Opinnäytetyö (YAMK)

Kyberturvallisuus

2025

Tuukka Vainio

Tietoturvaosaamisen ja tietoturvatietoisuuden kehittäminen korkeakoulussa

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (YAMK) | Tiivistelmä

Turun ammattikorkeakoulu

Kyberturvallisuus

2025 | 81 sivua

Tuukka Vainio

Tietoturvaosaamisen ja tietoturvatietoisuuden kehittäminen korkeakoulussa

Yliopistoissa halutaan kohonneen kyberuhkatason takia vähentää ihmisistä aiheutuvia tietoturvariskejä. Yhtenä ratkaisuna on ehdotettu yhteisen tietoturvatestin käyttöä yliopistoyhteisön tietoturvaosaamisen testaamiseen ja tietoturvatietoisuuden herättelyyn. Tämän opinnäytetyön tavoitteena oli selvittää, minkälaisia vaatimuksia yliopistojen tietoturvakoulutukselle on, millä tavoin ihmisiin liittyviä tietoturvariskejä saadaan vähennettyä, ja sopiiko tietoturvatestin käyttö tavoitteeseen.

Kirjallisuuskartoituksella selvitettiin minkälaisia vaatimuksia Suomen laeissa, EU-asetuksissa ja tietoturvan viitemalleissa asetetaan yliopistolaisten tietoturvakouluttamiselle. Käsiteanalyysillä selvitettiin mitä tietoturvatietoisuus ja tietoturvakulttuuri tarkoittavat, ja miten niitä voi kehittää yliopistoissa.

Tietoturvakoulutukselle asetetaan vaatimuksia henkilöstön kouluttamiselle tiedonhallintalaissa ja tietosuoja-asetuksessa. Ne eivät kuitenkaan puutu toteuttamistapaan. Tutkimustiedon mukaan tietoturvatietoisuudella kannattaa edistää käyttäytymisen muutosta ja kehittää positiivista tietoturvakulttuuria. Tietoturvan kypsyysmallien mukaan ehdotettu tietoturvatestaaminen ei vähennä tietoturvariskejä ja antaa väärän kuvan riskien hallinnasta.

Asiasanat:

Tietoturva, kyberturvallisuus, tietoturvakoulutus, tietoturvatietoisuus, tietoturvakulttuuri

Master’s Thesis | Abstract

Turku University of Applied Sciences

Cybersecurity

2025 | 81 pages

Tuukka Vainio

Developing cybersecurity skills and cybersecurity awareness in higher education

Due to the elevated cyber threat level, universities want to reduce their human-related cybersecurity risks. One proposed solution is the use of a common cybersecurity test to assess people’s security skills and increase their awareness of cyber threats. The purpose of this thesis was to find out what kind of cybersecurity training requirements there are for universities, how human-related cybersecurity risks can be reduced, and does the proposed test suit the purpose.

A literature survey was used to find out what kind of cybersecurity training requirements Finnish laws, EU regulation and information security frameworks set for universities. Concept analysis was used to establish what cybersecurity awareness and cybersecurity culture mean, and how they can be developed at universities.

Requirements for cybersecurity training are set for personnel in the Act on Information Management in Public Administration and the General Data Protection Regulation. They don’t go into details of their implementation. Based on research, cybersecurity awareness should be used to drive change in behavior and develop positive cybersecurity culture. According to cybersecurity awareness maturity models, the proposed test does not reduce human-related cyber risks and can give a false impression of their management.

Keywords:

Information security, cybersecurity, security awareness, security culture

Sisältö

Liitteet

Kuviot

Taulukot

Käytetyt lyhenteet tai sanasto

5Es	Educate why, Enable how, shape the Environment, Encourage the action, Evaluate the impact. (NPSA 2023)
AAPA	Ammattikorkeakoulujen tietohallintojohtajien verkosto
AMKSEC	Ammattikorkeakoulujen tietoturvaverkosto
CAF	Cyber Assessment Framework (NCSC 2024)
CERT NZ	Computer Emergency Response Team New Zealand
CIS	Center for Internet Security (CIS 2024)
CMI	Cultural Maturity Indicator (Carpenter & Roer 2022, 162)
COM-B	Capability, Opportunity, Motivation, Behavior. Käyttäytymisen muutoksen interventioiden yhteenvetomalli. (Michie ym. 2011)
CSF	Cybersecurity Framework (NIST CSF 2.0)
CSIRT	Computer Security Incident Response Team, tai Cyber Security Incident Response Team (Stikvoort ym. 2023)
eduGAIN	Superfederaatio kansallisille kirjautumisluottamusverkostoille (eduGAIN 2024)
ENISA	Euroopan unionin kyberturvallisuusvirasto
FIRST	Forum of Incident Response Teams
FUCIO	Suomalaisten yliopistojen IT-johtajien verkosto
GDPR	General Data Protection Regulation, Euroopan unionin Yleinen tietosuoja-asetus (Direktiivi 2016/679)
HAIS-Q	Human Aspects of Information Security Questionnaire (Parsons ym. 2019)

Haka	Kansallinen kirjautumisen luottamusverkosto (CSC 2024)
IEC	International Electrotechnical Commission (ISO/IEC 27001:2023)
IGP	Indicator of Good Practice (NCSC 2024a)
ISMS	Information Security Management System, tietoturvallisuuden hallintajärjestelmä (ISO/IEC 27001:2023)
ISO	International Organization for Standardization (ISO/IEC 27001:2023)
KAB	Knowledge–Attitude–Behaviour-malli (Kruger & Kearney 2006)
Kyberturvallisuus	Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. (Huoltovarmuuskeskus 2018)
Kyberuhka	Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon. (Huoltovarmuuskeskus 2018)
MFA	Multi-factor authentication, monivaiheinen kirjautuminen
NCSC	National Cyber Security Centre, Britannian kansallinen kyberturvallisuusviranomainen (NCSC 2024)
NIS	Network and Information Systems (Euroopan parlamentin ja neuvoston direktiivi 2022/2555)
NIST	National Institute of Standards and Technology, Yhdysvaltain kansallinen standardisointi- ja teknologiainstituutti (NIST 2020)
NPSA	National Protective Security Agency, Britannian kansallinen suojaavan turvallisuuden viranomainen (NPSA 2023)

NREN	National Research and Education Network, kansallinen tutkimus- ja opetusverkko
SIM3	Security Incident Management Maturity Model (Stikvoort ym. 2023)
SIRTFI	A Security Incident Response Trust Framework for Federated Identity (REFEDS 2022)
Tietoturva	Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Olot, joissa tietoturvariskit ovat hallinnassa. (Huoltovarmuuskeskus 2018)
UNIFI	Suomalaisten yliopistojen rehtorineuvosto UNIFI ry

1 Johdanto

Kohonneen kyberuhkatason takia yliopistoyhteisön tietoturvaosaamiseen on kiinnitetty aiempaa enemmän huomiota ja pakollisia tietoturvatestejä on toivottu yliopistoihin käyttöön tietoturvariskien vähentämiseksi. Yliopistoihin kohdistuu myös velvoitteita tietoturva-asioiden kouluttamiseen henkilöstölle. Ratkaisuksi on ehdotettu yliopistojen tietoturvayhteistyönä kehitettyä yleistä tietoturvakoulutusmateriaalia ja siihen liittyvää testiä, jonka suorittamista on esitetty pakolliseksi kaikille käyttäjätunnuksen haltijoille (Gynther 2023). Tässä opinnäytetyössä tutkitaan ihmiskeskeisen tietoturvan näkökulmasta, miten tietoturvaosaamista ja tietoturvatietoisuutta kannattaa kehittää yliopistoissa, jotta tietoturvariskit pienenisivät.

Hielscher ym. (2023, 2311) havaitsivat tutkimuksissaan, että tietoturvapäälliköt käsittävät ihmiskeskeisen tietoturvan ensisijaisesti markkinoilla olevien tietoisuusratkaisujen ja kalastelusimulaatioiden kautta, eivätkä ajattele asiaa ihmisten käyttäytymisen ja tietoturvan aiheuttaman hankaluuden kautta. Beyerin ym. (2015, 3) mukaan tietoturvakoulutuksella ja -viestinnällä on tarkoitus ohjata ihmisten käyttäytymistä organisaation tavoitteisiin, mutta geneerisillä verkkokursseilla ja tietoturvatesteillä ihmisten käyttäytyminen ei kuitenkaan muutu tietoturvallisemmaksi. Vestmanin (2020, 142) mukaan hyvää tarkoittavat ohjeet ja määräykset voivat pahentaa ongelmaa, jota niillä halutaan torjua, jos ne ovat vaikeaselkoisia, päivittämättömiä ja vaikeita noudattaa käytännössä. Myös Vilander (2021, 40) toteaa tietoisuutta kehittävien pyrkimysten olevan haitallisia, jos ne kuormittavat liikaa tai koetaan harmittaviksi. Yliopiston kaltaisissa moniammatillisissa organisaatioissa työtehtävillä, asemalla ja koulutuksella on vaikutus myös asenteeseen tietoturvaa kohtaan (Vestman, 2020, 149). Vilanderin (2021) tutkimustuloksissa asenne oli tietoa merkittävämpi tekijä käyttäytymisen kannalta ja Vilander suosittelee tietoturvakoulutuksessa ennemmin asenteiden kehittämistä kuin tiedon kerryttämistä. Vestman (2020, 143) toteaa, että tietoturva-asioita ei sisäistetä pelkästään verkkokoulutuksella tai lukemalla sääntöjä ja ohjeita.

Tässä opinnäytetyössä kartoitetaan yliopistoja koskevia tietoturvavaatimuksia sekä perehdytään tutkimuksiin ihmiskeskeisestä tietoturvasta, joka juontaa psykologian ja sosiologian eri alojen ihmisten käyttäytymistä koskevan tutkimustiedon soveltamisesta tietotekniikan käyttämiseen. Tavoitteena on löytää lähestymistapoja ihmisten huomioimiseen tietoturvaa kehitettäessä, jotta yliopistojen tietoturvariskit vähenisivät ihmisten tietoturvallisemman käyttäytymisen myötä.

Työssä selvitetään miten tietoturvakoulutusta kannattaa tutkimustiedon mukaan antaa, sekä miten ihmisten tietoturvaosaamista ja tietoturvatietoisuutta kannattaa mitata, kun tavoitteena on vähentää yliopistojen tietoturvariskejä. Työssä kartoitetaan myös mitä yliopistoilta edellytetään tietoturvakouluttamisen ja -testaamisen suhteen, jotta koulutukset vastaisivat lakien ja muihin ulkoisiin vaatimuksiin.

Opinnäytetyön toisessa luvussa kerrotaan yliopistojen saamasta tietoturvatestaamisen toimeksiannosta. Kolmannessa luvussa selvitetään mitä yliopistojen tietoturvallisuuden kouluttamisessa pitäisi huomioida, jotta yliopiston toiminta täyttäisi lakien, asetusten, viitekehysten ja sopimusten vaatimuksia. Neljännessä luvussa perehdytään tietoturvatietoisuuteen ja tietoturvakulttuuriin, sekä näiden mittaamiseen. Viidennessä luvussa analysoidaan yliopistojen tietoturvan kehittämisessä huomioitavia ominaispiirteitä sekä ehdotettujen käytäntöjen haasteita. Kuudennessa luvussa annan eväitä ihmiskeskeisen tietoturvaohjelman toteutukseen

Opinnäytetyö selvittää miten yliopistoissa kannattaa lähestyä tietoturvallisuutta ihmiskeskeisesti täyttäen tietoturvalle asetetut vaatimukset ja tietoturvariskejä vähentäen.

2 Kyberuhat ja tietoturvariskit korkeakouluissa

Korkeakoulut ovat olleet merkittäviä toimijoita Internetissä sen alkuajoista alkaen ja tietomurtoja on aina tehty yliopistoihin joko lopullisena kohteena tai välihyppynä varsinaiseen kohteeseen (Stoll 1990). Suomalaisiin yliopistoihin tehtiin 1990-luvulla tietomurtoja niin sanottuihin keskuskoneisiin, joihin tehdyillä hyökkäyksillä oli laaja vaikutus IT-ympäristön toimintaan kaikkien käyttäjätunnusten salasanojen vaihtamisten ja palvelinten uudelleenasennuksen takia, vaikka yliopistojen toiminta ei vielä ollut tietokoneista riippuvaista (Aarnio 2001). 2000-luvulla IT-arkkitehtuurit muuttuivat hajautetumpaan suuntaan, jonka myötä tietomurtojen vaikutusalue pieneni yhtä palvelua tarjoaviin palvelimiin. Itä-Suomen yliopiston ja muutamaan muun koulutusalan organisaation web-palveluihin 2011 tehdyssä tietomurrossa vuodettiin Internetiin paljon henkilötietoja (Yle 2011), joilla on ollut merkittävä vaikutus sen uhreille (Hämäläinen & Tuominen, 2017). Käyttäjätunnusten urkinta sähköpostitse kasvoi merkittäväksi tietomurtojen aloitustavaksi 2020-luvun taitteessa ja toistatuhatta ihmistä lankesi antamaan salasanansa rikollisille yksittäisissä kalasteluhyökkäyksissä pelkästään Helsingin yliopistolta (Hakkarainen 2018) ja Oulun yliopistolta (Kärkkäinen 2021).

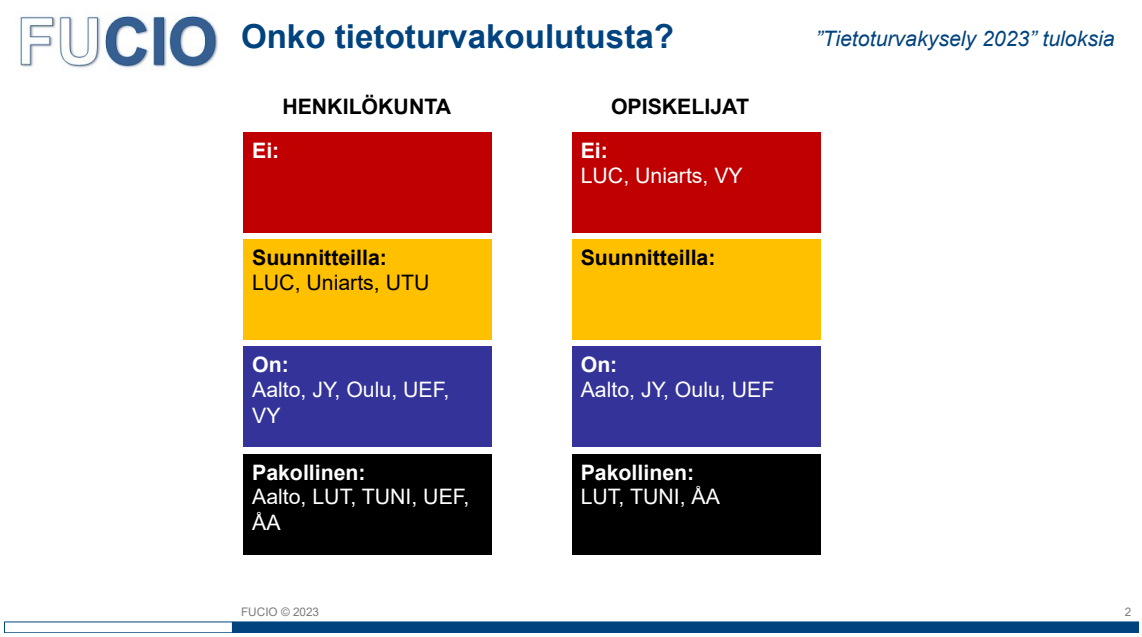
Kyberhyökkäysten uhka ja vaikutukset kasvoivat merkittävästi 2018, kun rikolliset siirtyivät tyypillisesti yksittäisten tietokoneiden käyttöä haittaavista autonomisista haittaohjelmista ja tietomurroista kiristyshyökkäyksiin ja niin sanottuun big game hunting -toimintamalliin, jossa rikollisryhmittymät ottavat panttivangeiksi kokonaisten organisaatioiden kaikki IT-järjestelmät ja tietokoneet (Baker 2022). Kiristyshyökkäys alkaa tietomurrolla, josta rikolliset etenevät IT-infrastruktuurin ohjauspalvelimille pääkäyttäjäksi, jonka laajoja käyttöoikeuksia hyödyntäen rikolliset kopioivat organisaation datan itselleen ja estävät tietokoneiden käytön tiedostoja salaavilla haittaohjelmilla. Aktiivisen hyökkäysvaiheen jälkeen uhrilta kiristetään sen liikevaihtoon pohjautuvia isoja lunnaita varastettujen tietojen vuotamisen uhalla ja salausten purkamiseksi. Nykypäivänä organisaatioiden toiminta lamaantuu, jos ne eivät voi käyttää IT-järjestelmiään ja niiden sisältämää tietoa. Moni organisaatio onkin maksanut lunnaat rikollisille, jos hyökkäyk-

sestä ei kyetty palautumaan varmuuskopioiden ja uudelleenasennusten avulla, tai palautumisessa olisi mennyt liian kauan – kiristyshyökkäyksestä toipuminen kestää keskimäärin useamman viikon (Petrosyan 2024). Hyökkäysmalli on osoittautunut erittäin kannattavaksi (Snyder 2022), jonka myötä hyökkäyksiä tehdään mihin tahansa organisaatioon.

Kiristyshyökkäyksiä tehdään laajasti korkeakoulusektorille ympäri maailmaa (Kondruss 2024). Korkeakouluilla on keskivertoa korkeampi riski joutua kiristyshyökkäyksen kohteeksi, koska niillä on tyypillisesti paljon Internetiin näkyviä julkisesti käytettäviä tietojärjestelmiä, ja korkeakouluyhteisöt koostuvat tuhansista ihmisistä. Suurin osa korkeakouluihin kohdistuneista kiristyshyökkäyksistä tehdään haavoittuvien järjestelmien ja haitallisten sähköpostien kautta, sekä vääriin käsiin päätyneillä käyttäjätunnuksilla (Sophos 2024). Tietojärjestelmien ylläpidon ja kehittämisen hajautuneisuus ja resursointi hankaloittaa niiden suojaamista. Laajassa korkeakouluyhteisössä riski haitallisiin sähköposteihin lankeamiselle ja käyttäjätunnusten vuotamiselle on korkea. Vuonna 2022 Suomen koulutussektorilla nähtiin onnistuneet kiristyshyökkäykset Savonia-ammattikorkeakouluun (Savonia 2022) ja Keski-Uudenmaan koulutuskuntayhtymä Keudaan (Keuda 2023). Kohonneen kyberuhkatason takia tietoturva tunnistettiin yliopistoissa vuoden 2023 tärkeimmäksi asiaksi (FUCIO 2024, 8).

2.1 Toimeksianto tietoturvatestien käytölle ja tietoturvakoulutukselle

Tammikuussa 2023 suomalaisten yliopistojen IT-johtajien FUCIO-verkostossa esiteltiin tuloksia yliopistoille tehdystä kyselystä tietoturvakoulutusten ja tietoturvatestien käytöstä. Tulosten mukaan suurin osa vastanneista yliopistoista tarjosi tietoturvakoulutusta niin henkilökunnalle kuin opiskelijoille ja tietoturvakoulutus oli pakollinen puolelle näistä (Kuvio 1). Tietoturvatesti oli käytössä melkein kaikissa tietoturvakoulutusta käyttäneissä yliopistoissa (Kuvio 2). (Seesto, T., sähköposti 30.1.2023)



Kuvio 1: Tietoturvakyselyyn vastanneiden yliopistojen henkilöstön ja opiskelijoiden tietoturvakoulutuksen tilanne. (Seesto, T., sähköposti 30.1.2023)

Kuvio 2: Tietoturvakoulutuskyselyyn vastanneiden yliopistojen tietoturvatestin tilanne. (Seesto, T., sähköposti 30.1.2023)

Suomalaisten yliopistojen rehtorineuvosto UNIFI pyysi FUCIO:ta valmistelemaan ehdotuksen yliopistojen tietoturvatestauskäytäntöjen harmonisoinnista, jolla saataisiin yliopistoille yhteiset toimintamallit ja menetelmät tietoturvatestien käyttöön. UNIFI:n pyynnössä testauksen toivottiin olevan henkilökunnalle pakollista, mahdollisimman kevyttä ja riittävän usein suoritettavaa. Testien suorittamista pitäisi seurata ja sopia mikä on käytäntö, jos testiä ei suoriteta. UNIFI:n pyynnössä tietoturvakoulutusta voisi tarvittaessa tarjota. (Risikko, T., sähköposti 15.2.2023)

UNIFI-pyyntöä toteuttavan yliopistojen tietoturvapäällikköjen sec-työvaliokunnan yhteistyönä oli julkaistu tietoturva-asioiden perusteita kouluttavat tietoturvaoppaat henkilöstölle ja opiskelijoille 2009 ja 2013 (Manninen ym. 2013a, Manninen ym. 2013b). Näiden pohjalta kehitettiin vuonna 2017 Moodle-oppimisalustassa käytettävä tietoturvakurssi, johon kuuluu myös testi. Koska kurssimateriaalia testikysymyksineen oli jo olemassa, sec-työvaliokunnan huomio kohdentui ensisijaisesti suoritusten seurantaan, yliopistojen välisen hyväksiluvun ehtoihin ja tekniseen toteutukseen, sekä sisällön yhtenäisyyteen ja tavoitetasoon.

