa oli käyttäytymisen osalta selvästi muista poikkeavan heikko B-arvo. Koska henkilökunnan osaaminen tästäkin alueesta oli erinomaista, kehittämisen painopiste on asenteiden muokkaamisella ja erityisesti käyttäytymistä parantamalla. Tämän parantaminen onnistuu kommunikoimalla aiheesta

säännöllisesti, organisaation sisäisillä koulutuksilla sekä myös pienryhmäkoulutuksilla, joissa on helpompi painottaa asian merkitystä juuri kyseisen osaston työtehtävien osalta. Uuden tietoturvatietoisuuden kehittämiseen hankitun järjestelmän mikrokoulutuksilla tulee olemaan tässä myös merkittävä rooli.

Tutkittavaksi otetaan myös mahdollisuus käyttää automatiikkaa viestittämään henkilökuntaa päätelaitteen tilasta, jos se on haavoittuvainen. Nykyään tieto on reaaliaikaisesti IT- ja OPS-tiimien käytössä, mutta sen jakaminen automaattisesti työntekijälle nopeuttaisi tilatiedon jakamista laitteen haltijalle.

11.3 Pitkän aikavälin suunnitelmat

Muiden viiden mitatun osa-alueen osalta ei ole tarvetta välittömiin korjaaviin tai edes keskipitkän välin korjaaviin toimenpiteisiin. Näiden alueiden osaamista mittaavat tulokset olivat erinomaisia, eikä myöskään asenne tai käyttäytymismittarit edellytä välittömiä toimenpiteitä.

Näiden viiden alueen osalta tietoisuuden parantaminen tulee olemaan osa organisaation jo olemassa olevia koulutuskäytäntöjä. Tutkimus toki auttaa kohdistamaan niitä oikeille ryhmille aikaisempaa paremmin sekä vastaajien osastotietojen perusteella tekemään osastokohtaisia rooliin perustuvia koulutuksia paremmin.

Organisaation olemassa olevat koulutukset tulevat luonnollisesti kuulumaan edelleen myös aiemmin mainittujen Company Security Practices ja Security Updates and System Maintenance-alueiden koulutusohjelmiin.

.

12 Tutkimuksen yhteenveto

Tutkimuksen tavoitteena oli selvittää organisaation henkilöstön osaamista ja käyttäytymistä eri tietoturvatietoisuuden osa-alueilla. Siinä hyödynnettiin tietoturvatietoisuuden laajennettua käsitettä, jossa osaamisen lisäksi mitattiin myös asenteita ja käyttäytymistä. Tulokset tukivat alkuperäistä oletusta siitä, että henkilökunta on hyvin valveutunutta tietoturvaan liittyvistä riskeistä, kyberuhista sekä oikeista toimintatavoista, mutta tutkimuksen perusteella tämä tieto ei kaikissa tapauksissa ole konkretisoitunut käytännön tekemiseen. Yksi tutkimuksen keskeinen havainto olikin, että se vahvisti tämän oletuksen.

Kyselytutkimus antoi arvokasta tietoa organisaation henkilöstön tietoturvatietoisuuden nykytilasta useilla mitatuilla osa-alueilla. Tulosten perusteella voidaan kehittää tiettyjä osa-alueita nopealla aikataululla, ja muiden osalta ne voidaan huomioida pidemmän aikavälin suunnittelussa.

Organisaation käytössä olevat koulutusratkaisut tukevat kehittämistä, ja niitä mukautetaan jatkossa paremmin kohdistetuiksi. Konkreettinen hyöty työstä saadaankin työntekijöiden tarkkojen kehitystarpeiden selvittämisessä. Lisäksi selvitetään teknisiä automaatioratkaisuja, jatkuvan tiedottamisen tueksi.