Yliopistojen ja ammattikorkeakoulujen tietoturvakoulutusten tilannetta käytiin läpi korkeakoulujen IT-päivillä marraskuussa 2023. Myös ammattikorkeakoulujen tietohallintojohtajien AAPA-verkosto oli antanut AMKSEC-verkostolle vastaavan toimeksiannon, jossa tavoitteena oli ainakin osittain yhteisen materiaalin käyttäminen ja kustannussäästöt, sekä ristiinopiskelun tukeminen. (Gynther 2023)

Yliopistojen puolella sec-työvaliokunta oli linjannut, että yliopistot voivat toteuttaa koulutuksen itselle parhaiten sopivalla tavalla, mutta tietoturvatesti olisi pakollinen. Opiskelijoille suositeltiin tietoturvan sisällyttämistä osaksi pakollisia opintoja. Koska toisaalla suoritetun testin hyväksiluku oli todettu hankalaksi toteuttaa, ja tietoturvatestin suorittamisen on toivottu vievän aikaa vain 5–10 min, useassa korkeakoulussa opiskeleville ja työskenteleville ehdotettiin paikallisen testin suorittamista testin hyväksiluvun sijaan. Mahdollisuus hyväksiluvulle jätettiin kuitenkin avoimeksi. Sec-työvaliokunnan ehdotuksessa vähimmäisvaatimukset, aihealueet ja testikysymykset käytäisiin läpi kahden vuoden välein ajantasaisuuden varmistamiseksi. (Gynther 2023)

2.2 Tutkimuksen metodologia

Tieteellisinä instituutioina yliopistojen voi odottaa hyödyntävän tutkittua tietoa omassa toiminnassaan. Helsingin yliopiston kanslerin mukaan yliopistojen pitäisi arvioida ihmisten kyvykkyysarviointien käyttöä, luotettavuutta ja tarkoituksenmukaisuutta tieteenalojen asiantuntijoita konsultoiden, eikä kopioida käytäntöjä vain siksi, että jokin toinenkin yliopisto käyttää niitä (Salomaa 2024). Myös yliopistoissa käyttöön otettavat tietoturvatestit ja tietoturvakoulutukset ansaitsevat saman arvioinnin.

Kirjallisuuskatsauksella kartoitetaan yliopistoille asetettuja tietoturvavaatimuksia, viitemallien parhaita käytäntöjä tietoturvakoulutusten käyttöön, sekä perehdytään tutkimuksiin ihmiskeskeisestä tietoturvasta.

Yliopistoyhteisöt ovat monimuotoisia, eivätkä tietoturvariskit koske kaikkia samalla tavalla. Työssä selvitetään, keiden kouluttamisella vastataan koulutusvaatimuksiin, ja miten eri ryhmiä kannattaa huomioida tietoturvaosaamisen kehittämisessä.

Tietoturvatietoisuudesta ja tietoturvakulttuurista puhutaan kasvavassa määrin. Käsiteanalyysillä selvitetään mitä tietoturvatietoisuudella ja tietoturvakulttuurilla tarkoitetaan, ja mitä niiden kehittyminen edellyttää yliopistoissa.

Tietoturvakoulutuksista halutaan pakollisia, ja hyväksiluettavia yliopistojen välillä. Vaatimuksista selvitetään keille ja missä määrin tietoturvakoulutusten pitää olla pakollisia. Samalla tutkitaan, onko pakollisuudella negatiivisia vaikutuksia, ja mitä vaihtoehtoja pakollisille koulutuksille on tietoturvallisuutta heikentämättä.

Tuloksena ehdotetaan ihmisiä huomioivaa ja osallistavaa mallia tietoturvan kehittämiseen yliopistoissa, niin että tietoturvariskit laskevat kokonaisuutena niin ihmisten kuin prosessien ja teknologian osalta.

3 Vaatimuksia tietoturvaosaamiselle ja -tietoisuudelle

Yliopistojen tietoturvaa ei juurikaan säädellä, mutta niitä velvoittavat Suomen lait, EU-sääntely, sekä viranomaisten määräykset. Yliopistojen pitää myös noudattaa solmimiaan sopimuksia, joissa sivutaan usein tietoturvaa. Lakien ja sopimusten vaatimukset määrittävät organisaatioiden tietoturvatoiminnalta odotettua vähimmäistasoa.

Viitekehykset määrittelevät yleisesti noudatettavia parhaita käytäntöjä. Vapaaehtoisesti noudatettavien viitekehysten vaatimuksien täyttämisellä tavoitellaan näiden parhaiden käytäntöjen tuomia hyötyjä. Osa viitemalleista on ohjaavia, jotka eivät tarkkaan kerro mitä pitäisi tehdä, ja näitä täydentävät tarkoista toimintaohjeista koostuvat mallit. Oman toiminnan tasoa ja laatua voidaan arvioida kypsyysmalleja käyttämällä, jotka opastavat toiminnan jatkokehittämisessä.

Vaatimukset edellyttävät asioiden tekemistä, ja viitekehysten mukainen toiminta osoitetaan tyypillisesti prosessien dokumentaatiolla ja haastatteluilla. Organisaatiot voivat todistaa viitekehysten mukaisesta toimintansa viitekehyskohtaisella sertifioinnilla, jonka myöntää ulkopuolinen tarkastaja auditoinnin jälkeen. Yliopistojen on moniammatillisina organisaatioina vaikea toteuttaa viitekehyksiä koko organisaation toimintaa kattavina, mutta useimpiin tarpeisiin riittää, että vastaavat toimintatavat voidaan osoittaa ilman sertifiointia.

Korkeakoulujen on hyödyllistä osoittaa toimivansa yleisesti käytössä olevien viitekehysten parhaiden käytäntöjen mukaisesti, koska se parantaa korkeakoulujen yhteistyömahdollisuuksia ulkoisten organisaatioiden kanssa, jotka haluavat yhteistyöhön luotettavia kumppaneita käytettävien tutkimusaineistojen ja kehitettävien innovaatioiden suojaamiseksi. Verkostoituneiden ja toimintaa ulkoistaneiden organisaatioiden kannattaa huolehtia luotettujen kumppaneidensa tietoturvasta myös toimitusketjuhyökkäysten varalta, jossa hyökkääjä voi päästä hyvin suojattuun organisaatioon heikommin suojatun kumppanin kautta.

Vaatimukset jakautuvat pääasiassa organisatorisiin vaatimuksiin, jotka kuvaavat itse organisaation järjestäytymistä, toimintaa ja prosesseja, sekä tietojärjestel-

miä koskeviin teknisiin vaatimuksiin. Tietoturvaosaamisen ja tietoturvatietoisuuden vaatimukset kuuluvat organisatorisiin vaatimuksiin.

Tässä luvussa käydään läpi Suomen lakeja ja EU-asetuksia, jotka asettavat velvoittavia vaatimuksia korkeakoulujen toiminnan tietoturvallisuudelle ja tietosuojalle. Koska tietoturvassakaan ei ole vain yhtä oikeaa totuutta, esiin tuodaan useampi eri kyberturvallisuuden viitemalli niiden erilaisten lähestymistapojen takia. Yleisistä kyberturvallisuuden viitemalleista käydään läpi kansainvälisen ISO/IEC:n tietoturvan hallintajärjestelmän (ISMS) sekä Yhdysvaltain NIST:n Cyber Security Framework -riskienhallintajärjestelmän kuvaamia linjauksia tietoturvatoiminnalle. Yksityiskohtaisempia toimintaohjeita tulee NIST:n SP 800-53 -standardista, Center for Internet Securityn (CIS) Critical Security Controls -viitemallista, sekä kansallisista Katakri-, Julkri, ja Pitukri-kriteeristöistä. Kyberturvallisuuden kypsyysmalleista käydään läpi Suomen Kyberturvallisuuskeskuksen Kybermittari, joka pohjautuu Yhdysvaltain Cybersecurity Capability Maturity Modeliin (C2M2), Britannian Cyber Assessment Framework, sekä Open CSIRT Foundationin ylläpitämä Security Incident Management Maturity Model (SIM3). Esiin tuodaan myös korkeakoulujen kumppanuussopimuksiin liittyviä tietoturvavaatimuksia.

3.1 Suomen lait, EU-asetukset ja viranomaismääräykset

Yliopistojen tietoturvasäännöstö pohjautuu yliopistolaista, jonka 5:41a.2 mukaan yliopisto voi hyväksyä järjestyssäännöt ja antaa muita järjestysmääräyksiä, joilla edistetään myös yliopistoyhteisön turvallisuutta. Lisäksi 5:41a.3 mukaan määräyksiä voidaan antaa yliopiston omaisuuden käsittelystä. (Yliopistolaki 24.7.2009/558)

Lain julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki) 2:4.2 kohta 3 edellyttää tiedonhallintayksikön johdon huolehtivan koulutuksesta, jolla varmistetaan, että henkilöstöllä ja muilla sen lukuun toimivilla on ”riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön oh-

jeista.” Tiedonhallintalaki edellyttää myös riskien selvittämistä ja suojaustoimien soveltamista riskiperusteisesti (4:13.1), sekä käyttöoikeuksien määrittelyä roolipohjaisesti tehtävien tarpeiden mukaan (4:16). (Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906)

Laki digitaalisten palvelujen tarjoamisesta (digipalvelulaki) edellyttää, että tietoturva ja tietosuoja varmistetaan digitaalisten palvelujen suunnittelussa ja ylläpidossa. (Laki digitaalisten palvelujen tarjoamisesta 15.3.2019/306, 2:4.1)

Euroopan unionin kyberturvallisuusdirektiivi (NIS2-direktiivi) tuli voimaan 2024, ja se korvasi aiemman NIS-direktiivin (Euroopan parlamentin ja neuvoston direktiivi 2022/2555). Suomessa kyberturvallisuuslaki on NIS2-direktiivin täytäntöönpaneva lainsäädäntö. Sääntely on ulotettu koskemaan julkishallintoa lisäämällä tiedonhallintalakiin uusi kappale 4a, jossa määritellään soveltamisalaan kuuluvat toimijat. Yliopistot ja ammattikorkeakoulut eivät kuulu niihin tutkimustoiminnan organisaatioihin, joihin sovelletaan kyberturvallisuuslakia (Lantto 2024).

Kyberturvallisuusdirektiivin luku 4 kyberturvallisuusriskien hallintatoimenpiteistä ja raportointivelvoitteista sisältää olennaiset velvoitteet sovellettavien alojen toimijoille. Kyberturvallisuusdirektiivin 4:21 linjaa, että toimijoiden on toteutettava asianmukaisia ja oikein mitoitettuja teknisiä, operatiivisia ja organisatorisia toimenpiteitä kyberturvallisuusriskien hallitsemiseksi. Toimenpiteet listataan pykälässä 4:21.2 ja kohta g sisältää ”perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutuksen”. 4:20.1 velvoittaa johtoa hyväksymään ja valvomaan toimenpiteitä ja niiden toimeenpanoa. Riskienhallinnan takia 4:20.2 velvoittaa johtoa kouluttautumaan, jotta heillä on ”riittävät tiedot ja taidot kyetäkseen tunnistamaan riskejä ja arvioimaan kyberturvallisuusriskien hallintakäytäntöjä ja niiden vaikutusta toimijan tarjoamiin palveluihin.” Organisaation työntekijöille vastaava koulutus ei ole velvoittava, mutta vastaavan koulutuksen säännölliseen tarjoamiseen kannustetaan. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555)

Myös Kyberturvallisuuskeskus on koostanut NIS2-direktiivin vaadituista kyberhygieniakäytännöistä 13 käytännön listan, ja nosti listalle ensimmäiseksi perus-

tason tietoturvakäytäntöjen ohjeistamisen henkilöstölle, alihankkijoille ja muille kumppaneille. Vaikka tietoturvaohjeistus on ensimmäisenä, myös listan muut 12 perustason käytäntöä pitää toteuttaa, ja organisaatioiden pitää oman riskiarvionsa perusteella toteuttaa mahdollisesti myös muita tietoturvakäytäntöjä (Kyberturvallisuuskeskus 2024b).

Euroopan unionin yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus 2016/679) edellyttää henkilötietojen käsittelyä tietoturvallisesti asianmukaisilla teknisillä ja organisatorisilla toimilla, joilla taataan henkilötietojen eheys, luottamuksellisuus ja saatavuus (2:5.1f, 4:32.1). Rekisterinpitäjä vastaa käsittelystä, ja sen on myös kyettävä osoittamaan, että toimia noudatetaan (2:5.2, 4:30.2d). Tekniset ja organisatoriset toimet on suhteutettava ”käsittelyn luonteeseen, laajuuteen, asiayhteyteen ja tarkoitukseen”, sekä ”henkilöiden oikeuksiin ja vapauksiin kohdistuviin, todennäköisyydeltään ja vakavuudeltaan vaihteleviin riskeihin” (4:24.1). Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että henkilötietoja käsitellään vain rekisterinpitäjän ohjeiden mukaisesti (4:29, 4:32.4). Asianmukainen tietosuojakoulutus mainitaan nimeltä vain kohdassa 5:74.2n liittyen henkilötietojen siirtoon kolmansiin maihin tai kansainvälisille järjestöille. Suomen tietosuojalaissa ei mainita ohjeista ja tietosuojakoulutuksista (Tietosuojalaki 5.12.2018/1050).

Käytännössä yliopiston toimiessa rekisterinpitäjänä, sen pitää ohjeistaa ja kouluttaa henkilötietoja käsittelevää henkilöstöä, niin omaa henkilökuntaa ja tutkijoita kuin henkilötietojen käsittelijänä toimivien kumppaneiden henkilöstöä, tietojen käsittelystä kunkin tietoaineiston riskeihin nähden, sekä pitää kirjaa koulutuksista, jolla voidaan osoittaa ohjeiden mukainen käsittely. Henkilötiedot voivat olla moninaisia ja myös henkilöön liittyviä, kuten tietoliikenteen laitteita ja käyttäjiä yksilöiviä tunnisteita, jolloin tietosuojakoulutusta pitää antaa muillekin kuin varsinaisten henkilötietojen kanssa työskenteleville.

Yliopistojen tutkimuksissa käsitellään kaikenlaista tietoa, jota voidaan muussa ympäristössä käsitellä tiukemmin vaatimuksin: se mikä sairaalassa on potilastietoa, on yliopistoissa tutkimusdataa, jonka keräämiselle ja käsittelylle on tyypillisesti erikseen sallitut ehdot. Mikäli potilastietoa pitää sellaisenaan käsitellä, se

tehdään pääasiassa sairaaloiden ehdoilla ja järjestelmissä. Vaikka lakia sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä ei tällöin tarvitse yliopistojen puolella noudattaa, lain 5:27 edellyttämän tietoturvasuunnitelman vaatimukset henkilöiden kouluttamista tietojärjestelmien käyttöön ohjeistusten mukaisesti, sekä tietojärjestelmien ohjeistusten mukaisesta ylläpidosta ja päivittämisestä tarvittavan asiantuntemuksen ja ammattitaidon omaavien henkilöiden toimesta, ovat hyviä käytäntöjä yliopistojenkin puolella noudatettaviksi. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, 784/2021)

Traficomin kyberturvallisuutta koskevissa määräyksissä (Traficom 2025) Määräys teletoiminnan tietoturvasta (M67) on soveltamisalaltaan rajattu yleistä teletoimintaa harjoittaviin yrityksiin, kun yliopistot ovat ei-yleisiä yhteisötilaajia (Laki sähköisen viestinnän palveluista 7.11.2014/917). Määräyksen 5:1.2 henkilöstöturvallisuudesta edellyttää henkilöstöltä riittävää tietoturvaosaamista ja säännöllisesti järjestettyä tietoturvakoulutusta, sekä tietoisuutta tietoturvapolitiikasta, toimintaperiaatteista, sekä niiden tavoitteista ja vaikutuksista omiin työtehtäviin. Määräyksen perustelumuistion mukaan koulutus voi olla tehtäväkohtaisesti kohdennettua, ja koulutuksiin osallistumista on perusteltua seurata. Perustelumuistion mukaan teleyritys voi testata tietoturvaosaamista, ja kehittää tietoturvakulttuuria ottamalla henkilöstön mukaan tietoturvan kehittämiseen. (Traficom 2024)

3.2 ISO/IEC 27001:2023 ja 27002:2022: Tietoturvallisuuden hallintajärjestelmät ja hallintakeinot

ISO:n ja IEC:n julkaisemat Tietoturvallisuus, kyberturvallisuus ja tietosuoja -sarjan standardit kattavat tietoturvallisuuden hallintaa. Näistä tunnetuin ja sovelletuin on ISO/IEC 27001:2023: Tietoturvallisuuden hallintajärjestelmät, joka kuvaa miten organisaatiot voivat toteuttaa tietoturvallisuuden hallintajärjestelmän (information security management system, ISMS) parantamaan organisaation tietoturvallisuutta (ISO/IEC 27001:2023). Hallintajärjestelmän toteuttamiseen tarvittavia tietoturvan toimenpiteitä kuvataan ISO/IEC 27002:2022: Tietoturvallisuuden hallintakeinot -standardissa. Standardien numeron perässä vuosiluku kertoo kyseinen version julkaisuvuoden.

ISO/IEC 27001:tä sovelletaan maailmalla laajasti, mutta toiminnan sertifiointi, eli standardin mukaisen toiminnan toteaminen ulkoisen auditoijan toimesta, ei ole pakollista. Akateemiset organisaatiot sertifioivat harvoin toimintaansa ISO/IEC 27001:n mukaan, varsinkaan koko organisaation laajuudella, mutta tietoturvallisuuden hallintaa pyritään yleensä tekemään standardin mukaan. Näin oman toiminnan tietoturvallisuuden osoittaminen on helpompaa.

ISO/IEC 27001:2023:ssa on 22 vaatimusta. Tietoturvakoulutuksen vaatimukset ovat kappaleessa 7.3: Tietoisuus, joka on korkean tason linjaus siitä, miten organisaation ohjauksessa työskentelevien henkilöiden on oltava tietoisia tietoturvapolitiikasta ja heidän omasta vaikutuksestaan tietoturvaan ISMS:n noudattamisella ja noudattamattomuudella. (ISO/IEC 27001:2023)

Tarkempi ohjeistus tietoisuusvaatimuksen toteuttamiseen kuvataan ISO/IEC 27002:2022:n hallintakeinossa 6.3: Tietoturvatietoisuus, -opastus ja -koulutus. Hallintakeinon mukaan organisaation ja sen tärkeimpien sidosryhmien henkilöstön on heidän työnsä kannalta saatava sopivaa tietoturvakoulutusta ja heidän on pysyttävä tietoisina organisaation tietoturvapolitiikasta, toimintaperiaatteista ja menettelytavoista. Koulutuksen tarkoituksena on saada henkilöstöt tietoisiksi heidän omasta vastuustaan tietoturvan toteutumiselle, jotta he ymmärtäisivät toimia vaatimusten mukaisesti. (ISO/IEC 27002:2022)

Tietoturvakoulutuksen pitää olla säännöllistä ja roolipohjaista, jotta uudet henkilöt, tai tehtävää vaihtavat, saavat tietoa tehtäviinsä liittyvistä tietoturva-asioista. Koulutuksen pitää kattaa myös ulkoinen henkilöstö omine rooleineen (kumppanit, toimittajat). Teknisen henkilöstön osaaminen on huomioitava erikseen, koska organisaation IT-järjestelmien tietoturva nojaa heidän tekemäänsä työhön ja ylläpitoon. Koulutuksen lopussa pitää olla testi, jolla varmistetaan koulutuksen menneen perille ja myös koulutuksen vaikutusta voidaan arvioida. (ISO/IEC 27002:2022)

Tietoturvatietoisuutta varten pitää kertoa johdon sitoutuminen tietoturvaan, organisaation toimintaa ohjaavat lait, politiikat, säännöt ja toimintatavat, henkilökohtainen vastuu, sekä tietoturvaan liittyviä teknisiä käytäntöjä. Koulutuksessa

pitää myös selittää miksi asioita tehdään, jotta henkilöstön ymmärrys tietoturvallisuuden tarkoituksesta ja heidän omasta vaikutuksestaan siihen paranee. Koulutusmenetelminä luetellaan pitkälti kaikenlaiset tavat välittää tietoa. (ISO/IEC 27002:2022)

Koulutuksen sisältöön kannattaa sisällyttää itsellä tai muualla tapahtuneiden tietoturvapoikkeamien opit (ISO/IEC 27002:2022). Tietoturvapoikkeamiin liittyy myös ISO/IEC 27001:2023:n vaatimus 6.1, joka edellyttää riskien ja mahdollisuuksien käsittelyä. Poikkeamat pitää huomioida riskienhallinnassa hallintajärjestelmän parantamiseksi, ja siten myös hallintajärjestelmän koulutusvaatimuksessa (ISO/IEC 27001:2023). Jatkuvasta parantamisesta on oma vaatimuksensa 10.1, jolla tavoitellaan hallintajärjestelmän soveltuvuuden, tarkoituksenmukaisuuden ja vaikuttavuuden jatkuvaa parantamista (ISO/IEC 27001:2023).

3.3 NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

National Institute of Standards and Technology (NIST) on Yhdysvaltain kansallinen mittaustekniikoita, standardeja ja tekniikkaa kehittävä virasto. NIST:n julkaisussa SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations määriteltyjen turvallisuus- ja yksityisyysmenetelmien noudattaminen on pakollista Yhdysvaltain liittovaltion virastoille. Vaikka NIST:n ohjeet eivät suomalaisiin korkeakouluihin suoraan vaikuta, kansainvälisessä yhteistyössä saattaa olla tarpeen osoittaa NIST:n standardien käytäntöjen noudattamista. NIST:n kattavat standardit ovat tarkastelun arvoisia niiden laajuuden ja yksityiskohtaisuuden takia.

SP 800-53 käsittelee tietoturvatietoisuutta ja koulutusta kappaleessa 3.2 Awareness and Training (NIST SP 800-53 Rev. 5., 86). Aiheeseen kuuluu kuusi kontrollia, joiden alla on yhteensä kymmenen alakontrollia (liite 1, Taulukko 7).