Käytetty mittaustapa oli onnistunut ja hyvin tutkimuksen kohderyhmälle soveltuva. Sähköisen kyselylomakkeen muokkaaminen kysymysten ja väittämien osalta vaati paljon aikaa, mutta ratkaisu toimi lopulta hyvin. Koska tutkimus perustui henkilöstön vastauksiin, tärkeää oli myös heidän sitoutumisensa tutkimukseen. Hyvä vastausprosentti kertoi, että myös tässä onnistuttiin.

Samaa mittaustapaa hyödynnetään jatkossa säännöllisesti, ja selvitys toteutetaan vähintään kerran vuodessa PDCA-mallin mukaisesti. Tämä mahdollistaa paitsi nykytilan arvioinnin myös tehtyjen parannustoimenpiteiden vaikuttavuuden seurannan. Lisäksi kyselylomakkeen sisältö tarkistetaan vuosittain, jotta se pysyy ajan tasalla ja vastaa kehittyviin tietoturvauhkiin.

Lähteet

[1] Verizon Busines. 2024. Verizon 2024 Data Breach Investigations Report. Viitattu 23.7.2024. https://www.verizon.com/business/resources/reports/dbir/. Vaatii käyttäjätunnuksen.

[2] Traficom. 2024. Traficom Tietoturvan vuosi 2023. Viitattu 24.7.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_Tietoturvan-vuosi-2023_web.pdf.

[3] Norwegian University of Science and Technology. 2023. A systematic literature review of how cybersecurity-related behavior has been assessed. Viitattu 16.3.2025. https://doi.org/10.1108/ICS-08-2022-0139.

[4] Puhakainen, P. 2006. A design theory for information security awareness. Viitattu 15.8.2024. Väitöskirja. Oulu: Oulun Yliopisto. https://urn.fi/URN:ISBN:9514281144.

[5] European Union Agency for Cybersecurity. 2024. ENISA Threat Landscape 2024. Viitattu 25.9.2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[6] SANS. 2024. SANS 2024 Top Attacks and Threats Report. Viitattu 1.8.2024. https://www.sans.org/white-papers/sans-2024-top-attacks-threats-report/. Vaatii käyttäjätunnuksen.

[7] SANS. 2024. SANS 2024 Security Awareness Report. Viitattu 14.2.2025. https://www.sans.org/mlp/ssa-2024-security-awareness-report/. Vaatii käyttäjätunnuksen.

[8] Vestman, T. 2020. Kriittinen analyysi neutralisoimisteorian soveltamisesta tietojärjestelmätieteessä. Viitattu 18.9.2024. Väitöskirja. Jyväskylä: Jyväskylän yliopisto. http://urn.fi/URN:ISBN:978-951-39-8174-7.

[9] Ojasalo, K; Moilanen, T; Ritalahti, J. 2009. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

[10] Parsons, K; McCormac, A; Butavicius, M; Pattinson, M; Jerram, C. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Viitattu 9.9.2024. http://dx.doi.org/10.1016/j.cose.2013.12.003.

[11] Parsons, K; Calic, D; Pattinson, M; Butavicius, M; McCormac, A; Zwaans, T. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Viitattu 16.9.2024. https://doi.org/10.1016/j.cose.2017.01.004

[12] Heikkilä, T. 2014. Tilastollinen tutkimus. 9. uudistettu painios. Porvoo: Edita Publishing Oy.

[13] SurveyMonkey. 2024. Mikä on Likert-asteikko?. Viitattu 27.12.2024. https://fi.surveymonkey.com/mp/likert-scale/.

[14] Hakala, M; Vainio, M; Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. 1. Painos. Porvoo: Docendo Finland Oy.

[15] Nikander, J; Manninen, O; Laajalahti, M. 2020. Requirements for cybersecurity in agricultural communication networks. Viitattu 17.3.2025. https://doi.org/10.1016/j.compag.2020.105776.

[16] F-Secure. 2023. Mitä on kyberturvallisuus?. Viitattu 17.9.2024. https://www.f-secure.com/fi/articles/what-is-cyber-security.