AT-2: Literacy training and awareness linjaa tietoturva- ja tietosuojakoulutuksen järjestämistä IT-järjestelmien käyttäjille (ml. johto ja alihankkijat) sekä sisällön päivittämisestä säännöllisesti ja huomioimaan itsellä tai muualla tapahtuneita

poikkeamia. Tietoturvatietoisuuden koulutusmateriaalin sisällön pitää liittyä organisaation tietoturva- ja tietosuojavelvoitteisiin, käyttöoikeuksiin ja myös työtapoihin – esimerkkinä etätyössä on huomioitava turvallisuutta eri tavoin kuin toimistolla (NIST 800-53 Rev. 5., 60).

AT-3: Role-based training linjaa tietoturva- ja tietosuojakoulutuksen järjestämisestä tietyn roolin omaaville henkilöille ennen pääsy antamista IT-järjestelmiin tai dataan, tai ennen tehtävien aloittamista. Roolipohjaisuutta varten organisaation pitää määritellä roolit, joissa organisaation tietoturva- ja tietosuojavelvoitteiden vastuut edellyttävät kohdennettua koulutusta – esimerkiksi tietyt käyttöoikeudet järjestelmiin ja dataan. (NIST SP 800-53 Rev. 5., 62).

Koulutusten suorittamista pitää seurata (AT-4) ja tuloksista pitää raportoida (AT-6) johdolle ja esihenkilöille, jotta tulosten mahdollisesti indikoiviin ongelmiin voidaan puuttua ajoissa.

Kohdennetulle koulutukselle tarjotaan selain- ja tietokonepohjaista koulutusta, luokassa annettavaa koulutusta, ja käytännön harjoittelua, mukaan lukien mikrokoulutukset (NIST SP 800-53 Rev. 5., 62). Suurin osa tietoturvakoulutuksesta on kirjallista, mutta tietoturvatesteihin on viittauksia kontrolleissa AT-2(1) kalastelusimulaatioiden osalta ja AT-3(3):ssa henkilötietojen tunnistamiseen ja käsittelyyn liittyen.

Vaatimuksissa ei suoraan sanota mitä tehdään, jos koulutuksia ei suorita. Koska aloitus- ja päivityskoulutuksia edellytetään käyttöoikeuksille ja tehtävässä toimimiselle, voidaan tulkita, että tehtävissä ei voi jatkaa ilman koulutusten suorittamista. (NIST SP 800-53 Rev. 5., 62)

Kokonaisuutena SP 800-53 -standardi antaa kattavaa ohjeistusta tietoturvakoulutuksen järjestämiseen. Varsinaisen tietoturvakoulutusohjelman toteuttamiseen kannattaa kuitenkin ennemmin käyttää NIST:n ohjeistusta SP 800-50r1: Building a Cybersecurity and Privacy Learning Program, johon SP 800-53:n kontrollit viittaavat.

3.4 NIST Cybersecurity Framework 2.0

NIST julkaisi 2024 kyberturvallisuuden riskienhallintaviitemallista Cybersecurity Frameworkista (CSF) version 2.0. CSF:n ensimmäisessä versiossa oli viisi kyberturvallisuusriskien lopputulemia kuvaavaa funktiota: Identify (kyberriskien tunnistaminen), Protect (suojatoimet kyberuhilta), Detect (hyökkäysten havaintokyky), Respond (hyökkäysten torjunta), Recover (poikkeamista toipuminen), joiden lisäksi versio 2.0 toi kuudennen pilarin Govern (kyberturvallisuuden hallinta). Funktiot kuvaavat toimia, joita käyttämällä organisaatiot hallitsevat kyberturvallisuuden riskejä. (NIST CSF 2.0)

Funktioiden ja kategorioiden lisäksi CSF 2.0 tarjoaa myös esimerkkiratkaisuja, joiden avulla organisaatioiden on helpompi toteuttaa toimia. (NIST 2024)

Protect-funktion alle kuuluu Awareness and Training -kategoria (PR.AT), jonka toimet kehittävät tietoturvatietoisuutta ja kouluttavat henkilökuntaa kyberturvallisuuteen liittyvien tehtävien suorittamista varten.

Ensimmäinen toimi PR.AT-01 koskee tietoisuutta ja koulutusta kyberriskeihin yleisellä tasolla (NIST CSF 2.0). Esimerkeissä säännöllisin väliajoin annettavan koulutuksen kohteena ovat kaikki ei-julkisten IT-järjestelmien käyttäjät ja peruskyberturvallisuuden osaamista suositellaan testattavaksi (NIST 2024).

Toinen toimi PR.AT-02 koskee kohdennettujen roolien tietoisuutta ja koulutusta kyberriskeihin (NIST CSF 2.0). Esimerkeissä opastetaan tunnistamaan kyberturvallisuudesta lisäkoulutusta kaipaavat roolit, kuten turvallisuus- ja tietoturvahenkilöstö, taloushallinto, johto, ja muut keillä on pääsy liiketoiminnalle kriittiseen tietoon, mukaan lukien ulkopuoliset kumppanit ja toimittajat.

3.5 CIS Critical Security Controls 8.1

Yhdysvaltalaisen Center for Internet Securityn (CIS) ylläpitämä Critical Security Controls -viitekehikko tarjoaa käytännöllisiä ohjeistuksia tietoturvan toteuttamiseen tehokkaasti. Critical Security Controls koostuu 18 kontrolliluokasta, joihin

kuhunkin kuuluu useampia suojatoimia. Nämä ovat teknisiä, hallinnollisia, ja ihmisiä koskevia. Suojatoimet on luokiteltu NIST:n CSF 2.0:n funktioiden mukaan ja jaoteltu kolmeen toteutusryhmään (Implementation Group, IG1–IG3), joissa alemman ryhmän toimet myös ylempään. (CIS 2024)

Toteutusryhmät mitoittavat suojatoimia eri kokoisten organisaatioiden oletetun toteuttamisvalmiuden mukaan. IG1-ryhmän suojatoimet ovat olennaisia kyberhygieniakäytäntöjä, jotka ovat myös pienten ja keskisuurten yritysten toteutettavissa rajallisilla resursseilla. IG2-ryhmän suojatoimet ovat isommille organisaatioille, joilla on dedikoitua henkilökuntaa hallitsemassa ja suojaamassa IT-ympäristöjä. IG3-ryhmän vaatimukset ovat yhteiskunnalle kriittisille organisaatioille, joilla on useampia tietoturvan eri osa-alueisiin erikoistuneita asiantuntijoita. Suomalaiset yliopistot kuuluvat pitkälti IG2-tasolle. (CIS 2024)

Kontrolliluokka 14: Security Awareness and Skills Training sisältää yhdeksän suojatoimea tietoturvakoulutuksen ja -tietoisuuden kehittämiselle. Suojatoimi 14,1 edellyttää tietoturvatietoisuusohjelmaa ja suojatoimet 14,2–8 kuvaavat koulutettavia aiheita. Suojatoimi 14,9 edellyttää kohdennettua koulutusta organisaation tietoturvaan vaikuttaville henkilöille, kuten kehittäjille ja ylläpitäjille, sekä korkean profiilin henkilöille, jotka todennäköisimmin voivat joutua sosiaalisen manipuloinnin kohteeksi. (CIS 2024)

Suojatoimia kohdennetaan yleisesti organisaation työvoimalle eli käytännössä omalle ja ulkoistetulle henkilöstölle. Kaikki suojatoimet kuuluvat IG1-tasolle lukuun ottamatta roolipohjaista tietoisuus- ja koulutusvaatimusta, jota edellytetään IG2-tasolta alkaen. Suojatoimi 14,1 edellyttää säännöllistä koulutusta, vähintään uudelle henkilöstölle ja vuosittain kaikille, mutta tietoturvaosaamisen testauksesta suojatoimissa ei ole mainintaa. (CIS 2024)

3.6 Kansalliset tietoturvallisuuden arviointikriteeristöt: Julkri, Katakri, Pitukri

Suomessa on kolme tietoturvallisuuden arviointiin tarkoitettua kriteeristöä: valtionvarainministeriön julkaisema Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), ulkoministeriön Tietoturvallisuuden auditointityökalu viran-

omaisille (Katakri), sekä liikenne- ja viestintäministeriö Traficomin alaisen Kyberturvallisuuskeskuksen Pilvipalveluiden turvallisuuden arviointikriteeristö (Pitukri). Näistä Katakri on vanhin, sen ensimmäinen versio julkaistiin jo 2009, ja sitä on myös eniten käytetty, erityisesti turvaluokitellun sisällön käsittelyyn (Ulkoministeriö 2020). Pilvipalveluiden käytön arviointiin käytetty Pitukri julkaistiin 2019 (Kyberturvallisuuskeskus 2019) ja julkishallintoa koskeva Julkri 2022 (Valtionvarainministeriö 2022).

Katakri-vaatimusten hallinnollisen tietoturvallisuuden alla on vaatimus T-12: Turvallisuuskoulutus. Henkilöstöllä ja organisaation lukuun toimivilla pitää olla riittävä tuntemus tiedonhallintaa, tietojenkäsittelyä sekä tietojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja organisaation ohjeista. Koulutuksessa pitää kertoa turvallisuusluokiteltuun tietoon kohdistuvista ja tehtävien kannalta keskeisistä uhista sekä niihin liittyvistä ajantasaisista ohjeista. Koulutuksen pitää olla säännöllistä ja osallistumista on seurattava.

Pitukri-vaatimuksissa henkilöstöturvallisuuden alla on vaatimus HT-04: Turvallisuustietoisuus, joka koskee omaa sekä ulkoisten palveluntarjoajien ja toimittajien henkilöstöä. Vaatimuksessa edellytetään, että organisaation keskeiset turvallisuutta koskevat periaatteet ja toimintatavat on dokumentoitu, ja henkilöstön riittävästä turvatietoisuudesta pystytään varmistumaan. Tämän jalkauttamista käytäntöön pitää olla säännöllisesti, vähintään vuosittain, ja osallistujista pidetään kirjaa. Annetussa esimerkissä ehdotetaan kohderyhmittäin räätälöityä koulutusta ja turvallisuustietoisuuden kehittämisohjelmaa. Tavoitteena on, että henkilöstö pystyy käytännössä toimimaan turvallisten toimintatapojen mukaisesti myös erikoistilanteissa. Tämä käytännössä edellyttää tietoturvatietoisuutta, jolloin henkilöstö ymmärtää tilanteet myös koulutettujen tilanteiden ulkopuolelta.

Julkri-vaatimuksissa hallinnollisen turvallisuuden alla on vaatimus HAL-13: Koulutukset, jolla varmistetaan, että henkilöstö ja muut organisaatiolle toimivat henkilöt ovat tietoisia voimassa olevista tietoturvallisuutta koskevista määräyksistä ja ohjeista, sekä tietoihin kohdistuvista uhista ja riskeistä. Erityishuomiota ohjataan korkeamman riskin tehtäviin, kuten etäkäyttöön ja tietojärjestelmien ylläpitoon. Esimerkissä koulutus huomioi työtehtävien tarpeet, eli se on roolipohjais-

ta. Vaatimus HAL-14 käyttö- ja käsittelyoikeuksista linjaa, että käsittelyoikeudet voidaan antaa vain henkilölle, jolle on selvitetty tietojen suojaamista koskevat ohjeet.

Käytännössä kaikki kolme arviointikriteeristöä edellyttävät säännöllistä ja seurattua koulutusta tietojen turvallisesta käsittelystä organisaatiossa. Vaatimuksissa edellytetään osaamisen varmistamisesta, mutta varmistustapaa ei vaatimuksissa sanota. Käytännössä sen voi kuitenkin tulkita tarkoittavan osaamisen testaamista pelkän koulutukseen osallistumisen seuraamisen lisäksi.

Vaikka roolipohjaista kohdennettua koulutusta ei vaatimuksissa suoraan edellytetä, siihen kuitenkin viitataan esimerkeissä. Pakollisen koulutuksen kohteena ovat kaikki organisaation lukuun työskentelevät omat ja ulkoiset henkilöt.

3.7 Kybermittari-arviointityökalu v2.1

Kyberturvallisuuskeskuksen kehittämä Kybermittari on Suomessa toimivien huoltovarmuuskriittisten yritysten ja organisaatioiden tarpeisiin räätälöity kypsyysmalli, joka vaatimusten sijaan arvioi organisaation toiminnan kypsyyttä tasoasteikolla. Kybermittari tarjoaa näkymän toiminnalle tärkeiden kyberkyvykkyyksien kypsyystasoon osa-alueittain ja tavoitteittain. Mittari näyttää, millä tasolla kyberriskien tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen ovat organisaatiossa. Kybermittari pohjautuu NIST:n kyberturvallisuuden riskienhallintaviitemalliin Cybersecurity Frameworkiin (CSF) sekä Yhdysvaltain Department of Energyn kyberturvallisuuden kypsyysmalliin Cybersecurity Capability Maturity Modeliin (C2M2). (Kyberturvallisuuskeskus 2024)

Tietoturvakoulutuksen kypsyyden arviointi löytyy Kybermittarin WORKFORCE-osiosta, joka koskee organisaation kykyä kehittää ja ylläpitää henkilöstön kyberturvallisuusosaamista ja -valmiutta. Osio jakautuu viiteen osa-alueeseen: kyberturvallisuuden vastuiden jakaminen (WORKFORCE-1), kyberturvallisuuteen keskittyvän henkilöstön kehittäminen (WORKFORCE-2), henkilöstöhallinnon prosessit (WORKFORCE-3), koulutus ja kybertietoisuuden lisääminen (WORK-

FORCE-4), sekä yleiset hallintatoimet (WORKFORCE-5). (Kybermittari-arviointityökalu 2.1).

Kybermittarin eri osa-alueiden arviointikysymyksiin vastataan viisiportaisella asteikolla. Vastauksista lasketaan osa-alueiden kypsyys tasoasteikolla 0–3, jossa 3 on korkein kypsyystaso. (Kybermittari-arviointityökalu 2.1)

WORKFORCE-2:ssa tasolle 1 pääsee henkilöstön kyberturvatietoisuuden kohottamistoimilla. Tasolla 2 kyberturvallisuustietoisuudelle on asetettu organisaation uhkiin vastaavia tavoitteita, ja tietoisuutta parantava toiminta on säännöllisestä ja seurattua. Tasolla 3 tietoisuustoimet on kohdennettu roolipohjaisesti, niiden tehokkuutta arvioidaan ja ne kytkeytyvät organisaation toimintatiloihin, esim. korotetun turvallisuuden tilaan.

WORKFORCE-4 koskee henkilöitä, joilla on kyberturvallisuuteen liittyviä vastuita. Tasolla 1 näille on tarjolla kohdennettua koulutusta, ja kyberturvallisuusosaamisen vaatimukset ja puutteet on tunnistettu. Tasolla 2 tunnistettuja puutteita paikataan koulutuksella, rekrytoinneilla ja vaihtuvuuden pienentämiseen tähtäävillä toimilla. Kohdennettu kyberturvallisuuskoulutus on edellytys käyttöoikeuksille toiminnon kannalta tärkeisiin tietojärjestelmiin ja tietoihin. Tasolla 3 koulutustoiminnan tehokkuutta arvioidaan ja kehitetään säännöllisesti testien tai arviointien avulla, ja merkittävää kyberturvallisuusvastuuta omaaville henkilöille on tarjolla ammatillisia kehitysmahdollisuuksia.

3.8 NCSC Cyber Assessment Framework 3.2

Britannian kansallisen kyberturvallisuusviranomaisen National Cyber Security Centren (NCSC) Cyber Assessment Framework (CAF) -viitekehikko on kehitetty organisaatioiden käytössä olevien kyberturvallisuustoimien arviointiin. CAF koostuu neljästä korkean tason tavoitteesta (objective) ja 14 periaatteesta (principle), jotka on kuvattu saavutettavina tuloksina (outcome) tarkistuslistojen sijaan. Tulosten saavuttamista arvioidaan asioilla, joita pidetään merkkeinä hyvistä käytännöistä (indicator of good practice, IGP). Tuloksia pidetään joko saa-

vutettuina tai ei-saavutettuina, mutta joidenkin periaatteiden osalta myös osin saavutettu tulos on mahdollinen. (NCSC 2024a, 3)

Yleisluontoisuudestaan huolimatta CAF:n periaatteet eivät välttämättä sovellu sellaisenaan kaikille sektoreille. NCSC suosittelee tavoitteiden saavuttamiseksi sopimaan sektorikohtaisista CAF-profiileista, IGP-tulkinnoista ja mahdollisista lisä-IGP:istä. Esimerkiksi koulutussektori poikkeaa muista sille ominaisten opiskelijoiden ja oppilaiden osalta, jotka voisi sopia jäämään tietoturvakoulutusten ulkopuolelle. (NCSC 2024a, 5)

Periaate B6: Staff Awareness and Training edellyttää, että henkilöstöllä on kyberturvallisuudesta työtehtäviinsä sopivat tiedot, taidot ja tietoisuus. Periaate jakautuu kyberturvallisuuden kulttuuriin (B6.a) ja kyberturvallisuuden koulutukseen (B6.b). (NCSC 2024a, 29)

B6.a: Cyber Security Culture (liite 2, Taulukko 8) edellyttää positiivisen kyberturvallisuuskulttuurin kehittämistä ja ylläpitämistä. Tietoturvakulttuurin merkitys on tärkeä, kun teknologista ratkaisua ei voida käyttää, ja ihmisten edellytetään tekevän oikeita valintoja. (NCSC 2024b)

B6.b: Cyber Security Training (liite 2, Taulukko 9) edellyttää säännöllistä tietoturvakoulutusta, jonka suorittamista seurataan. Koulutuksessa ja tietoisuusviestinnässä käytetään monia menetelmiä ja kanavia, ja niiden tavoittavuutta ja tehokkuutta arvioidaan säännöllisesti. (NCSC 2024a, 30)

CAF poikkeaa muista viite- ja kypsyysmalleista sen ihmislähtöisen suhtautumisen ja tietoturvakulttuuriin huomioinnin takia.

3.9 GÉANT Security Baseline v1.2.1

Pan-eurooppalaista tutkimuksen ja koulutuksen runkoverkkoa ja digitaalisia palveluja tarjoavan GÉANT-yhdistyksen Security Baseline on tietoturvallisuuden viitekehys kansallisten tutkimuksen ja koulutuksen tietoliikenneverkkojen (NREN) operaattoreille. NREN-verkot, kuten suomalainen Funet-verkko, mahdollistavat kansainvälistä tieteellistä yhteistyötä ja NREN-verkkojen keskinäiset

riippuvuudet edellyttävät yhtenäisten ja vertailukelpoisten tietoturvakäytäntöjen noudattamista. Security Baseline jakautuu neljään osioon: Policy, People, Threats ja Operations, joilla kullakin on 3–5 alakohtaa. Vaatimusten alakohdat on jaettu kolmelle kypsyystasolle: Baseline (1), Advanced (2), ja Expert (3), jotta tietoturvaohjelmaa voidaan kehittää vaiheittain. (GÉANT 2024a)

Security Baselinen koulutus- ja tietoisuusvaatimukset ovat People-osion ensimmäisessä alakohdassa Training and Awareness, joka koostuu seitsemästä vaatimuksesta (Taulukko 1). (GÉANT 2024a)

Taulukko 1. Security Baselinen koulutusvaatimukset (GÉANT 2024a).

#	Requirements	1	2	3
TA1.1	All employees, (sub) contractors, temporaries etc. must follow an information security awareness training regularly.	●	●	●
TA1.2	Training records are maintained.	●	●	●
TA1.3	Achieving high standards for information security is cultivated and all staff are aware of their responsibilities.	●	●	●
TA2.1	A plan for role-based training is created once a year.		●	●
TA2.2	A security communication plan including internal and external communication is in place.		●	●
TA3.1	Regular audits verify the security awareness of employees.			●
TA3.2	Top management is highly aware of security aspects and sets an example to its employees.			●

Security Baseline lähtee liikkeelle vähintään henkilöstön kouluttamisesta ja suoritusten seuraamisesta. Tietoturvatietoisuudella on tarkoitus ensisijaisesti nostaa ihmisten tietoisuutta erilaisista uhista, menetelmistä ja huijauksista, joita hyökkääjät käyttävät päästäkseen tavoitteeseensa. Tietoturvaosaamisen säännöllistä tarkastamista, esimerkiksi tietoturvatestillä, edellytetään vasta korkeimmalla Expert-tasolla. (GÉANT 2024a)

3.10 Security Incident Management Maturity Model v2 Interim

Security Incident Management Maturity Model eli SIM3 on kypsyysmalli tieto- ja kyberturvapoikkeamien hallintaa hoitavien organisaatioiden arviointiin. Mallia voidaan soveltaa tällaista kyvykkyyttä tarjoaviin organisaatioihin niiden nimityksestä ja järjestämistavasta riippumatta, kuten CSIRT-ryhmiin tai SOC-palveluihin. SIM3 käyttää CSIRT-termiä sen tunnettuuden takia. (Stikvoort ym. 2023)

SIM3:n kypsyysmalli rakentuu kypsyysparametreista, joita arvioidaan viisitasoisella kypsyysasteikolla. Parametrit jakaantuvat neljälle osa-alueelle: organisaatio, ihmiset, työkalut ja prosessit. Osa-alueiden parametreja mitataan viisitasoisella kypsyysasteikolla, joka arvioi miten muodollisesti asiaa hoidetaan. Organisaatioparametreilla selvitetään CSIRT:n toimeksiantoa, sisäistä toimintaa, ja palveluja. Ihmisparametreilla mitataan CSIRT:n inhimillistä puolta: etiikkaa, resilienssiä, taitoja ja verkostoitumista. Työkaluparametrit liittyvät CSIRT:n käyttämiin järjestelmiin ja työkaluihin. Prosessiparametreilla mitataan CSIRT:n tietoturvapoikkeamien hallinnan kypsyyttä. (Stikvoort ym. 2023)

SIM3:n tietoturvakoulutukseen liittyvät parametrit (Taulukko 2) ovat ihmiset-osiossa ja niissä selvitetään, onko CSIRT:n tehtävissä tarvittuja taitoja määritelty, miten näitä tarvittuja taitoja kehitetään, ja onko tarkempaa suunnitelmaa teknisten ja pehmeiden taitojen kerryttämiseksi. Teknisen koulutuksen vaatimus parametri sisällyttää perehtymistä uusiin aiheisiin ja teknologioihin, joita tietoturvahenkilöstö tarvitsee pysyäkseen ajan tasalla teknologian ja hyökkäysten saralla. (Stikvoort ym. 2023)

SIM3-mallista on hyötyä korkeakouluille niiden tietoturvatoiminnan kypsyyden kehittämisessä, sekä tason osoittamisessa FIRST:n ja Trusted Introducerin kaltaisiin uhkatietoa jakaviin CSIRT-verkostoihin osallistuessa. Koulutusvaatimukset parantavat tietoturva-asiantuntijoiden ymmärrystä uhista ja niiltä suojautumista ihmisten, prosessien ja teknologian avulla. Erityisesti H-6-vaatimus viestintä- ja esiintymistaidoista on hyödyksi, kun tietoturva-asiantuntijat osallistuvat tietoturvakoulutusten ja -tietoisuuden kehittämiseen ajantasaisen tiedon ja ohjeiden osalta.

Taulukko 2. SIM3-kypsyysmallin tietoturvakoulutukseen liittyvät parametrit. (Stikvoort ym. 2023)

Parameter	Parameter name	Parameter description
H-3	Skillset Description	Describes the skills needed on the CSIRT job(s).
H-4	Staff Development	Staff development policy, to facilitate the training of new team members and improve the skills of existing ones.
H-5	Technical Training	Programme to allow staff to get job-related technical training - like TRANSITS, ENISA CSIRT Training, or commercial training programs (CERT/CC, SANS, etc.).
H-6	Soft Skills Training	Programme to allow staff to get soft skills training, including especially (human) communication/presentation training.

3.11 Sopimusvaatimukset

Yliopistot tekevät laajasti yhteistyötä yksityisten ja julkisten organisaatioiden kanssa. Kyseessä voi olla molempia osapuolia hyödyttävää tutkimus-, kehitys- ja innovaatiotoimintaa, tai ulkoinen organisaatio voi luovuttaa aineistoa yliopistolla tehtävää tutkimusta varten. Molemmissa tapauksissa osapuolten välisissä sopimuksissa on myös tietoturvaan ja tietosuojaan liittyviä vastuita ja velvollisuuksia, esimerkiksi yliopiston toimiessa henkilötietojen käsittelijänä ja kumppanin ollessa rekisterinpitäjä.

Organisaatiot haluavat suojautua riskeiltä, jotka voivat aiheutua suoraan kumppanista, sekä epäsuorilta riskeiltä, joissa kumppani on välikätenä. Suoraan kumppanista aiheutuvia riskejä ovat esimerkiksi haittaohjelmien saastuttamat tietokoneet, luottamuksellisten tietojen vuotaminen, tai vaarallisesti toimiva henkilöstö. Epäsuoria riskejä aiheutuu muun muassa toimitusketjuhyökkäyksistä,

joissa hyökkääjä tunkeutuu organisaatioon kumppanin kautta hyväksikäyttämällä näiden välistä luottosuhdetta, esimerkiksi pääsemällä organisaation sisäisiin tietojärjestelmiin.

Lakitermein organisaatiot haluavat due diligence -tarkastuksilla vahvistaa, että kumppanit toimivat asianmukaisella huolella (due care), myös tietoturvan osalta (ZenGRC 2024). Usein tietoturvan osalta kysytään, onko kumppanilla käytössä sertifioitua tietoturvan hallintajärjestelmää, kuten ISO/IEC 27001, tai miten vastaavat toimet on hoidettu sertifioinnin puuttuessa. Organisaatioilla voi olla kumppanien arviointiin valmiita tarkistuslistoja niiden oman toiminnan tai tietojen suojaamisen kannalta tärkeimmiksi koettujen kontrollien osalta, jos kumppaneilla ei useimmiten ole näyttää sertifikaattia toiminnastaan. Henkilöstöriskien osalta voidaan kysyä tietoturvakoulutusten, tietoturvatietoisuustoimien sekä tietosuojakoulutusten järjestämisestä ja sisällöstä.

Yliopistojen on helpointa osoittaa parhaiden käytäntöjen mukaista toimintaa sertifioidulla tietoturvan hallintajärjestelmällä, kuten ISO/EC 27001. Sertifioinnin puuttuessa vastaavan toiminnan osoittaminen onnistuu näyttämällä dokumentaatiota käytetyistä tietoturvan hallintatoimista, joissa viitataan viitemallien käytäntöihin.

3.12 Vaatimusten mukainen tietoturvakoulutus

Taulukko 3 on koottu edellä käsitellyt vaatimukset tietoturvakoulutukselle. Yliopistoja koskevia vaatimuksia tietoturvakoulutukselle tulee vain tiedonhallintalaista ja tietosuoja-asetuksesta, jotka edellyttävät yliopistojen tietoturvakoulutuksien pohjautuvan tunnistettujen riskien käsittelyyn. Tätä varten yliopistoilla on hyvä tehdä tietoturvan ja kyberturvallisuuden riskienhallintaa järjestelmällisesti, jotta myös tietoturvakoulutusten sisältö osana suojatoimenpiteitä vastaisi riskiarviointia. Jos riskienhallintaa ei tehdä, koulutuksissa voidaan huomioida vääriä riskejä, jotka voivat olla näkyviä, mutta vaikutukseltaan pieniä. Riskienhallinnassa suojatoimenpiteet voidaan myös kohdentaa prosesseissa tai teknologialla ratkaistaviksi, jolloin riskeistä ei välttämättä tarvitse kouluttaa ihmisiä.

Taulukko 3. Vertailtujen lakien, asetusten ja viitemallien koulutusvaatimukset.

	Tiedonhallintalaki	NIS2-direktiivi	**Tietosuoja-asetus**	Traficom M67	ISO/IEC 27001 & 27002	NIST SP 800-53	NIST CSF	CIS CSC	Kansalliset viitemallit	Kybermittari	NCSC CAF	GÉANT Security Baseline	SIM3
Riskipohjainen sisältö	●	●	●		●	●	●	1	●	1	●	1	
Henkilöstön koulutus	●	●	●	●	●	●	●	1	●	1	●	1	●
Tietoturvavastuisten					●	●	●	1	J	1			●
Kaikkien, ml. opiskelijat						●		1			●		
Roolipohjainen sisältö	●		●	○	●	●	●	2	●	3	●	2	
Edellytys oikeuksille			●			●			J	2			
Säännöllinen koulutus				●	●	●	●	1	●	2	●	1	
Suorituksia seurattava			●	●	●	●			●	2	●	1	
Osaamista arvioitava				○	●	○	○			3		3	
Sisällön tarkastusväli						Itse		1v			Itse	1v	

Selitykset: ●) pakollinen, ○) valinnainen, 1–3) kypsyysmallin taso, J) Julkri

Kaikki tutkitut vaatimukset edellyttävät henkilöstön kouluttamista, joka kattaa käytännössä kaikki yliopistolle työskentelevät henkilöt eli myös ulkoistuskumppanien ja alihankkijoiden henkilöstön. Lähes kaikki viitemallit edellyttävät erikseen tietoturvavastuita omaavan henkilöstön kouluttamista tietoturvan saralla, koska heidän on tunnettava uhkaympäristö, ymmärrettävä miten hyökkäyksiä tehdään, ja osattava soveltaa teknologiaa organisaation suojaamiseksi ja suojakaiteiden rakentamiseksi.

Kaikkien tietojärjestelmien käyttäjien kouluttamista, johon voidaan laskea myös yliopistojen opiskelijat ja harjoituskoulujen oppilaat, edellytetään SP 800-53:ssa, Critical Security Controlsissa ja Cyber Assessment Frameworkissa. Opiskelijoiden asemaa yliopistoyhteisössä on pohdittu digipalvelulain (Laki digitaalisten palvelujen tarjoamisesta 306/2019) vahvan tunnistautumisen vaatimukseen

2:6.1 liittyen. Olennainen ero tutkinto-opiskelijoiden suhteessa muuhun yliopistoyhteisöön on, että he eivät käytä tietojärjestelmiä palvelussuhteen perusteella, vaan ovat digipalvelulain silmissä yleisöä (Aivio ym. 2022). Tätä tulkintaa käyttäen kaikkia tietojärjestelmiin käyttäjätunnuksen omaavia ei tarvitse tietoturvakouluttaa, jos organisaation riskienhallinta tämän sallii. Koulutus on kuitenkin tarpeen opiskelijoiden siirtyessä henkilöstöön rinnastettaviksi tutkijoiksi, ja kun opiskelija tarvitsee pääsyn korkean riskin tietojärjestelmiin.

Henkilöstön tehtäviin kohdennettu roolipohjainen koulutus on vaatimuksena lähes kaikissa tutkituissa lähteissä, erityisesti organisaation toiminnalle tärkeissä tehtävissä työskenteleville. Tietosuoja-asetus ja SP 800-53 vaativat kohdennettua koulutusta edellytyksenä käyttöoikeuksien myöntämiselle. Kybermittari edellyttää tätä tietoturvahenkilöstön käyttöoikeuksille tasolla 2.

Pitkälti kaikki viitemallit edellyttävät koulutuksen säännöllistä järjestämistä, kuten uuden henkilön aloittaessa tehtävässä, sekä vähintään vuoden välein kertauksena ja uusien riskien osalta. Koulutusta on hyvä antaa myös tehtävää vaihtaessa, ja muista organisaation määrittelemistä perustelluista syistä.

Kirjanpitoa tietoturvakoulutuksiin osallistumisesta edellytetään suurimmassa osassa viitemalleja. Seuranta on henkilötietoja käsittelevän henkilöstön osalta pakollista tietosuoja-asetuksen osoittamisvelvollisuuden takia.

Henkilöstön tietoturvaosaamisen varmistaminen on pakollista vain ISO/IEC 27001:ssä ja GÉANT Security Baselinen korkeimmalla tasolla. Mainінta valinnaisesta tietoturvaosaamisen testaamisesta löytyy ISO/IEC 27001:tä peilaavasta Traficomin määräyksestä teletoiminnan tietoturvasta sekä NIST:n SP 800-53:sta ja Cybersecurity Frameworkista. SP 800-53 ehdottaa erilaisia käytännön harjoituksia lisäyksenä koulutuksiin ja CSF tarjoaa esimerkeissä säännöllistä tietoturvaosaamisen arviointia tai testausta.

Tietoturvakoulutuksen sisällön tarkastaminen ja päivittäminen mainitaan muutamassa viitemallissa. SP 800-53 jättää organisaation määriteltäväksi, kuinka usein sisältöä päivitetään, mutta listaa monia perusteita, joiden myötä sisältöä pitäisi päivittää: tietoturva-arviointien tulokset, tietoturvapoikkeamat, muutokset

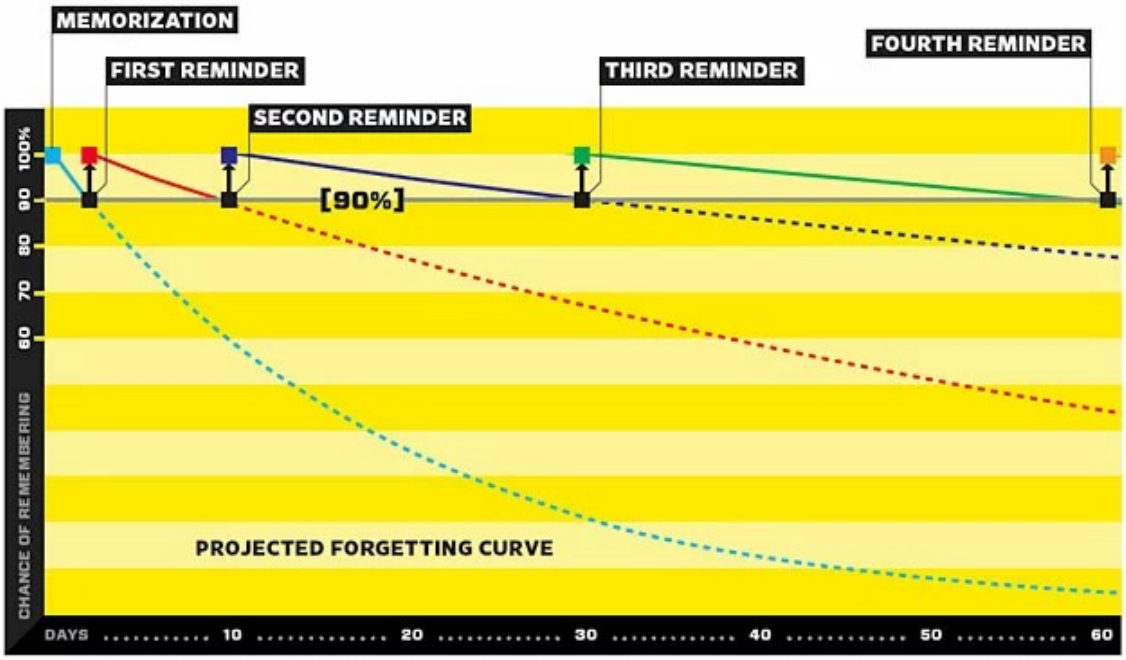
laeissa, asetuksissa, politiikoissa ja ohjeissa. Myös tekoälyn yleistymisen kaltaisten nopeiden muutosten yhteydessä pitää olla nopeasti tuomassa tietoa koulutusmateriaaleihin. CAF edellyttää rutiininomaista päivittämistä sisällön mahdollisimman laajan yleisön tavoittamiseksi ja tehokkuuden takaamiseksi. Critical Security Controls ja GÉANT Security Baseline linjaavat vähintään vuoden päivitysvälin. ISO/IEC 27001:2023 edellyttää jatkuvaa parantamista ja ISO/IEC 27002:2022 huomioimaan tietoturvapoikkeamista opitut asiat.

Yliopistojen sec-työvaliokunta on sopinut yhteiseksi tavoitteeksi Kybermittarin tason 1 saavuttamisen kaikilla osa-alueilla 2025 loppuun mennessä. Vaatimustason täyttävä koulutus pohjautuu kunkin yliopiston omiin riskiarvioihin, on pakollista henkilöstölle ja kaikille kumppaneille ja toimittajille. Sisältö on tehtäväkohtaista eli roolipohjaista, ja tietoturvavastuita omaaville henkilöille on oma koulutuspolku. Tietosuoja-asetuksen mukaisesti koulutus pitää suorittaa ennen kuin henkilötietoja sisältäviin järjestelmiin saa oikeudet, ja osallistumista seurataan erityisesti henkilötietoja käsittelevien henkilöiden osalta.

Ehdotettu vuosittain 5–10 minuutissa suoritettava, kaikille yliopistolaisille pakollinen ja sisällöltään samanlainen, kahden vuoden välein päivitettävä, kouluttava tietoturvatesti ei täytä edellä kuvattuja vaatimuksia eikä viitemallien parhaita käytäntöjä. Parhaimmillaan se voi lisätä yliopistolaisten tietoturvatietoisuutta, mutta testin käyttämistä vaatimukset täyttävän koulutuksen rinnalla kannattaa harkita.

4 Tietoturvatietoisuus ja tietoturvakulttuuri

Tietoturvatietoisuus on, tietoturvauhkiin liittyen, informaation tietoista käsittelyä, jolloin tehdään tietoisia valintoja automaattisten toimien sijaan (Richter ym. 2018). Tietoturvatietoisuus on tiedon levittämistä omassa toimintaympäristössä tarvittavista tietoturvallisista toimintatavoista ja tietoturvauhista, jotta ihmiset osaisivat toimia oikealla tavalla kohdatessaan näitä uhkia. Koska rikolliset hyödyntävät kasvavassa määrin sosiaalista ulottuvuutta, ihmisten tietoturva-tietoisuuden puute on itsessään tietoturvauhka (Vilander 2021, 78). Tietoturva-tietoisuuden tärkeimpiä tehtäviä on saada ihmiset ymmärtämään tietoturvan tarkoitus, sekä heidän oma vastuunsa ja vaikutuksensa – niin positiivinen kuin negatiivinen – organisaation tietoturvallisuuteen (ISO/IEC 27002:2022).



Kuvio 3. Unohtamiskäyrä kuvaa opitun tiedon unohtamisen määrää ajan myötä, ja kertaamisen vaikutusta muistamiseen. (Biedalak & Woźniak 2017)

Tietoturvatietoisuuden kehittämisessä olennaista on tiedon iskostamisen toistuvuus, koska ihminen unohtaa nopeasti asiat, joita ei kerrata, tai joita ei joudu soveltamaan käytännössä. Unohtamiskäyrän (forgetting curve) teorian mukaan ihmiset voivat unohtaa yli puolet vasta oppimastaan tiedosta parissa viikossa

(Winkler & Brown 2021, 67; Kuvio 3). Vain vuoden välein toistettava tietoturvatesti tai -koulutus ei välttämättä pysy ihmisten mielessä, tai onnistu muuttamaan käytöstä, ja siten vähennä tietoturvariskejä.

Tehokkaat tietoturvatietoisuusohjelmat ottavat huomioon unohduskäyrän ja toistavat viestejä useita keinoja ja kanavia käyttäen (Winkler & Brown 2021, 227). ISO/IEC 27002:2022 6.3 ehdottaa tietoisuuden parantamiseen fyysisiä tai virtuaalisia kanavia, kuten kampanjoita, ohjelehtisiä, julisteita, uutiskirjeitä, verkkosivuja, tietoiskuja, esittelyjä, verkko-opintoja ja sähköposteja. NIST:n SP 800-53 Rev. 5:n vaatimus AT-2 listaa keinoina julisteet, tietoturvasta ja tietosuojasta muistuttavat toimistotarvikkeet, viestit kirjautumisikkunoissa, sähköposti-ilmoitukset sekä tietoisuustapahtumat. Tietoturvan ja tietosuojan oppimisohjelman rakentamiseen opastava SP 800-50 Rev. 1 listaa kaikille sopivina esimerkkeinä kirjautumisruutujen viestit, näytönsäästäjät, sähköpostin allekirjoitusten viestit, uutiskirjeet, paperiset ja digitaaliset julisteet, tietoisuustapahtumat, muistutukset työvälineissä ja toimistotarvikkeissa, sekä säännölliset tai poikkeamiin liittyvät sähköpostiviestit (NIST SP 800-50 Rev 1, 2024, 30). Tietoisuutta voi edistää myös tietokonepohjaisella harjoittelulla, kalastelusimulaatioilla, koostettua tietoa tarjoavilla tietämyskannoilla sekä tietoturvatietoisuuden puolestapuhujien välityksellä (Winkler & Brown 2021, 238). Hiirimattojen ja kahvikuppien kaltaisten tietoisuusviesteillä varustettujen tarvikkeiden ei ole tarkoitus saada aikaan suurta muutosta, vaan passiivisesti pitää asiat ihmisten mielessä (Winkler & Brown 2021, 243).

Tietoisuusaktiviteetit voivat olla laajempia kampanjoita tai satunnaisia tietoiskuja riippuen aiheesta, uhasta tai haavoittuvuudesta. Tietoturvatietoisuutta kannattaa järjestää myös kausiluontoisesti, esimerkiksi globaalisti yleistyneen lokakuisen kyberturvallisuuskuukauden sekä akateemisen vuoden ajankohtien yhteydessä (SP 800-50 Rev. 1, 30). Tietoturvatietoisuutta kannattaa tuoda mukaan yleisiin tietojenhallinnan, tietotekniikan, tietoturvallisuuden, tietosuojan ja turvallisuuden koulutuksiin (ISO/IEC 27002:2022).

Tietoturvatietoisuudella pitäisi ISO/IEC 27002:2022 6.3:n mukaan kattaa organisaatiolle yleisiä näkökohtia, kuten johdon sitoutuminen koko organisaation tieto-

turvallisuuteen, tietoturvasäännöt ja velvoitteet, yleiset tietoturvamenettelyt, sekä mistä saa apua ja lisätietoa tietoturvaan liittyen. Tietoisuusohjelmassa pitäisi ohjeiden lisäksi myös perustella miksi asiat ovat tärkeitä.

Tietoturvatietoisuuden kehittämistä on tutkittu Knowledge–Attitude–Behavior- eli KAB-mallilla, jonka mukaan mitä enemmän ihmiset tietävät tietoturvasta, heidän asenteensa tietoturvaa kohtaan paranee, ja sen myötä myös käytös muuttuu tietoturvallisemmaksi (Kruger & Kearney 2006).