[17] Kruger, H.A; Kearney, W.D. 2006. A prototype for assessing information security awareness. Viitattu 28.9.2024. https://doi.org/10.1016/j.cose.2006.02.008.

[18] National Institute of Standards and Technology. 2024. NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program. Viitattu 2.9.2024. https://doi.org/10.6028/NIST.SP.800-50.

[19] European Union Agency for Cybersecurity. 2019. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Viitattu 22.10.2024. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

[20] ICASA. 2020. Building a Culture of Security. Viitattu 1.10.2024. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security.

[21] SFS-EN ISO/IEC 27001:2023. 2024. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS ry.

[22] Gardner B; Thomas, V. 2014. Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats. Viitattu 19.10.2024. https://www.researchgate.net/publication/291092430_Building_an_Information_Security_Awareness_Program_Defending_Against_Social_Engineering_and_Technical_Threats_1st_Edition

[23] Tietoturva ry. 2021. Ajankohtaiskatsaus – henkilöstön tietoturvatietoisuuden kasvattaminen. Viitattu 19.10.2024. https://www.youtube.com/watch?v=LpIVyCz3JPg.

[24] Gartner. 2024. Forecasts Global Information Security Spending to Grow 15% in 2025. Viitattu 28.2.2025. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025.

[25] Cybersecurity Ventures. 2023. 2023 Security Awaraness Training Report. Viitattu 24.9.2024. https://cybersecurityventures.com/security-awareness-training-market-to-hit-10-billion-annually-by-2027/.

[26] The World Economic Forum. 2025. Global Cybersecurity Outlook 2025. Viitattu 13.1.2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.

[27] Tietoturva ry. 2020. Tietoturvatietoisuuden merkitys kasvaa. Viitattu 25.9.2024. https://www.tietoturva.org/tietoturvatietoisuuden-merkitys-kasvaa/.

[28] Traficom. 2022. The security threat of AI-enabled cyberattacks. Viitattu 25.9.2024. https://www.traficom.fi/en/publications/security-threat-ai-enabled-cyberattacks.

[29] The MITRE Corporation. 2024. MITRE ATT&CK Matrix for Enterprise. Viitattu 7.9.2024. https://attack.mitre.org/matrices/enterprise/.

[30] Mirsky, Y.; Demontis, A.; Kotak, J.; Shankar, R.; Deng, G.; Yang, L.; Zhang, X.; Lee, W.; Elovici, Y.; Biggio, B. 2021. The Threat of Offensive AI to Organizations. Viitattu 17.3.2025. http://dx.doi.org/10.48550/arXiv.2106.15764.

[31] Wiley, A.; McCormac, A.; Calic, D. 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. Viitattu 10.10.2024. https://doi.org/10.1016/j.cose.2019.101640.

[32] McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. 2017. Individual differences and Information Security Awareness. Viitattu 7.10.2024. https://doi.org/10.1016/j.chb.2016.11.065.

[33] Kranz, J.; Haeussinger, F. 2013. Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. Viitattu 7.10.2024. https://www.researchgate.net/publication/258926834_Information_Security_Awareness_Its_Antecedents_and_Mediating_Effects_on_Security_Compliant_Behavior.

[34] Tilastokeskus. 2022. Pilvipalveluita käytti 81 % yrityksistä vuonna 2022. Viitattu 10.9.2024. https://stat.fi/julkaisu/cktvztyy82z790b55dz6j23q3.

[35] SANS. 2024. SANS Cloud Security Exchange 2024. Viitattu 9.12.2024. https://www.youtube.com/watch?v=ZcFZKKL1_qc.

[36] StandardFusion. 2024. ISO 27000 Series of Standards: Everything You Need to Know. Viitattu 1.3.2025. https://www.standardfusion.com/blog/iso-27000-series.

[37] Business Enterprise Mapping. 2023. The Effectiveness of the Plan-Do-Check-Act Cycle. Viitattu 18.3.2025. https://businessmapping.com/bl160-the-effectiveness-of-the-plan-do-check-act-cycle.php.