Tiedon tarjoamisesta ja toistamisesta huolimatta ihmiset eivät kuitenkaan välttämättä ymmärrä tietoa, muista tietoa, anna arvoa tiedolle, sovella tietoa, tai toimi tiedon mukaisesti (Carpenter & Roer 2022, 29). Tutkimuksen mukaan säännöllisen tietoturvakoulutuksen suorittamisesta ei ole selkeää hyötyä kalasteluviestien tunnistamisessa (Ho ym. 2025). Toisessa tutkimuksessa tietoturvakoulutusta suorittaneet avasivat herkemmin kalasteluviestien haitallisia linkkejä kuin koulutusta suorittamattomat (Lain ym. 2022). Gartnerin kyselyssä 92 prosentilla organisaatioista on käytössä tietoturvakoulutuksia, ja silti 69 prosenttia näiden henkilöstöstä on kertonut toimivansa tietoturvaohjeistusten vastaisesti (Candrick ym. 2023). Tietoturvakoulutuksissa ja -tietoisuusohjelmassa tiedolla on tärkeä rooli, mutta lopputulosten kannalta tärkeintä on saada aikaan muutoksia ihmisten arvoissa ja käytöksessä. Ilman muutosta tietoturvan tasoonkaan ei tule muutosta ja eivätkä riskit vähene. (Carpenter & Roer 2022, 29–30)

4.1 Käyttäytymisen muuttaminen

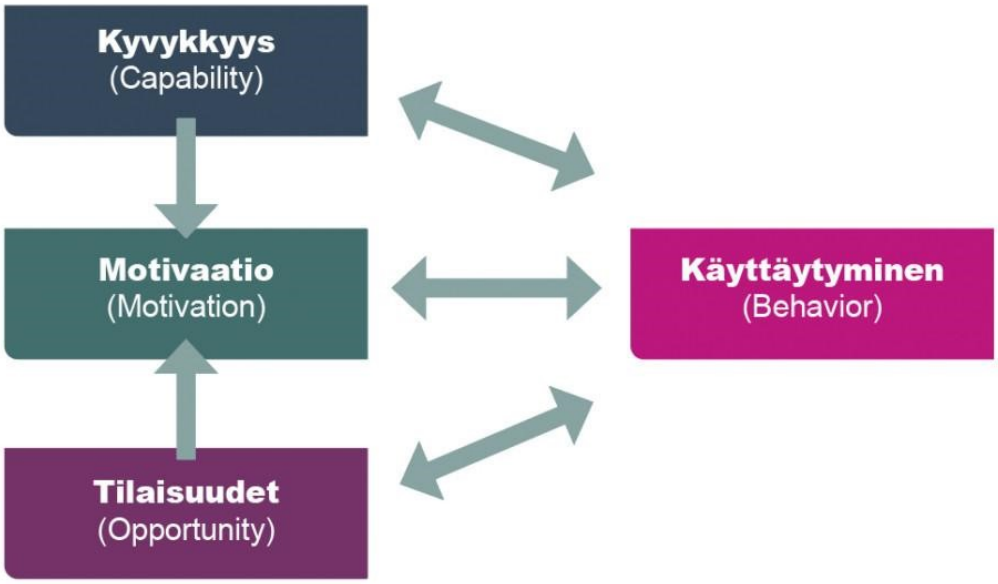
Psykologiassa tutkitaan ihmisen mieltä ja käyttäytymistä. Tietokoneiden käytön yleistymisen ja verkottumisen myötä ihmisten osuus tietoturvan toteutumisessa on kasvanut ja siksi myös ajattelu- ja käyttäytymistapojen huomiointi on tärkeää ihmisten tietoturvallisuuden kehittämisessä (Thomson & von Solms 1998). Sen sijaan, että tietoturvaan liittyvää ihmisen toimintaa tutkittaisiin uutena tieteenalana, kannattaa psykologiassa kertynyttä tietoa ihmisistä ja käyttäytymisestä soveltaa myös tietoturvaan. Cybersecurity for Psychology -hankkeessa on koottu materiaaleja psykologian aiheiden, psykologian alojen ja kyberturvallisuuden

teemojen mukaan. (CySec4Psych n.d.) Tiedon tai aikomuksen ja käytöksen välistä kuilua on tutkittu sosiaalipsykologiassa asenteisiin ja käyttäytymiseen vaikuttamiseksi, sekä terveystieteissä elintapojen muuttamiseksi.

Käyttäytyminen tarkoittaa päivittäisiä rutiineja, jotka ovat ihmisille juurtuneita tottumuksia, joita ihmiset tekevät automaattisesti ilman tietoista ajattelua. Myös ympäristö vaikuttaa rutiinien muodostumiseen. Käyttäytymiseen vaikuttavia monenlaisia tekijöitä kutsutaan determinanteiksi ja niihin kuuluvat muun muassa tiedot, taidot, asenteet, uskomukset ja sosiaaliset normit. Determinanttien ja niiden yhdistelmien vaikutusta käyttäytymiseen on selvitetty lukuisissa tutkimuksissa, joissa on syntynyt lähes sata käyttäytymistä selittävää teoriaa. Käytännöllisiä sovelluksia varten eri teorioista voidaan muodostaa yhteenvetoja. (Aittasalo 2024)

Näitä yhteenvetoja voidaan soveltaa myös tietoturvallisten käyttäytymismallien kehittämiseksi. Tietoturvatietoisuuden saralla sovellettuja yhteenvetomalleja ovat muun muassa Integrated Behavior Model ja COM-B, joista jälkimmäistä voi käyttää sellaisenaan tai eri yhteenvetoja yhdistelevissä viitemalleissa.

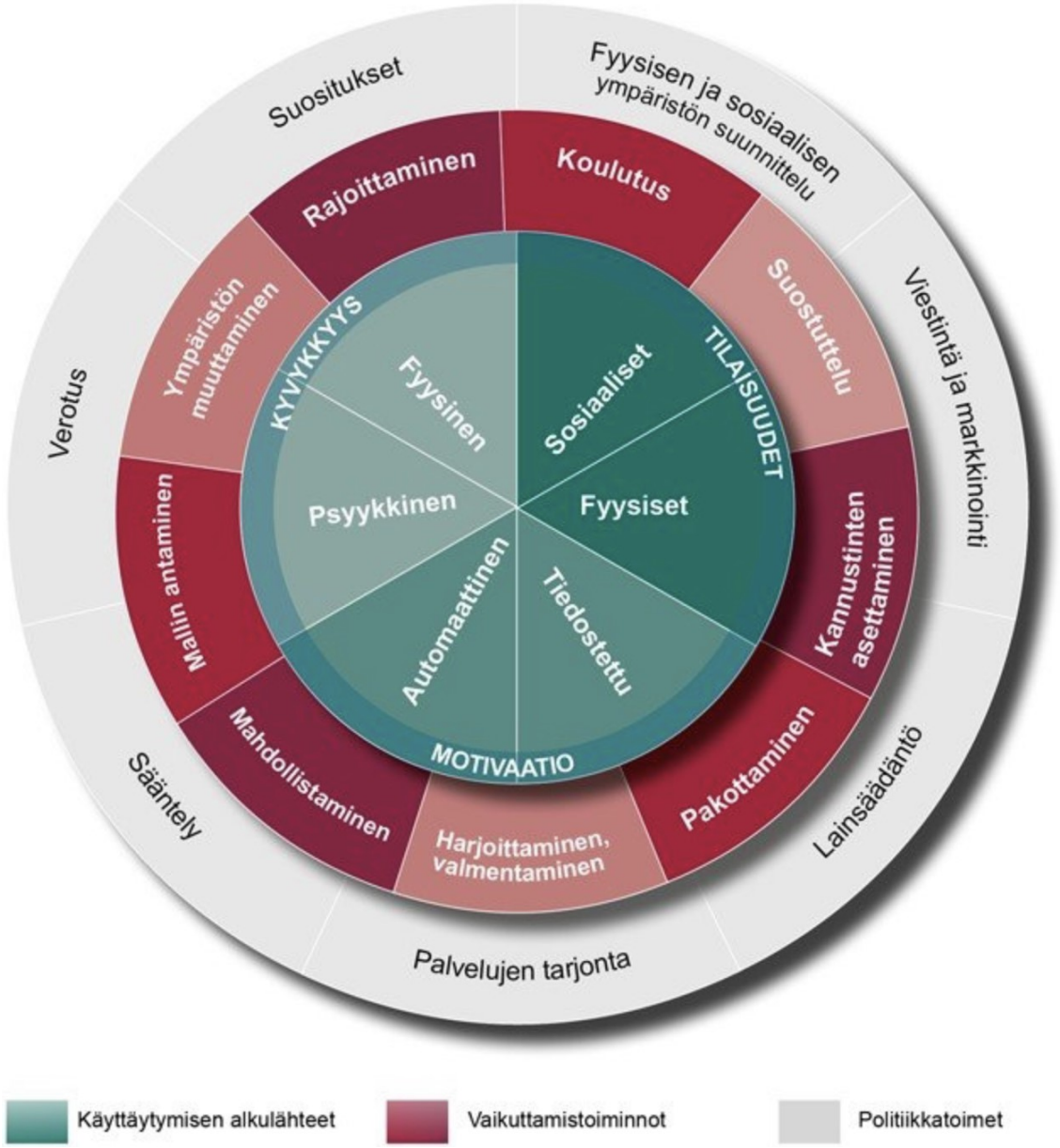
Michie ym. (2011) tutkivat 19:ää käyttäytymisen muutoksen interventioiden viitemallia yhteneväisyyksien ja eroavaisuuksien löytämiseksi, ja tiivistivät niiden yhtäläisyyksistä COM-B-mallin ja sitä tukevan käyttäytymisen muutospyörän (Behaviour Change Wheel). COM-B-malli käyttää Yhdysvaltain rikoslaissa syyllisyyden, eli käytännössä tahdonalaisen toiminnan, osoittamiseen tarvittavia komponentteja: kyvykkyys (capability), tilaisuus (opportunity) ja motivaatio (motivation). Kyvykkyys ja tilaisuus vaikuttavat motivaatioon, ja kaikki kolme komponenttia vaikuttavat käyttäytymiseen (behaviour), joka vaikuttaa myös komponentteihin (Kuvio 4).



Kuvio 4. COM-B-mallissa kyvykkyys ja tilaisuudet vaikuttavat motivaatioon ja käyttäytymiseen (Michie ym. 2011, Aittasalo 2024)

COM-B-malli on osa käyttäytymisen muutospyörää (Behaviour Change Wheel, Kuvio 5), jonka keskellä ovat käyttäytymisen kolme alkulähdettä (sources of behaviour) eli edellä mainitut komponentit: kyvykkyys, tilaisuudet, ja motivaatio. Pyörän keskimmäisellä kehällä kuvataan yhdeksän vaikuttamistoimintoa (intervention functions), jotka ovat keinoja käytöksen muuttamiseen. Uloimmalla kehällä ovat politiikkatoimet (policies), joilla ohjataan ja tuetaan vaikuttamistoimia.

Käyttäytymisen muutospyörän vaikuttamistoiminnot ovat suoraviivaisia ja helposti tietoturvaan sovellettavia. Myös politiikkatoimien soveltaminen onnistuu yliopistoissa niiden laajan toiminnan myötä, vaikkakin termistöä pitää lainsäädännön ja verotuksen osalta hieman muuttaa: lainsäädäntö vastaa yliopiston tietoturvapolitiikkaa ja heikomman tietoturvan ratkaisuihin tulee ”tietoturvavero” kompensoivien kontrollien myötä.



Kuvio 5. Käyttäytymisen muutospyörä (Michie ym. 2011; Aittasalo ym. 2017)

Kukin käyttäytymisen alkulähde voidaan jakaa vielä kahteen vaikuttimeen (Taulukko 4), joiden avulla voidaan tutkia tarkemmin minkälaiset asiat vaikuttavat kuhinkin alkulähteeseen. (Michie ym. 2011, 4)

COM-B-malli on riittävän yleinen, jotta sitä voi käyttää tietoturvatietoisuustoimien suunnittelussa, vaikka osa terveystieteistä johdetuista vaikuttimista ei täydellisesti sovellu tietoturvan pitkälti digitaaliseen käyttöön, kuten kyvykkyyden fyysinen vaikutin. Esimerkiksi psyykkinen kyvykkyys on taito tunnistaa huijaussäh-

köposti, fyysinen tilaisuus käyttää tietokoneen USB-porttia voi olla estetty ylläpidon toimesta, tiedostettu motivaatio on suhtautumista tietoturvaan, ja automaattinen motivaatio tapa tarkistaa sähköpostien vastaanottajat ennen lähettämistä tietovuotojen ehkäisemiseksi. (CySec4Psych 2023)

Taulukko 4. COM-B:n käyttäytymisen alkulähteiden vaikuttimet (Aittasalo ym. 2017).

Kyvykkyys	
Fyysinen	Fyysiset taidot, voima, kestävyys.
Psyykkinen	Tiedot tai psyykkiset taidot, vahvuus tai sinnikkyys toteuttaa tarvittavat henkiset prosessit.
Tilaisuus	
Fyysinen	Ympäristön tarjoamat tilaisuudet, kuten aika, resurssit, paikat, vihjeet ja fyysiset tarjoumat.
Sosiaalinen	Ihmisten väliseen vuorovaikutukseen perustuvat tilaisuudet, sosiaaliset vihjeet ja kulttuuriset normit siitä, miten asioista ajatellaan.
Motivaatio	
Tiedostettu	Harkinta, johon kuuluu tietoiset aikomukset ja seurausten punnitseminen (käsitykset siitä, mikä on hyväksi tai pahaksi).
Automaattinen	Automatisoituneet ja rutinoituneet tunnereaktiot, halut ja tarpeet, yllykkeet ja estot sekä refleksit.

Käyttäytymisen muutospyörää ja COM-B-mallia voidaan käyttää sellaisenaan, tai mallia voidaan soveltaa muihin teorioihin yhdistämällä, kuten Britannian National Protective Security Authorityn 5Es-viitemallissa ja Uuden-Seelannin CERT NZ:n Cyber Change -mallissa.

GÉANT:n Security Awareness Community Workshopin harjoitus on esimerkki suorasta käytöstä. Tietoturvallisemmalle käyttäytymiselle perustellaan alkulähteitä käyttäen, miksi käyttäytyminen on tarpeen (motivaatio), mitä taitoja käyt-

täytymiseen tarvitaan (kyvykkyys), sekä mitkä tilanteet ja välineet tukevat ja edistävät käyttäytymistä (tilaisuus). Samalla pitää miettiä käyttäytymisen muutospyörän vaikuttamistoimintojen ja politiikkatoimien tasolla mitä tavoitellaan, mikä on kohderyhmä, miksi käyttäytyminen on tärkeää, mitä hyötyjä käyttäytymisestä on kohderyhmälle ja mitä seuraamuksia on noudattamattomuudesta, mitä kanavia viestintään käytetään, mitä harjoittelua käytöksen oppimiseen, toistamiseen ja vahvistamiseen on tarjolla, sekä mitä välineitä ja prosesseja tarjotaan käyttäytymisen mahdollistamiseksi. (GÉANT 2024b, liite 3)

Britannian NPSA kehitti 5Es-viitemallin ihmisten turvallisuustietoisuuden ja sitä ylläpitävän työympäristön tukemiseksi. Malli pohjautuu COM-B-malliin, Protection Motivation -teoriaan, vaikutustutkimukseen sekä tutkimuksiin sosiaalisesta vetelehtimisestä, ja se soveltuu käytettäväksi niin fyysisessä kuin digitaalisessa ympäristössä. (NPSA 2023)

Kuvio 6: 5Es-viitemallin viisi periaatetta sekä tukeva elementti Endorsed by credible sources (NPSA 2023, 14).

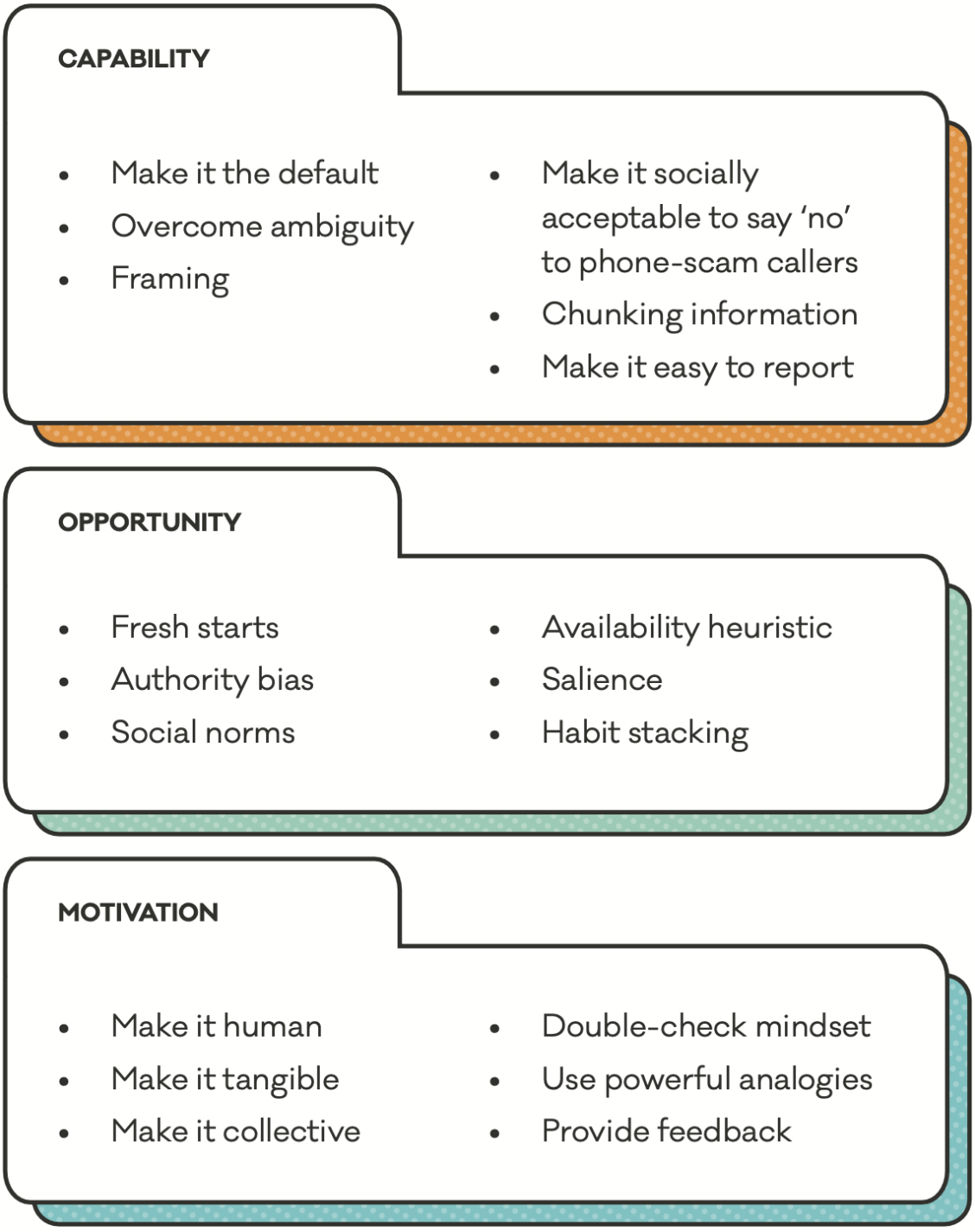
5Es koostuu viidestä periaatteesta sekä niitä tukevasta kuudennesta elementistä (Kuvio 6). Periaatteiden soveltamista varten organisaation pitää selvittää minkälaista käytöstä se odottaa työntekijöiltään, joka onnistuu miettimällä kysymyksiä: mitä pitää suojata, mitä turvallisuusuhkia organisaatiolla on, mikä on organisaation riskitaso, mikä on organisaation riskinottohalukkuus, ja minkä verran suojatoimia kannattaa käyttää. Pohdintojen myötä organisaatio voi päättää minkälaista käyttäytymistä henkilöstöltä tarvitaan täydentämään olemassa olevia fyysisiä, kyber- ja henkilöstötoimia. Näiden avulla organisaatio voi myös hallita ja suunnitella turvallisuutta strategisesta näkökulmasta ja kehittää siten turvallisuuskulttuuriaan. (NPSA 2023, 5)

5Es-mallin Educate why- ja Enable how -periaatteet ovat tärkeitä, koska työntekijöiden on tärkeä tietää ja ymmärtää miksi tietoturvakäytännöt ovat olemassa, ja minkälaiset konkreettiset seuraukset niiden laiminlyönnistä voi aiheutua. Heille on tärkeää näyttää ja opettaa oikeat tavat toimia heidän omissa töissään. (Vestman 2020, 142–143)

Uuden-Seelannin CERT NZ (2022) kehitti Cyber Change -ohjeistuksen, jotta kansalaisia saataisiin ”tönäistyä” toimimaan turvallisesti Internetissä. Ohjeistuksessa kerrotaan miten ihmisiä autetaan tekemään tietoturvallisten valintoja yhdistämällä tönäisyteoriaa COM-B-malliin. Tönäisyt (nudge) ovat vaikuttamista haluttuun käyttäytymiseen, joilla ihmiset ohjataan toimimaan halutusti.

Cyber Change -ohjeistuksessa on luotu 18 käytöksellistä oivallusta yhdistämällä COM-B-mallin käyttäytymisen alkulähteet tönäisyihin (Kuvio 7). Käytökselliset oivallukset koostuvat vakioasetuksista ohjeisiin, sanamuotoihin, visuaalisiin elementteihin, inhimillistämiseen ja palautteeseen. Ohjeistus opastaa tönäisyjen soveltamiseen viiden vaiheen kautta:

1. määrittele tavoite käyttäytymisen muutokselle,
2. tutki COM-B-mallia käyttäen muutoksen esteitä ja ajureita,
3. suunnittele mahdollisimman tehokas tönäisy,
4. testaa tehokkuus,
5. jalosta ja laajenna tönäisyjen käyttöä (CERT NZ 2022, 62–65).



Kuvio 7: Cyber Change -ohjeistuksen 18 käytöksellistä oivallusta, joita soveltamalla ihmiset toimivat turvallisemmin. (CERT NZ 2022, 20)

Tönäisyjä kannattaa käyttää erityisesti tietoturvallisten vaihtoehtojen esiintuonnissa oletusvalintoina tai muuten helpoimpina keinoina. Kun turvallinen tapa tehdä asia on oletuksena käytössä, poikkeaminen siitä vaatii enemmän vaivan-

näköä. Vakiovaihtoehdot ovat ihmisille helpompia myös sen takia, että niiden käyttäminen ei edellytä ohjeistuksiin perehtymistä. Tällaisessa tilanteessa Candrickin ym. (2023) havaitsema enemmistön poikkeaminen organisaation tietoturvaohjeistuksista ei olisi mahdollinen.

Ihmisten käytöstä ohjaa myös niin sanottu noudattamisbudjetti (compliance budget), jonka mukaan ihmiset budjetoivat rajallisia resurssejaan. Panostus tietoturvalliseen toimintaan kilpailee muiden resurssien kanssa, useimmiten ajan. Käytännössä noudattamisbudjetissa huomioidaan asioiden kulut ja hyödyt, niin itselle kuin organisaatiolle. Budjettia kuluttavia toimia ei välttämättä noudateta, ja hyödyttäviä toimia todennäköisemmin noudatetaan. Tämän takia tietoturvatietoisuusohjelman kaikessa toiminnassa pitää huomioida ihmisten motivointi tuomalla hyötyjä esiin selkeällä viestinnällä. (Winkler & Brown 2021, 68–69)

4.2 Positiivinen tietoturvakulttuuri

Ihmisten kouluttamisesta ja tietoisuudesta huolimatta tietoturvapoikkeamia tapahtuu teknologian ja prosessien kehittymisen, haavoittuvuuksien hyväksikäyttämisen, uusien rikostapojen, ja myös vahinkojen myötä. Varauduttujen uhkien lisäksi tulee uusia uhkia, joiden varalta ihmisiä ei ole voitu etukäteen kouluttaa toimimaan tietoturvallisella tavalla. Organisaation tietoturvakulttuuri tukee sen sietokykyä uusissa tilanteissa, joissa ihmiset joutuvat soveltamaan tietotaitoaan, ja joista organisaatio voi ottaa opiksi tulevaisuutta varten. (NCSC 2019)

Tietoturvakulttuuria voi olla vaikea hahmottaa ja se voidaan mieltää uudelleen nimetyksi tietoturvatietoisuudeksi. Carpenter & Roer (2022, 66) kuvaavat tietoturvakulttuuria yleisen kulttuurin määritelmän mukaisesti ihmisryhmän ideoiksi, tavoiksi ja sosiaalisiksi käytännöiksi, jotka vaikuttavat ryhmän tietoturvaan. Carpenter & Roer ovat kehittäneet myös tarkemman määritelmän, jossa on seitsemän sosiologiassa kuvattua toisistaan riippuvaista ja toisiinsa vaikuttavaa ulottuvuutta:

- Asenne (attitude): Suhtautuminen tietoturvaan ja miten ihmiset välittävät tietoturvasta.

- Käyttäytyminen (behavior): Mitä pidetään hyväksyttävänä käytöksenä ja miten muiden nähdään toimivan.
- Kognitio (cognition): Ihmisten osaaminen ja tietoisuus, ymmärrys tietoturvan tärkeydestä. Miten ihmiset oppivat ja miten tietotaitoa sovelletaan.
- Viestintä (communication): Miten tietoturvasta viestitään organisaatiossa.
- Noudattaminen (compliance): Miten ihmiset noudattavat sääntöjä ja politiikkoja.
- Normit (norms): Missä määrin tietoturvaan liittyvät uskomukset, käyttäytyminen ja arvot vaikuttavat epävirallisiin sääntöihin ja käytäntöihin.
- Vastuut (responsibilities): Missä määrin työntekijät voivat vaikuttaa tietoturvaan ja missä määrin he pitävät huolta, että kollegat noudattavat sääntöjä. (Carpenter & Roer 2022, 67)

Asenteella on tietoon verrattuna kaksinkertainen vaikutus tietoturvalliseen käytökseen (Vilander 2021, 69), joten organisaation kannattaa ylläpitää positiivista suhtautumista tietoturvaan. Tietoturvan tärkeyttä organisaatiolle pitää muistaa korostaa johdon toimesta. Samalla on hyvä tuoda esiin odotettuja tapoja toimia. Dialogi henkilöstön kanssa on tärkeä, jotta viralliset säännöt ja epäviralliset normit olisivat mahdollisimman lähellä toisiaan. Tämä helpottaa henkilöstöä sääntöjen mukaan toimimisessa. (Carpenter & Roer, 2022, 69–71)

Tietoturvakulttuuria voi lähestyä myös toimintakulttuurin ja psykologisen turvallisuuden kautta. Ilmailualalla poikkeamilla voi olla merkittäviä seurauksia ja poikkeamien juurisyyt pyritään selvittämään perinpohjaisesti, jotta ongelmat saataisiin vältettyä jatkossa kokonaan. Ongelmien ja vaaratilanteiden raportointi on kriittisen tärkeää. Tätä varten alalla pyritään luomaan ja ylläpitämään oikeudenmukaista toimintakulttuuria (just culture), jossa ihmisiä ei rangaista suunnittelemattomista tai tahattomista toimista, laiminlyönneistä tai päätöksistä, jotka ovat näiden henkilöiden kokemuksen ja koulutuksen kannalta oikeasuhteisia. Oikeudenmukaisessa toimintakulttuurissa ei kuitenkaan suvaita törkeää huolimattomuutta, tahallisia rikkomuksia ja vahingollisia toimia. Just culture sisältää myös luottamuksellisen ilmapiirin, jossa ihmiset voivat tuoda esiin turvallisuuteen liittyviä asioita tietäen, että ne käsitellään ja huomioidaan oikeudenmukaisesti. (Traficom 2022)

Ilmailualaa koskeva raportointivelvoite tulee Euroopan unionin poikkeama-asetuksesta (Euroopan parlamentin ja neuvoston asetus 2014/376). Myös kyberturvallisuuden

vallisuuteen on NIS2-direktiivin myötä tullut vastaava raportointivelvoite. Vaikka NIS2-vaatimuksia Suomessa toimeenpaneva kyberturvallisuuslaki ei koske korkeakouluja, luottamuksellinen turvallisuuskulttuuri mahdollistaa laadukkaan ja kattavan turvallisuustiedon saamista organisaation sisältä (Traficom 2022). Positiivinen tietoturvakulttuuri antaa ihmisille luottamusta siihen, että heidän kannattaa tuoda asioita esille ja parantaa organisaation toimintaa, luottaen reiluun ja oikeudenmukaiseen käsittelyyn. Ihmiset ovat tällöin vapautuneita keskittymään organisaation etuihin oman selustansa suojaamisen sijaan. Raportoituja poikkeamia tutkittaessa pitää huomioida miten organisaatiossa normaalisti toimitaan ja tehdään päätöksiä, ja minkälaisilla tiedoilla. Tutkinnassa pitää huomioida tilanne ja käytettävissä ollut tieto, jotta saadaan selville mikä oikeasti meni pieleen, ja mitä parantamalla vastaavia tilanteita voidaan ehkäistä. (NCSC 2019)

Ihmisille on kuvattava ja viestittävä miten heidän ilmoittamiaan poikkeamia käsitellään ja minkälaisilla reunaehdoilla päätöksiä tehdään, jotta kaikilla on yhdenmukainen kuva oikeudenmukaisesta toiminnasta. (Traficom 2022)

Tärkeä osa positiivista tietoturvakulttuuria on, että tietoturvasäännöt ja -käytännöt sopivat organisaation todellisiin työskentelytapoihin (NCSC 2019). Uhilla ja sanktioilla pelottelu voi etäännyttää ihmisiä, joten viestinnässä on keskityttävä positiivisiin viesteihin siitä, miten ihmiset voivat auttaa (NCSC 2021). Ihmiset voivat noudattaa hankalia käytäntöjä hyväntahtoisuuttaan, mutta noudattamisbudjetin loppuessa ihmiset alkavat kiertää sääntöjä, luovat varjoratkaisuja tehdäkseen töitään, tai suhtautuvat negatiivisesti organisaation kulttuuriin. (NCSC 2019; Beyer ym. 2015, 9). Tietoturvakäytännöt on voitu kehittää ilman ymmärrystä organisaation päivittäisestä toiminnasta, tai ne ovat voineet jääneet jälkeen kehityksessä (NCSC 2019). Jotta tietoturvan huomiointi ei jäisi varsinaisten töiden jalkoihin, työtapoja pitäisi kehittää organisaation riskinottohalukkuuteen sopivaksi. Se voi käytännössä tarkoittaa korkeampaa riskiä, kunnes käyttöön saadaan tietoturvallisempi ratkaisu. Joka tapauksessa organisaation pitää kantaa vastuu tilanteessa (NCSC 2017).

Esimerkiksi pilvipalveluna käytetty tiedostojen verkkotallennustila voi edellyttää tietyn luokittelutason tiedostojen salausta erillisellä sovelluksella ennen tallentamista. Tietoturvallinen toimintatapa hidastaa työskentelyä, ja virheellisestä käytöstä rangaistaan (Beyer ym. 2015, 9). Jos ihmiset pelkäävät rangaistuksia tietoturvaan liittyen, he eivät uskalla tuoda esiin ongelmia ja piilottelevat oikaisujaan ja kiertoteitään (NCSC 2017). Tietoturvan kannalta parempi ratkaisu olisi käyttää verkkotallennustilaa, joka ei edellyttäisi erillisen salaussovelluksen käyttöä, jolloin ihmiset eivät voisi toimia väärin. Tällöin tietoturva tukee ihmisten työskentelyä eivätkä ihmiset koe tietoturvan olevan jotain, joka toimii heitä vastaan (NCSC 2017).

Ihmisiä ei pidä syyttää virheistä, vaan poikkeamia pitää pyrkiä käyttämään käsittelemään poikkeamaa parantamismahdollisuutena niin sen osapuolille kuin organisaatiolle. Ihmisille kannattaa antaa mahdollisuus vastuunsa kantamiseen ja heidät kannattaa ottaa mukaan vahinkojen korjaamiseen, jolloin todennäköisyys poikkeamalle laskee. Reilu käsittely ja poikkeaman käyttäminen kehittämismahdollisuutena luo luottamusta ja lisää halukkuutta auttamiseen. (NCSC 2019)

Tietoturvakulttuurin kehittyminen ottaa oman aikansa, eikä sitä todennäköisesti saavuteta pelkillä kirjallisilla ohjeilla tai koulutustapahtumilla (NCSC 2024b). Isommissa organisaatioissa voi, korkeakoulujen tapaan, olla monia erilaisia toimintakulttuureja rinnakkain eri yksiköissä. Tämä vaikeuttaa tietoturvasta viestimistä, koska kaikki eivät koskaan ymmärrä viestiä samalla tavalla. Jotta pysyvää kulttuurillista muutosta saataisiin aikaan, pitää perehtyä siihen, miten ihmiset työskentelevät päivittäin, olla vuoropuhelussa ja kuunnella tarpeita, ja ohjata toimintaa tietoturvallisempaan suuntaan. (NCSC 2017)

4.3 Tietoturvatietoisuuden ja tietoturvakulttuurin kypsyysmalleja

Tietoturvatietoisuuden kehittämistoimien kypsyyden mittaamiseen on kehitetty erilaisia malleja. Kypsyysmalleilla pyritään hahmottamaan organisaatioiden tietoisuusohjelmien nykytilaa. Osa kypsyysmalleista auttaa myös toiminnan kehit-

tämisessä antamalla konkreettisia esimerkkejä seuraavalle tasolle pääsemiseen vaadituista toimista.

Britannian NCSC:n Cyber Assessment Framework kuvaa tietoturvakulttuurille ja tietoturvakoulutuksille kolmitasoiset kypsyysmallit (liite 2), joissa annetaan esimerkkejä ominaispiirteistä kullekin tasolle: ei-saavutettu, osin saavutettu, saavutettu. CAF ei kuitenkaan ohjeista miten asioita pitäisi toteuttaa, vaan se kuvaa lopputuloksia. (NCSC 2024a)

Tietoturvakoulutuksia tarjoavan SANS:n Security Awareness Maturity Model on viisitasoinen kypsyysmalli (Taulukko 5), joka kuvaa tietoisuusohjelman ja ihmisten toimintaa, kunkin tason saavuttamiseen tarvittavaa aikaa, mittaustapoja ja seuraavalle tasolle tarvittavia toimia. Liitteen 4 taulukko luonnehtii yksityiskohtaisesti eri tasoilta odotettavia ominaisuuksia tietoisuusohjelman suunnitelmallisuuden, henkilöstöresursoinnin, organisaatioon sijoittumisen, johdon tuen, yksiköiden välisen yhteistyön, viestinnän ja mittaamisen osalta. (SANS 2025)

Taulukko 5. Tiivistelmä SANS Security Awareness Maturity Modelin kypsyystasoista. (SANS 2025)

Kypsyystaso	Kuvaus
Taso 1	Tietoturvatietoisuusohjelmaa ei ole, eikä organisaatio täytä sille asetettuja vaatimuksia ja ihmiset aihettavat poikkeamia.
Taso 2	Tietoturvatietoisuusohjelma on ensisijaisesti vaatimustenmukaisuutta varten, jonka myötä tietoturvakoulutusta annetaan vain vuosittain tai satunnaisesti. Vaikka ohjelma täyttää asetetut vaatimukset, organisaatio ei silti hallitse ihmisiin liittyviä riskejä. Tämä taso voi olla kaikkein vaarallisin, jos organisaation johto on siinä uskossa, että riskejä käytännössä hallitaan, vaikka niitä ei oikeasti hallita.
Taso 3	Organisaatiossa on tunnistettu tärkeimmät ihmislähtöiset riskit ja niitä hallitaan. Koulutus menee vuosittaista pidemmälle ja oppia vahvistetaan läpi vuoden. Kypsemmissä organisaatioissa tunnistetaan kohdennettua koulutusta tarvitsevia rooleja. Positiivisella viestinnällä tavoitellaan muutosta käyttäytymiseen.
Taso 4	Organisaatiossa kehitetään tietoturvakulttuuria ja ohjelma on resursoitu riittävästi pitkän aikavälin kehittämiseen johdon tuella.
Taso 5	Ohjelman vaikuttavuutta mitataan toimintaan liittyvillä mittareilla, joilla seurataan organisaation riskien vähenemistä ja tavoitteiden saavuttamista.

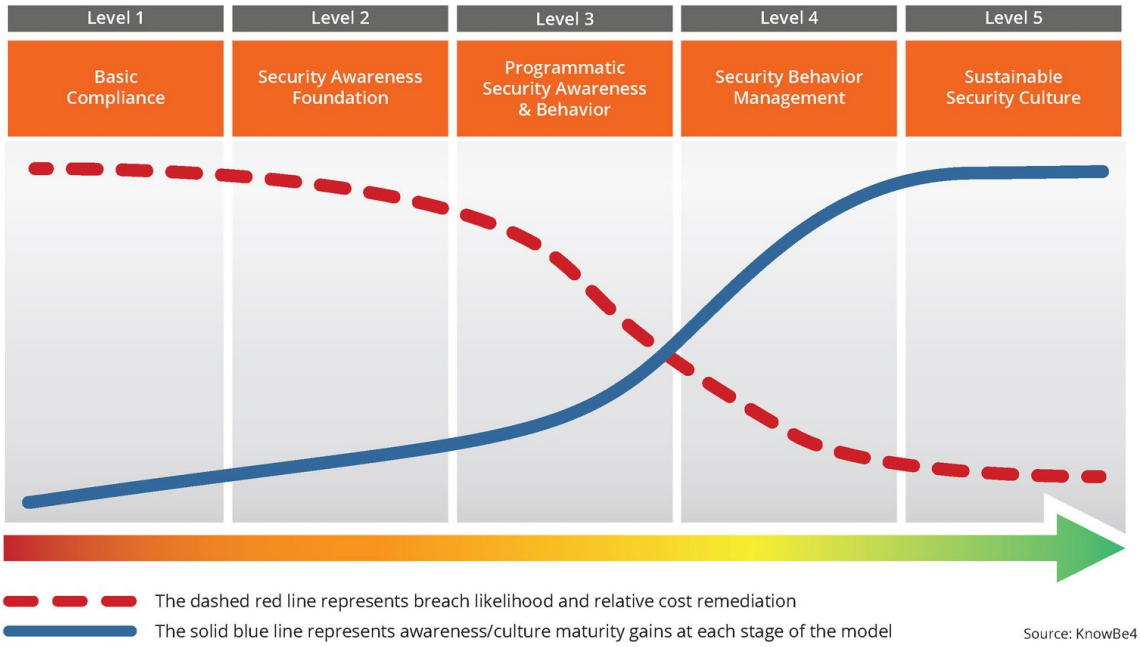
Carpenterin & Roerin (2022, 161) Security Culture Maturity Model pohjautuu heidän työhönsä KnowBe4:lla, joka tarjoaa ensisijaisesti tietoturvakoulutusta simuloiduilla kalasteluviesteillä. Heidänkin mallissaan on viisi tasoa (Taulukko 6), mutta tason 1 vaatimuksenmukaisuuden tavoittelu vastaa SANS:n tasoa 2.

Taulukko 6. Security Culture Maturity Modelin kypsyystasojen kuvaukset. (KnowBe4 n.d.)

Kypsyystaso	Kuvaus
Taso 1	Basic Compliance • Bare minimum of training • Limited metrics • “Check the box”
Taso 2	Security Awareness Foundation • At least annual and onboarding training • Occasional phishing simulations • Focus on variety of content
Taso 3	Programmatic Security Awareness & Behavior • Intentional awareness program with integrated tools • Quarterly training with simulated phishing • Focus on security-aware behaviors
Taso 4	Security Behavior Management • Continuous training across varied delivery methods and audiences • Heavy use of integrated tools to inform training strategy • Program focused on real behavior change
Taso 5	Sustainable Security Culture • Program that intentionally measures, shapes and reinforces security culture • Multiple methods of behavior-based encouragement • Security values woven through fabric of entire organization

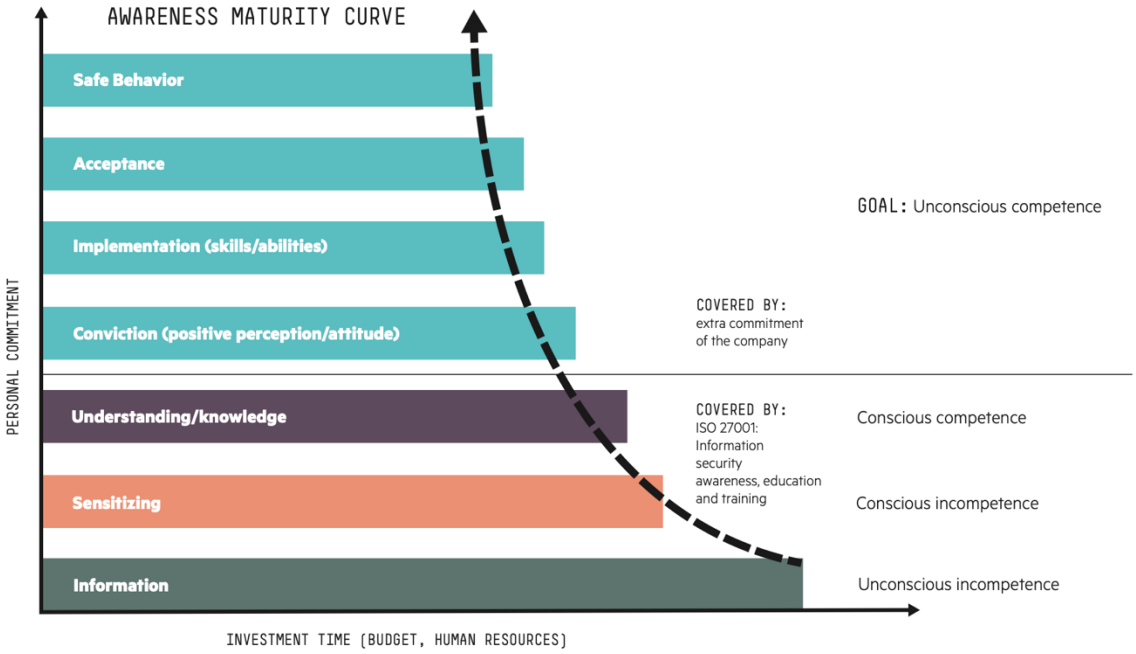
Security Culture Maturity Modelissa näkyy KnowBe4:n vaikutus tietoturvatietoisuuden toteuttamisen teknisenä runkona, joka alkaa tasolla 2 kalastelusimulaatioharjoituksista ja etenee teknisten työkalujen laajemman käytön myötä automaattisempaan ja useammin tehtävään toteutukseen. Työkalujen käyttö helpottaa toimien toteuttamista sekä vaikutuksen mittaamista ja raportointia, varsinkin isommissa organisaatioissa.

Carpenter & Roer (2022, 161) ovat KnowBe4:n dataan pohjautuen mallintaneet Security Culture Maturity Modeliin S-käyrät (Kuvio 8) kuvaamaan tietomurtojen todennäköisyyttä ja niistä toipumisen kustannusta, sekä tietoturvatietoisuuden ja tietoturvakulttuurin kasvua kullakin kypsyystasolla. Kaavion perusteella ihmisten käyttäytymiseen keskittyvät toimet alkavat merkittävästi laskemaan tietomurtojen riskiä ja vakavuutta tason 3 muutosta tavoittelevilla toimilla. Tasolta 3 alkaen ihmisten tietoisuuden ja taitojen karttuminen on pysyvämpää.