[38] ENISA. 2006. A Users Guide:How to Raise Information Security Awareness. Viitattu 30.11.2024. https://www.csialliance.org/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf.

[39] Kont, K. 2023. Information Security Awareness of Librarians in the Baltic countries: A Comparative Analysis. Viitattu 1.12.2024. Estonian Academy of Security Sciences, Institute of Internal Affairs. https://doi.org/10.22364/bjmc.2023.11.3.07.

[40] Baruch, Y.; Holtom, B. 2008. Survey Response Rate Levels and Trends in Organizational Research. Viitattu 12.12.2024. http://dx.doi.org/10.1177/0018726708094863.

[41] Tietoarkisto. 2021. Kvantitatiivisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 11.3.2025. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus.

[42] Statictics How To. 2023. What is a correlation coefficient? Viitattu 17.3.2025. https://www.statisticshowto.com/probability-and-statistics/correlation-coefficient-formula/.

[43] KvantiMOTV. 2004. Korrelaatio ja riippuvuusluvut. Viitattu 18.3.2025. https://www.fsd.tuni.fi/menetelmaopetus/korrelaatio/korrelaatio.html.

[44] Crowdstrike. 2024. CrowdStrike 2024 Global Threat Report. Viitattu 2.3.2025. https://go.crowdstrike.com/global-threat-report-2024.html. Vaatii käyttäjätunnuksen.

[45] Microsoft. 2024. Microsoft Digital Defense Report 2024. Viitattu 3.3.2025. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

[46] Google. 2024. Cybersecurity Forecast 2025 Report. Viitattu 3.3.2025. https://cloud.google.com/security/resources/cybersecurity-forecast.

[47] Siponen, M.; Mahmood, M.; Pahnila, S. 2013. Employees' adherence to information security policies: An exploratory field study. Viitattu 10.3.2025. http://dx.doi.org/10.1016/j.im.2013.08.006.

[48] Euroopan Unioni. 2025. Yleinen tietosuoja-asetus. Viitattu 22.3.2025. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm.

[49] IBM. 2024. IBM X-Force Threat Intelligence Index 2024. Viitattu 3.3.2025. https://www.ibm.com/reports/threat-intelligence. Vaatii käyttäjätunnuksen.

[50] Gray, J. 2022. Practical Social Engineering: A Primer for the Ethical Hacker. 1. Painos. San Francisco: No Starch Press. ISBN:978-1-7185-0093-3.

Organisaation HAIS-Q kyselylomake

Taulukko 2. HAIS-Q Osa-alueet ja kysymykset.