Kuvio 8. Security Culture Maturity Modelin S-käyrät (KnowBe4 n.d.; Carpenter & Roer 2022, 161).

Beyer ym. (2015, 6) kehittivät tietoturvatietoisuustoimien kypsyyskäyrän (Kuvio 9), joka kuvaa alhaalta alkaen, miten ihmisten tietoturvatietoisuuden ja tietoturvallisen käyttäytymisen kehittämiseen tarvitaan useita eri vaiheita. Kaavion alaosan koulutustoimilla saavutettavat tietoisesti käytettävät taidot riittävät ISO/IEC 27001 -standardin kaltaisten vaatimusten täyttämiseen, mutta usein organisaatioissa ei ymmärretä yläosassa kuvattujen jatkotoimien tarpeellisuutta, jotta tietoturvatietoisuustoimista tulisi tehokkaita.



Kuvio 9. Hewlett Packard Enterprise Awareness Maturity Curve (Beyer ym. 2015, 6)

Alimmat Information- ja Sensitizing-vaiheet kattavat järjestelmällistä viestintää useita kanavia hyödyntäen. Understanding- ja Conviction-vaiheissa organisaation johdon osallistuminen on tärkeää, jotta johto viestii yhdenmukaisesti tietoturvasta ja näyttää esimerkkiä. Implementation-vaiheessa kehitetään työntekijöiden henkilökohtaista vastuuta tietoturvasta. Sekä Acceptance- että Safe Behavior -vaiheet ovat riippuvaisia työntekijöiden sitoutumisesta tietoturvaan ja sen harjoitteluun. Näissä tutkitaan dokumenttien sijaan tietoturvan toteutumista käytän-nössä ja tarvittavia kehityskohteita. (Beyer ym. 2015, 6–7)

SANS:n (2025) kypsyysmallin tasokuvauksia (liite 4, Taulukko 10) apuna käyttäen kuka tahansa pystyy oman organisaation kypsyystason määrittämiseen ja samalla katsomaan millä toimilla päästään seuraavalle tasolle. Myös CAF on käytännöllinen tietoturvakulttuurin ja tietoturvakoulutusten tason arviointiin, mutta konkreettiset ohjeet tekemiseen kannattaa katsoa muista viite- tai kypsyysmalleista. Carpenter & Roerin (2022) Security Culture Maturity Model on toistaiseksi vain KnowBe4:n asiakkaiden käytettävissä, koska arvion tekemiseen tarvittavia CMI-tietoja ei ole saatavilla avoimesti (KnowBe4 n.d.).

Korkeakouluille esitetyt vuosittaiset tietoturvakoulutukset ja tietoturvatestit jäävät kaikissa esitellyissä kypsyysmalleissa perustasolle, jolla saavutetaan vaatimustenmukaisuus checbox-tyyliin. Carpenterin ja Roerin (2022) Security Culture Maturity Modelin mukaan tiedon tankkaaminen koulutuksilla ja tietoisuustoimilla tasoilla 1 ja 2 ei vielä merkittävästi vaikuta organisaation tietoturvariskeihin. Korkeakoulujen johdon onkin tärkeä tunnistaa SANS:n varoitus siitä, että alimmilla kypsyystasoilla ihmisiin liittyviä riskejä ei vielä hallita järjestelmällisesti, vaikka jotain tehdäänkin, ja toimintaa pitää laajentaa ja kehittää riskitason vähentämiseksi (SANS 2025). Jos tietoturvan suojakeinot eivät tuo oikeata suojaa, ne saattavat jäädä tietoturvateatteriksi – keinoiksi, jotka näennäisesti suojaavat uhalta, mutta oikeasti tuovat vain tietoturvallisuuden tunnetta (Schneier 2003, 38). Mikäli suojakeinot antavat virheellisen kuvan tietoturvan tilasta, ne voivat olla myös vaaraksi.

4.4 Ihmiskeskeisen tietoturvan mittaaminen

Tietoturvakoulutuksia, -testejä ja -tietoisuustoimia käytetään mittareina erilaisista syistä: tekemisen ja kehityksen osoittamiseen johdolle (Hielscher ym. 2023, 2317), tavoitteiden seuraamiseen (SANS 2025), tiedolla johtamiseen, osaamisen tarkistamiseen, koulutustarpeiden ja tietoisuuden tilanteen selvittämiseen. Yksinkertaisimmillaan mittarit osoittavat tietoturvakoulutuksien olemassaolon ja niihin osallistumista. Suurimmalla osalla tietoisuusohjelman tavoitteena on saada aikaan mitattavaa muutosta työntekijöiden käytöksessä, mutta vain alle puolet organisaatioista mittaa johdonmukaisesti työntekijöiden käytöstä (Candrick ym. 2023).

Luvun 3 yliopistoja koskevat vaatimukset eivät edellytä mittaamista, mutta viitemalleissa edellytetään osaamisen arviointia (Taulukko 3). Viitemallit eivät mene yksityiskohtiin ja yleisesti tarkoituksena on SP 800-53:n tapaan edellyttää käytännön harjoituksia työntekijöille (AT-3(3)), joiden tulokset raportoidaan esihenkilöille (AT-6), jotta epäonnistumisiin voidaan tarvittaessa puuttua (NIST SP 800-53 Rev. 5.). Kybermittarin WORKFORCE 4e ehdottaa koulutustoiminnan arviointiin testausta koulutuksien yhteydessä, sekä kyselyillä koulutuksen jäl-

keen, niin koulutukseen osallistuneilta henkilöiltä, kuin heidän esihenkilöiltään palautteeksi koulutuksen vaikutuksesta työntekijöiden osaamiseen (Kybermittari-arviointityökalu 2.1).

ISO/IEC 27001 -standardin edellistä 2013-versiota vasten tehdyn ISO/IEC 27004:2016: Tietoturvallisuuden hallintajärjestelmien seuranta, mittaus, analysointi ja arviointi -standardin kohta 7.2 auttaa tietoturvan hallintajärjestelmän hallintakeinojen kattavuuden mittaamisessa. Kohdassa 7.3 opastetaan vaikuttavuuden mittaamiseen eli toimivatko hallintajärjestelmä ja hallintakeinot kuten pitäisi, ja saadaanko niillä toivottuja tuloksia. Standardi tuo esiin, että mittaaminen ei ole yksinkertaista, vaan vaatii useita datapisteitä kuten koulutuksen sisältöön liittyvän testin tulosten lisäksi aiheeseen liittyvien poikkeamien tutkimisen ja tukipyyntöjen määrät. (ISO/IEC 27004:2016)

Standardin liitteen esimerkit kertovat pääosin osallistumismääristä, koulutuksen jälkeisen tietämyksen mittaamisesta, sosiaalisen manipuloinnin tunnistamisesta eli kalastelusimulaatioiden tuloksista (avasivat linkin, raportoivat viestin asianmukaisesti, haksahtivat antamaan tietonsa kalastelulinkissä), sekä salasanojen laadusta (ISO/IEC 27004:2016). Standardin esimerkkejä ei kannata käyttää nykytiedon valossa. Kalastelusimulaatioiden käyttö ei välttämättä anna oikeaa kuvaa ihmisten tietoturvaosaamisesta (Ho ym. 2025; Winkler & Brown 2021, 241) ja ne nakertavat positiiviseen tietoturvakulttuuriin tarvittavaa luottamusta (NCSC 2018), joten kalastelusimulaatioita ei kannata välttämättä käyttää mittaamiseen. Salasanojen merkitys on laskenut kertakirjautumisen ja MFA:n käytön laajentumisen myötä (Weinert 2019), ja yleisesti salasanakäytäntöjä ohjaava NIST:n ohjeistus on löysäämässä suositeltuja salasanakriteerejä (NIST SP 800-63B Second Public Draft of Revision 4).

SANS:n Security Awareness Maturity Modelin (liite 4, Taulukko 10) toisella tasolla mitataan koulutuksiin osallistumista, koulutus- ja tietoisuustapahtumien määrää ja tiheyttä, joilla pystytään osoittamaan vaatimusten täyttämistä. Tietoisuutta ja käyttäytymisen muutosta edistävällä tasolla 3 mukaan tulee ihmisiin liittyvien tietoturvariskien kannalta tärkeiden turvallisuutta parantavien asioiden seuraaminen, kuten MFA:n ja salasanasäilöjen käyttöasteet, ja erilaisten ihmi-

sistä johtuvien poikkeamien määrät. Kulttuurimuutoksen tasolla 4 mittarit sisältävät kyselyjä ihmisten tietoturvaan liittyvistä asenteista, mielikuvista ja uskomuksista, pyyntöjä tietoturvan tiedotustilaisuuksiin, tietoturvasta kysyvien tai parannuksia ehdottavien ihmisten määrä. Korkein taso 5 on nimetty strategisten mittareiden mukaan, jotka kertovat toimien vaikutuksesta tietoturvariskien kehittymiseen, kuten poikkeamien määriin, hyökkäysten havaitsemis- ja toipumisaikoihin, sekä käytäntöjen rikkomusten määriin. (SANS 2025)

Security Culture Maturity Modelin indikaattorit (liite 5, Taulukko 11) mittaavat organisaation toimintaa monelta suunnalta, mutta organisaation sijaan suoraan ihmisiin liittyvät mittarit pohjautuvat pääosin kalastelusimulaatioista saatavaan dataan ja kyselyihin (Carpenter & Roer 2022).

Security Culture Survey mittaa organisaation tietoturvakulttuurin nykytilaa ja kehittämistarpeita luvussa 4.2 kuvattujen tietoturvakulttuurin seitsemän ulottuvuuden kautta (Carpenter & Roer 2022, 67). Käytännössä tutkimuksen kysymyksillä selvitetään tietoturvariskien kannalta kiinnostavia asioita ulottuvuuksien kautta. Jotta tietoturvakulttuurista saadaan todellinen kuva, on kriittistä saada mahdollisimman rehellisiä vastauksia. Tästä syystä ihmisiltä ei kysytä heistä itsestään ja heidän tekemisistään, koska he saattavat vastata omia tuloksia kaunistelevalla tavalla. Sen sijaan kannattaa kysyä kollegoiden tekemisistä, tai mitkä ovat organisaation yleisiä tapoja ja arvoja. Kun kysely tehdään henkilötasolla, esiin voi tulla henkilöitä ja ryhmiä, jotka toimivat väärin tai kaipaavat enemmän tietoa. Vastaavasti esiin voi myös tulla hyvin toimivia yksilöitä ja ryhmiä, joiden toimintaa kannattaa vahvistaa ja juhlistaa. (Carpenter & Roer 2022, 71)

Ihmisten tietoturvatietoisuuden arviointiin on kehitetty KAB-malliin pohjautuva HAIS-Q-kyselylomake (Human Aspects of Information Security Questionnaire), jolla kysytään tietoturva-aiheista tietämyksen, suhtautumisen ja käyttäytymisen kannalta (Parsons ym. 2014). Alkuperäisessä HAIS-Q-lomakkeessa on yhteensä 63 kysymystä seitsemältä aihealueelta (Parsons ym. 2017), mutta kyselylomake kannattaa muokata kohdeorganisaation tarpeiden mukaan. Voitaneen olettaa, että kaikki eivät uskalla tai halua vastata rehellisesti kyselyyn, varsinkaan jos positiivinen tietoturvakulttuuri ja oikeudenmukainen toimintakulttuuri ei-

vät ole vielä juurtuneet organisaatioon. Tällöin tulokset saattavat antaa väärän kuvan tietoturvasta.

Kyselyjä tietoturvan sopimisesta työpäivään voi tehdä myös suoraan henkilöstölle haastattelujen ja kyselyjen muodossa. Saatu palaute tuo esiin turvatonta käyttäytymistä ja mahdollistaa tietoturvakäytäntöjen ja -koulutusten kehittämisen niiden muuttamiseksi. Samalla saadaan kuva siitä, miten tietoturva kytkeytyy henkilöstön työrutiineihin. (Beyer ym. 2015, 9)

Mittaamisessa on tärkeää kerätä dataa jatkuvasti ja vertailukelpoisesti kehittymisen seuraamiseksi pitkällä aikavälillä. Mittarit kannattaa valita tukemaan organisaation tietoturvatavoitteiden saavuttamista. Tietoturvan kehittyminen vie aikansa, joten seurantaa kannattaa tehdä useamman vuoden jänteellä. Mittarit on hyvä suunnitella etukäteen myös tietosuojan kannalta, jotta henkilödata kerätään vain tarpeellinen määrä. Osa mittareista voi toimia myös anonyymeinä yksikön tasolla. Tulokset kannattaa säilyttää sellaisessa tietojärjestelmässä, joka mahdollistaa pitkän aikavälin seurannan, eikä tyhjennä tuloksia esimerkiksi koulutusmateriaalin muokkauksen yhteydessä.

Jos osaamista mitataan testillä joko tietoturvakoulutuksen yhteydessä tai erillisellä tietoturvatestillä, testiä ei pidä toteuttaa niin, että käyttäjälle näytetään väärin vastattuihin kysymyksiin oikeat vastaukset, joiden avulla vastaamalla testistä pääsee läpi. Virheellisestä vastauksesta voi kertoa oikean vastauksen, mutta ensimmäisen kerran tuloksista on pidettävä kirjaa, jotta suoritusten tuloksista saadaan mitattavaa dataa, jota voidaan käyttää koulutusten ja tietoisuuden kehittämiseen. Jos tulos ei oikeuta läpipääsyyn, uusinta voi edellyttää uutta yritystä myöhemmin, tai koulutustilaisuuteen osallistumista paremman oppimisen vuoksi.

5 Tietoturvakouluttamisesta yliopistoissa

Tietoturvakoulutusten, tietoturvatietoisuuden ja tietoturvakulttuurin kehittämisessä on huomioitava yliopistojen ainutlaatuisuus yhteisöinä ja ympäristöinä. Yliopistoihin ei voi sovittaa vain yhtä tietoturvakoulutusta tai -testiä, koska niissä työskentelee ja opiskelee erilaisia ihmisiä, erilaisissa rooleissa, ja ihmisten vaihtuvuus on suurta opiskelijoiden aloittaessa, valmistuessa sekä henkilökunnan pätkätöissä.

Yliopistot toimivat myös avoimesti ja verkottuneesti tehden laajaa yhteistyötä kaikenlaisten organisaatioiden kanssa, joka tarkoittaa laajoja verkostoja, avointa suhtautumista uuden teknologian kokeilemiseen ja käyttämiseen. Tietoturvariskejä ei voida tällöin hallita samaan tapaan kuin yritysten kaltaisissa suljetuissa ympäristöissä.

Erilaisille kohderyhmille sovitettu koulutus kattaa vaatimuksen roolipohjaisesta koulutuksesta ja samalla motivoi ihmisiä, kun he saavat heille tarpeellista tietoa. Monimuotoisuus vaikuttaa myös tietoturvakoulutusten pakollisuuden suunnitteluun. Kaikki eivät ole samanlaisessa asemassa, jolloin yhtä käytäntöä on hankala sovittaa koko yliopistoyhteisöön niin, että kaikki olisivat tyytyväisiä.

Korkeakouluyhteisöt ovat vahvasti verkottuneet, joka mahdollistaa tutkimusten tekemisen ja opintojen suorittamisen yli organisaatiorajojen. Yhdessä korkeakoulussa suoritetun tietoturvakoulutuksen hyväksiluvulla vastaavaa koulutusta ei tarvitsisi suorittaa muissa korkeakouluissa, joka helpottaisi ihmisten elämää ja loisi luottamusta muiden korkeakoulujen tietojärjestelmien käytölle. Tietoturvakoulutuksiin ja -testeihin liittyvät käytännöt vaihtelevat kuitenkin paljon yliopistojen välillä (Gynther 2023).

Tässä luvussa esiin tuotuja asioita huomioimalla yliopistot voivat vähentää tietoturvariskejään sekä kehittää tietoturvakoulutuksiaan kohti yhtenäisiä ja suositusten mukaisia parhaita käytäntöjä.

5.1 Tietoturva rakentuu ihmisten, prosessien ja teknologian varaan

Tietoturvan – monen muun asian tavoin – voi sanoa rakentuvan ihmisten, prosessien ja teknologian varaan, ja niiden väliseen sopivaan tasapainoon. Teknologia on tietokoneita, tietojärjestelmiä, tietoverkkoja ja dataa. Prosessit tiedon käsittelyä, teknisesti tai muilla tavoin. Ihmiset ovat tietoa käsitteleviä, tietokoneiden ja -järjestelmien käyttäjiä. Käytännössä riskejä tietoturvalle muodostuu ihmisten, prosessien ja teknologioiden suhteen epätasapainosta.

Ihmisistä puhutaan monesti tietoturvan heikoimpana lenkkinä, vaikka ihminen on olennainen ja tarpeellinen osa kokonaisuuden toiminnassa (Vilander 2021, 79). Ihminen on myös usein hyökkäyksen kohde samalla, kun se on tietoturvan eteen toimiva taho. Kun ihmisen sanotaan olevan heikoin lenkki, ihminen on tyypillisesti kuormitetuin lenkki paikatessaan muiden osa-alueiden puutteita, esimerkiksi liian vähäisiä tai vääränlaisia panostuksia teknologiaan (Hielscher ym. 2023). Tällöin yksittäisen ihmisen tiedoilla, taidoilla, valinnoilla, keskittymisellä ja jaksamisella on vaarallisen suuri vaikutus tietoturvaan. Kuormituksen vähentämiseksi organisaatioiden kannattaa riskienhallinnassaan selvittää mahdollisuus riskien välttämiseen kokonaan, tai riskien mitigointiin tietoturvakontrolleilla teknisesti tai prosesseissa (Winkler & Brown 2021, 66).

Mielikuva ihmisistä heikoimpana lenkkinä voi syntyä myös, jos teknologian tietoturvallisuudesta on liian positiivinen mielikuva ja siihen uskotaan katteettomasti. Kun käytetyn teknologian puutteita, haavoittuvuuksia, ja myös mahdollisuuksia, ei tunneta, tietoturvaongelmat voivat näyttäytyä ihmisistä johtuvina. Organisaatio voi kuvitella käyttävänsä maailman parhaita tietoturvaratkaisuja, ja silti syyttää korttitalonsa tietoturvan olevan ihmisen yhden väärän klikkauksen tai huolimattomuuden varassa.

Niin sanotut turvakaiteet suojaavat ihmisten taitamattomuudelta, tai rajoittavat virheiden vaikuttavuutta. Parhaassa tapauksessa ihmisten osuus saadaan poistettua kokonaan, esimerkiksi automaatiolla tai tekoälyllä, jolloin ihmiset eivät voi tehdä organisaatiota haittaavia virhettä, eikä heitä tällöin tarvitse edes kouluttaa toimimaan asiassa tietoturvallisella tavalla (Venables 2024). Turvakaiteet voi-

daan kuitenkin suunnitella vain tunnettujen riskien varalta, eivätkä ne suojaa uudenlaisilta uhilta. Näiden varalta tarvitaan ihmisten kouluttamista, jotta myös uusien ongelmien kanssa osataan toimia oikein (Beyer ym. 2015, 8).

Organisaation prosessien, teknologioiden, ja ihmisten osaamisen nykytila pitää selvittää, jotta tarvittavat kehitystä tehdään tietoturvan kannalta tärkeimpiin osaalueisiin. Selvitystyö kannattaa aloittaa organisaation tietoturvatason, suojausten ja haavoittuvuuksien, sekä uhkien nykytilan kartoituksella, jonka pohjalta voidaan luoda kehityssuunnitelma tietoturvan konkreettiseen parantamiseen sekä teknisten suojausten ja turvakaiteiden käyttöönottoon. Tässä tehokkainta on tehdä tunkeutumistestaus, jossa hyökkääjän tavoitteita ja toimia simuloiden koetellaan organisaation olemassa olevien tietoturvakontrollien (ihmiset, prosessit, teknologiat) tehokkuutta ja kestävyyttä hyväksikäyttämällä niissä olevia heikkouksia. (CIS 2024, 86)

Kun tietoturvan kehityssuunnitelmia tehdään, käyttäjät pitää ottaa mukaan tietoturvan suunnitteluun, jotta organisaation todelliset työskentelytavat tulevat huomioiduksi (NCSC 2019). Mikäli käyttäjät eivät osallistu tietoturvallisuuden suunnitteluun, tietoturvasta vastaaville tulee tahattomasti negatiivinen kuva käyttäjistä, ja epäluottamuksesta käyttäjiä kohtaan rakennetaan teknisiä suojausratkaisuja, joihin käyttäjillä ei ole mitään vaikutusvaltaa (Reinfelder ym. 2019). Ihmiset haluavat suojata organisaatiotaan, mutta se on hankalaa ja kuormittavaa, jos tietoturvaratkaisuja ja käytäntöjä ei ole suunniteltu heidän kanssaan huomioiden jokapäiväistä käyttökokemusta (Blythe ym. 2020).