	Knowledge	Attitude	Behaviour
Focus area: Password Management			
Password Reuse	Using the same password for multiple accounts increases security risks.	It's acceptable to use the same password for work and personal accounts if it's convenient. *	I use a different password for my personal and work accounts.
Sharing Passwords	I am allowed to share my work passwords with colleagues. *	Sharing personal work passwords is risky, even with colleagues.	I never share my work passwords with anyone.
Password Storage	I understand how a password manager helps secure passwords.	I believe a password manager is the safest place to store my work passwords.	I sometimes store my passwords in less secure places, like in a document, browser, or on paper. *
Focus area: Phishing Awareness and Email Use			
Recognizing Phishing Emails	I understand the key signs of phishing emails, such as poor grammar, unusual links, or urgent requests.	It's unnecessary to examine the content of emails if they appear legitimate. *	I always review the content and structure of emails to identify potential phishing attempts.
Clicking Links from Unknown Senders	I understand that links from unknown senders should not be clicked.	Nothing bad can happen if I click on a link in an email from an unknown sender. *	I sometimes click on links in emails from unknown senders if they look interesting. *
Opening Attachments	It is acceptable to open email attachments without verifying the sender's identity. *	It's risky to open an email attachment without confirming the sender's authenticity.	I only open email attachments after verifying the sender's identity and the attachment's relevance.
Focus area: Internet Use and Online Behaviour			
Downloading files	It is OK to download any files onto my work computer if they are helpful for my job. *	It can be risky to download files onto my work computer.	I download any files onto my work computer that will help me get the job done. *
Accessing Websites from Work Computer	I understand that certain websites are restricted or unsafe to access at work.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. *
Entering Information Online	Due to scam sites, entering business-related data on a website can be dangerous.	If it helps me to do my job, it doesn't matter what information I put on a website. *	I assess the safety of websites before entering information.
Focus area: Security Updates and System Maintenance			
Security Updates	I understand the importance of regularly updating my device's security software.	I believe that delaying security updates does not pose significant risks. *	I promptly install security updates when my device or the IT department recommends them.
Security Update Skills	I know how to check for and install security updates on my device.	I feel confident in my ability to perform security updates on my device without assistance.	I regularly check for and install security updates on my device independently.
Importance of Timely Updates	I understand that outdated software can expose my organization to cybersecurity risks.	I feel that updating software regularly is an unnecessary disruption to my workflow. *	I only install security updates when reminded or instructed by my device or company IT.
Focus area: Secure Data Handling			
Removable Media	I am aware that attempting to use USB ports could pose security risks, even if they are blocked	Testing or bypassing USB port restrictions compromises device security.	I never attempt to test or bypass USB port restrictions on my device
Information Sharing	I know that sharing sensitive information digitally requires secure methods	Sharing sensitive information digitally without security measures is not risky. *	I always use encrypted channels or secure methods when sharing confidential information
Handling Classified Information	I know the different ways to handle information based on its classification level.	Classified information handling guidelines are unnecessary in some cases. *	I follow the company guidelines for handling information based on its classification level
Focus area: Incident Reporting and Response Guidelines			
Reporting Missing Company Property	I understand the importance of promptly reporting lost or stolen company assets, like laptop, phone, key, etc.	I feel reporting lost or stolen company assets can wait until the next workday. *	If I lost or had company assets stolen, I would immediately report it to the appropriate channel.
Ignoring Poor Security Behaviour	I know the risks of ignoring poor security practices in my workplace.	I feel that addressing security breaches in my workplace is not my responsibility. *	If I noticed poor security behaviour, I would report it to the appropriate channel.
Incident Reporting	It's optional to report security incidents. *	Reporting security incidents is unnecessary if the issue seems minor. *	If I notice a security incident, I would report it immediately.
Focus area: Company Security Practices			
Awareness and Usage of Security Policies	I know where to find the organization's security policies and guidelines.	Reading and following the organization's security policies is unnecessary for my role. *	I refer to the organization's security policies whenever I need guidance in my work.
Security Incident Contacts	I know who to contact in my organization if I suspect a data breach or security incident.	Using the correct reporting process for security incidents ensures the issue is handled efficiently	I know how to access the organization's guidelines, like policies, for reporting a security incident or breach.
Safeguarding Company Assets	Leaving company-owned devices unattended, even for a short time, is unacceptable.	It's acceptable to leave company-owned devices unattended in a car or other unsecured location for a short time. *	I never leave company-owned devices unattended in unsecured locations, such as a car or public area.
Software Installation Practices	I know the organization's policy for installing new software on company devices.	It's acceptable to bypass the software installation guidelines if the software is urgently needed to make my work easier. *	I install software only by following the organization's approved process.
Locking Computer	Locking my computer when I step away is unnecessary because the system locks itself automatically. *	I feel that locking my computer every time I step away is unnecessary. *	I always lock my computer when leaving my desk, even for a short time

Kysymyksiin vastataan viisiportaisella asteikolla jossa ääripäät ovat "Täysin samaa mieltä" ja "Täysin eri mieltä".
Negatiivisesti asetellut kysymykset on merkattu lomakkeeseen * - merkillä.