Esimerkiksi sähköpostiuhkien torjumisen kannalta on tehokkainta panostaa roskapostisuodatukseen ja CSIRT-yksikön prosessiin, jossa raportoidut viestit tarkastetaan ja poistetaan koko organisaation laajuisesti, kun yksikin henkilö on osannut raportoida epäilyttävän viestin. Tällöin tietoturva ei ole kaikkien ihmisten jatkuvan tietoisen sähköpostiviestien yksityiskohtien analysoinnin varassa, ja koulutukseksi riittää viestien epäily ja raportointi ohjeistetusti. (NCSC 2018)

5.2 Yliopistolaisten roolipohjainen tietoturvakoulutus ja tietoturvatietoisuus

Yliopistot ovat monimuotoisia yhteisöjä, jotka koostuvat eri oppiaineiden opiskelijoista, tutkimus-, opetus- ja tukihenkilökunnasta, ja myös opettajankoulutuksen harjoittelukoulujen peruskoulu- ja lukio-oppilaista. Päätoimisten perus- ja jatkotutkinto-opiskelijoiden lisäksi yliopistoissa opiskellaan avoimen yliopiston, erillisopintojen ja erikoistumiskoulutusten kautta. Osa opiskelijoista tulee ulkomailta, joko varsinaisiksi opiskelijoiksi tai lyhemmäksi ajaksi vaihto-opiskelijana. Korkeakoulujen opiskelijat voivat suorittaa opintoja muissa korkeakouluissa kotimaisen opiskelijaliikkuvuuden mahdollistamana. (Turun yliopisto 2024a)

Yliopistojen henkilöstö koostuu pääosin tutkijoista, yliopisto-opettajista, professoreista, tohtorikoulutettavista, hallinto- ja toimistohenkilökunnasta, opetuksen ja tutkimuksen tukihenkilökunnasta, sekä kirjasto- ja IT-henkilökunnasta (Turun yliopisto 2024b). Lisäksi yliopistolle työskentelee lyhytaikaisesti vierailevia tutkijoita, opettajia ja professoreja, sekä yhteistyö- ja ulkoistuskumppaneiden henkilöstöä.

Henkilöstöllä ja siihen rinnastettavilla on tyypillisesti työtehtäviään varten laajemmat käyttöoikeudet yliopiston tietojärjestelmiin, joissa käsitellään suojattavaa tietoa. Henkilötietojen osalta henkilöstö käsittelee muidenkin tietoja, kuten opetushenkilökunta opiskelijoiden tietoja, tutkijat tutkimusaineistojaan ja hallinto- ja tukitehtävissä olevat kaikkien yliopistolaisten tietoja. Opiskelijat näkevät tietojärjestelmissä tyypillisesti vain omat tietonsa.

Yliopistojen tietoturvakouluttamiselle asetetut vaatimukset edellyttävät vain henkilökunnan, ja muiden yliopistolle työskentelevien, kouluttamista roolipohjaisesti heidän tehtäviinsä. Opiskelijoiden ja harjoittelukoulujen oppilaiden kouluttamiselle ei ole vaatimusta. Vaatimuksissa tietoturvakoulutusta pidetään myös edellytyksenä henkilöstön töiden tekemiselle ja niihin tarvittaville käyttöoikeuksille.

Tietoturvan kannalta on hyvä noudattaa vähimpien oikeuksien periaatetta, jota noudattaen käyttäjätunnukselle annetaan oikeudet vain niihin järjestelmiin, joita tunnuksen haltijan täytyy käyttää yliopistolla työskentelyyn tai opiskeluihinsa

(Saltzer & Schroeder 1975). Vähimpien oikeuksien periaatteella riski tietojärjestelmien väärinkäytöstä vähenee, kun henkilön käyttäjätunnuksella ei ole pääsyä ylimääräisiin tietojärjestelmiin.

Henkilöstön osalta perustason tietoturvakoulutuksen pitää kattaa kaikkia koskevat yliopiston tietoturvapolitiikoista ja -käytännöistä, sekä perustason käyttöoikeuksien mukaisten järjestelmien tietoturvalliseen käyttöön tarvittavat ohjeet.

Työtehtäviin, joihin tarvitaan enemmän käyttöoikeuksia, pitää järjestää kohdennettua lisäkoulutusta kyseisten tehtävien riskiarvioiden pohjalta. Tällaiset koulutusta edellyttävät roolit on tunnistettava ja sovittava yliopistossa. Kohdennettu koulutus kannattaa suunnitella kullekin henkilöstöryhmälle sen tehtävien, vastuiden ja yleisten käyttöoikeuksien mukaan, tai kohdennetusti tiettyjen tietojärjestelmien osalta.

Koska tietosuoja-asetus edellyttää koulutusta ennen käyttöoikeuksien antamista, samaa käytäntöä kannattaa soveltaa myös tietoturvakoulutukseen. Tällöin koulutus pitää suorittaa ennen uudessa tehtävässä aloittamista tai uuden tietojärjestelmän käyttöä.

Käytännössä yleisten ja kohdennettujen tietoturvakoulutusten suorittaminen kannattaa kytkeä tarvittavien käyttöoikeuksien saamiseen yliopiston identiteetin- ja pääsynhallinnan järjestelmissä, jolloin vain tietyn roolin henkilöt voivat saada tietojärjestelmiin tarvittavat oikeudet (rooli, attribuutti tai ryhmäjäsenyys) suorittamalla vaaditun koulutuksen. Henkilöstön tehtäviin liittyvä positio pitää huomioida käyttöoikeuksien myöntämisessä tai koulutuksen suorittamisessa, jotta käyttöoikeuksia ei voi saada pelkästään pakollisen koulutuksen suorittamalla.

Käyttöoikeuksiin kytketty koulutus tavoittaa myös paremmin ihmisiä kuin kalenterivuoteen ajastettu koulutus. Tarpeeseen kohdennettu ajankohta vähentää myös infoähkyä, kun uuden henkilöstön ei tarvitse kaikkia koulutuksia suorittaa heti ensimmäisenä.

Kohdennettu koulutus tai ohjeistus kannattaa kytkeä myös optionaalisten käyttöoikeuksien – esimerkiksi etäyhteyden käyttöoikeuden ja työaseman ylläpito-

oikeuden – anomisen yhteyteen, koska ihmiset sisäistävät tietoa tietojärjestelmiin liittyvistä riskeistä ja tietoturvallisista toimintatavoista parhaiten omiin tarpeisiinsa liittyen. Kyseisiä käyttöoikeuksia tarvitsemattomat eivät saa koulutusta heille irrelevantista aiheesta, mutta käyttöoikeuksia tarvitsevat saavat ajankohtaista tietoa tietoturvauhista ja tulevat tietoisemmiksi omista vaikutusmahdollisuuksistaan. Kohdentamaton sisältö taas vähentää koulutuksen vaikutusta ja laskee ihmisten motivaatiota osallistua organisaation suojaamiseen. (Beyer ym. 2015, 3)

Käyttöoikeudet kannattaa antaa määräaikaisina, jolloin oikeudet poistuvat käyttäjätunnukselta, mikäli niihin liittyvää säännöllistä koulutusta ei ole suoritettu ajoissa. Tällöin käyttäjätunnusten tarpeettomista käyttöoikeuksista aiheutuvat riskit vähenevät ja harvoin järjestelmiä käyttävät saavat tuoretta tietoa, kun tarvitsevat pääsyä. Eri käyttöoikeuksien edellyttämä koulutuksen aikaväli voi vaihdella riskiarvioiden mukaan, mutta yhden vuoden välein suoritettava koulutus noudattaa luvun 3 suosituksia. Uusien riskien osalta tietoturvakoulutusta voidaan edellyttää useamminkin, mutta uusista riskeistä voidaan tiedottaa ja ohjeistaa muutenkin kuin tietoturvakoulutuksen kautta.

Opiskelijoiden ja oppilaiden kouluttamisesta

Opiskelijoiden osalta tietojärjestelmien käyttöön liittyy vähemmän riskejä ja ne ovat yleensä pienempiä, koska opiskelijat käsittelevät ensisijaisesti vain omia tietojaan. Yliopistojen kannattaa omien riskiarvioidensa perusteella arvioida tarvitsevatko opiskelijat tietoturvakoulutusta perusopinnoissaan, vai ovatko tarvitut prosessit ja tietojärjestelmät riittävän turvallisia käyttää ilman koulutustakin. Opiskelijoiden käyttämien tietojärjestelmien tietoturvan pitäisi lähtökohtaisesti olla sillä tasolla, että tietoturva ei ole kymmenien tuhansien käyttäjien aktiivisen huomion varassa.

Kaikilla opiskelijoilla ei ole myöskään samanlaisia oikeuksia, joka vähentää niihin liittyvää koulutustarvetta. Esimerkiksi avoimessa yliopistossa ja erillisopintoja opiskelevilla ei välttämättä ole yliopiston sähköpostia käytössä, jolloin sähkö-

postista koituvat riskit ovat marginaalisia. MFA:n laaja käyttö suojaa vääriin käsiin päätyneiltä salasanoilta ja oletuksena rajatut käyttöoikeudet vähentävät riskejä tunnusten väärinkäytölle.

Opiskelijoiden tietoturvaosaaminen perustuu pitkälti yleiseen tietotekniseen osaamiseen. Nuorilla ei kuitenkaan välttämättä ole kokemusta yliopistoissa käytetyistä tietoteknisistä ympäristöistä, jotka pohjautuvat perinteisempiin tietokoneisiin modernien älylaitteiden sijasta (Chin 2021). Opiskelijoille pakollisen tietoturvatestin sijaan voisi olla parempaa sisällyttää laajempi tietoturva-asioitakin sisältävä tietotekniikan käyttöä opettava kurssi pakollisiin opintoihin (Gynther 2023, 7). Kun tietokoneita ja tietojärjestelmiä osaa käyttää paremmin, myös tietoturvaan liittyvät aspektit on helpompi oppia. Esimerkiksi Helsingin yliopistossa Opiskelijan digitaidot -kurssilla opetetaan tietokoneiden käytön perusteita, Helsingin yliopiston tietoteknisestä ympäristöstä, tiedonhankinnasta sekä tietoturvasta ja tietosuojasta (Helsingin yliopisto 2021). Opiskelijoille voi myös tarjota kansalaisten tietoturvataitojen opettamiseen kehitettyä Tietoturva 24/7 -kurssia (Laurea-ammattikorkeakoulu 2024) sekä Cyber Citizen -hankkeessa luotua kyberturvallisuuden kansalaistaitojen oppimisportaalia (Cyber Citizen 2024).

Harjoittelukoulut voivat käyttää yliopistojen tarjoamia tietojärjestelmiä, mutta lähtökohtaisesti yliopistojen kannattaa vähentää riskejä oppilaista johtuvia riskejä eriyttämällä harjoittelukoulut omiin järjestelmiinsä mahdollisuuksien mukaan, sekä estämällä tai rajoittamalla koululaisten käyttöoikeuksia yliopiston tietojärjestelmiin ja dataan. Microsoftin pilvipalvelujen kaltaisissa kaikkien käyttämissä yhteisalustoissa, kuten Teams, käyttöoikeuksien rajaaminen voi olla haasteellista ja tietoturvaongelmilla voi olla laajoja vaikutuksia. Teknologisia ja prosessiratkaisuja, kuten valvontaa tietoturvavalvomolla, kannattaa soveltaa ensisijaisesti, koska tietoturvaa ei voi jättää oppilaiden varaan.

Tietoturvariskien lisäksi yliopistot joutuvat huomioimaan myös käytettävyyttä, jolla voi olla vaikutus yliopiston houkuttelevuuteen. Esimerkiksi avoimen yliopiston opiskelijat maksavat opinnoistaan ja liian vaivalloiset tietoturvakoulutukset voivat turhauttaa opiskelijoita, jotka voivat suorittaa vastaavia opintoja muuallakin. Tietoturvatietoisuustoimet voivat olla riittäviä näissä rajatuissa tapauksissa.

5.3 Pakollisuus ja seuraamukset

Tietoturvakoulutuksen hyödyt realisoituvat, kun ihmiset osallistuvat koulutukseen, oppivat tunnistamaan riskitilanteita, ja välttävät riskialtista käytöstä. Hyödyt jäävät vähäisiksi, jos tietoturvakoulutusta ei suoriteta erinäisistä syistä, esimerkiksi asiasta tietämättömyyden tai mielletyn tarpeettomuuden takia. FUCIO:n tietoturvakyselyn mukaan tietoturvakoulutus oli linjattu pakolliseksi monessa yliopistossa, mutta kaikissa yliopistoissa suorittamista ei kuitenkaan seurattu tai osaamista testattu tietoturvatestillä (Seesto, T., sähköposti 30.1.2023).

Henkilökunnan ja siihen rinnastettavien henkilöiden osalta kouluttaminen on pakollista, niin uusille työntekijöille kuin uusiin tehtäviin vaihtaville. Kappaleessa 3.12 esitellyt tiedonhallintalain ja tietosuoja-asetuksen vaatimukset edellyttävät henkilöstön kouluttamista tietoturva- ja tietosuoja-asioista riski- ja roolipohjaisesti. Työnantaja voi työsopimuslain työnjohto- eli direktio-oikeudella määrätä työntekijät suorittamaan työnantajan tarpeelliseksi näkemät koulutukset ja testit.

Tietosuoja-asetus edellyttää, että henkilöstö pitää kouluttaa ennen kuin henkilötietoja päästetään käsittelemään, ja koulutusten suorittamista pitää seurata. Käytännössä vaatimukset on tehokkainta ja helpointa täyttää tekemällä koulutuksista edellytyksiä käyttäjätunnuksen erilaisille käyttöoikeuksille, jolloin tekniset estot vähentävät myös tietoturvariskejä. Roolipohjaisista käyttöoikeuksista kannattaa tehdä määräaikaisia, jolloin töihin tarvittavat oikeudet saa pidettyä tarvitun koulutuksen suorittamalla, ja ne poistuvat, mikäli vaadittua koulutusta ei ole suoritettu. Koulutus voi olla pakollinen esimerkiksi muutaman vuoden välein suoritettavana, koska riskipohjaisia päivityksiä ja ohjeita voi antaa tarvittaessa muillakin tietoisuutta lisäävillä keinoilla. Varsinaisen koulutuksen suorittaminen säännöllisesti antaa ajankohtaiset päivitykset käytäntöihin ja uudet huomioitavat seikat kattavamman kertauksen lisäksi.

Opiskelijoiden suhde yliopistoon on erilainen kuin henkilöstöllä. Kappaleessa 3.12 käytiin läpi opiskelijoiden yleisöön rinnastettavaa suhdetta yliopistoyhteisössä. Luvun kolme vaatimukset henkilöstön kouluttamisesta eivät siis koske

opiskelijoita. Opiskelijat myös käyttävät tietojärjestelmiä rajatummin, ja käyttöön liittyy vähemmän ja pienempiä riskejä, kuten kappaleessa 5.2 kuvattiin.

Yliopistot voivat kuitenkin omien riskiarvioidensa mukaisesti edellyttää tietoturvakoulutusten tai -testien suorittamista opiskelijoiltakin, mutta koulutusten pakollisuutta hyötyihin nähden kannattaa harkita. Opiskelijoidenkin valinnaisista käyttöoikeuksista kannattaa tehdä määräaikaisia ja koulutukseen sidottuja, kuten henkilökunnankin osalta. Opiskelijoiden tehdessä tutkimusta heiltä on edellytettävä samoja koulutuksia kuin tutkijoiltakin vastaavassa tilanteessa.

Tietoturvakoulutuksesta kannattaa tehdä pakollinen kaikille tietoturvapoikkeamissa osallisina olleille ja riskialtista käytöstä osoittaneille asemasta ja roolista riippumatta. Samalla on hyvä muistuttaa oikeudenmukaisen toimintakulttuurin hengessä, että vaadittava lisäkoulutus ei ole rangaistus, vaan toimenpide, jolla varmistetaan turvallisuutta (Traficom 2022).

Seuraamukset suorittamattomuudesta

Henkilöstön työnteko ja opiskelijoiden opiskelu ovat yliopiston tärkeimpiä tehtäviä. Työnteon ja opiskelun rajoittaminen tai estäminen tietoturvan takia on järeä toimi, koska se asettaa henkilöstön ja opiskelijoiden ensisijaiset tarpeet tietoturvallisuutta vastaan. Tietoturvasääntöjen ja -käytäntöjen pitäisi osana positiivista tietoturvakulttuuria sopia organisaation todellisiin työskentelytapoihin, jotta tietoturva on osa työtä – ei asia, josta pitää erikseen huolehtia (NCSC 2019).

Ohjeistus käyttäjätunnusten käytöstä ja käyttöoikeuksien edellyttämät tietoturvakoulutukset ja -testit pitää huomioida ja tuoda julki velvoittavina yliopiston tietoturvapolitiikassa sekä IT-käyttösäännöissä, jolloin tietoturvakoulutukset ovat käyttäjätunnuksen ja käyttöoikeuksien ominaisuus. Nämä luovat pohjan yliopiston tietoturvallisuudelle ja tietojärjestelmien käytön edellytyksille, niin työnteon kuin opiskelun osalta.

Pakollisten tietoturvakoulutusten suorittamattomuudesta seuraa edellä ehdotetun käyttöoikeuksiin sidotun mallin mukaisesti käyttöoikeuksien vanheneminen

ja poistuminen. Henkilöitä pitää tiedottaa asiasta hyvissä ajoin, jotta he voivat suorittaa koulutuksen ennen oikeuksien vanhenemista.

Henkilöstön osalta esihenkilöitä pitää tiedottaa alaisten oikeuksien poistumisesta, jotta työntekijöitä voidaan opastaa tarvittujen koulutusten pakollisuudesta työtehtäviä varten. Esihenkilöiden pitää järjestää aikaa pakollisten tietoturvakoulutusten suorittamiseen, jotta suoritus ei jäisi tästä kiinni (Hielscher ym. 2023, 2317). Mikäli henkilön töiden tekemiselle edellytettyjen käyttöoikeuksien vaatimia koulutuksia ei ole suoriteta, työnantajan ohjeista poikkeaminen pitää käsitellä työlainsäädännön mukaisesti.

Opiskelijoilla ei ole henkilökunnan tapaan työsuhdetta korkeakouluun, joten työlainsäädännön sijaan opiskelijoiden kurinpidosta säädetään sekä yliopistolaissa (5:45) että ammattikorkeakoululaissa (6:38). Näiden molempien pykälien kohta 3 vilpillisestä menettelystä tai korkeakoulun järjestyksen rikkomisesta oikeuttaa kurinpitotoimiin. Yliopisto- ja ammattikorkeakoululakien mahdollistamia kurinpitotoimia kannattaa soveltaa vasta muiden vaihtoehtojen jälkeen.

Osa yliopistoista on tehnyt säännöllisen tietoturvakoulutuksen tai tietoturvatestin hyväksytystä suorittamisesta edellytyksen yliopiston palvelujen käytölle (Gyntther 2023), jolloin suorittamattomuudesta tai testin läpäisemättömyydestä seuraa sanktio, joka vaihtelee päivittäisistä salasanavaihdoista (Tampereen yliopisto 2024) käyttäjätunnuksen sulkemiseen (Åbo Akademi 2024, Helsingin yliopisto 2022). Näillä toimilla rajoitetaan mahdollisuutta käyttäjätunnuksen väärinkäyttöön varsinkin silloin, kun tietoturvatestiä ei ole suoritettu käyttäjätunnuksen tarpeettomuuden takia, mutta tunnus on jollain perusteella aktiivinen. Käyttäjätunnuksen rajoittaminen haittaa samalla merkittävästi myös käyttäjätunnuksen oikeaa käyttöä työntekoon ja opiskeluun, molempien edellyttäessä merkittävästi sähköisten palvelujen ja aineistojen käyttöä yliopiston käyttäjätunnuksella.

Seuraamuksia suunnitellessa täytyy arvioida, onko seuraamus oikea suhteessa tietoturvariskeihin, joihin perustason tietoturvakoulutuksella tai -testillä voidaan realistisesti vaikuttaa. Arvioinnissa pitää myös huomioida mihin kaikkiin palveluihin esimerkiksi käyttäjätunnuksen sulkeminen tai käyttöoikeuksien poistaminen

vaikuttaa: otetaanko sähköpostia vastaan vai palautetaanko lähettäjälle virhe toimimattomasta osoitteesta, mihin palveluihin toimimaton sähköposti voi vaikuttaa, käytetäänkö käyttäjätunnusta automaattiseen tietojenkäsittelyyn, sekä muihin vastaaviin, ja niiden riippuvuuksiin.

Tietoturvariskien ja käyttäjätunnuksen pääasiallisen käytön kannalta käyttöoikeuksien rajoittaminen roolipohjaisten oikeuksien kautta voi sanktiona olla tasapainoisempi ratkaisu, kuin käyttäjätunnuksen käytön estäminen kokonaan.

Yliopistot voivat aina estää käyttäjätunnuksen käytön, mikäli se on välttämätöntä viestintäverkkojen tai niihin liitettyjen palvelujen, tietojärjestelmien, tai käyttäjätunnusten henkilökohtaisten tietojen tietoturvasta huolehtimiseksi (Laki sähköisen viestinnän palveluista 917/2014, 10:272.1).

5.4 Suoritusten hyväksiluku ja yhteinen koulutusmateriaali

Pakollisten tietoturvakoulutusten ja -testien on ehdotettu pohjautuvan yhteisiin vähimmäisvaatimuksiin, ja sen myötä suoritukset hyväksyttäväksi ristiin. Suoritustiedon teknistä siirrettävyyttä ei kuitenkaan pidetty pakollisena, varsinkin kun tietoturvatestin suorittamisen on tarkoitus viedä aikaa vain 5–10 minuuttia vuodessa kussakin korkeakoulussa. (Gynther 2023)

Verkottuneessa korkeakoulumaailmassa ihmisten tietoturvaa helpottaa mahdollisuus käyttää oman kotikorkeakoulun käyttäjätunnusta myös muiden korkeakoulujen palveluihin kirjautumiseen niin sanotuilla federoiduilla kirjautumisjärjestelmillä, kuten kansallisella Haka- (CSC 2024) tai kansainvälisellä eduGAIN-käyttäjätunnistusjärjestelmällä (eduGAIN 2024). Joillakin ihmisillä voi myös olla opintojen, työn tai yhteistyön takia käyttäjätunnus useampaan kuin yhteen korkeakouluun.

Mikäli kussakin korkeakoulussa on suoritettava pakollinen tietoturvatesti, ihmiset pääsisivät helpommalla, kun aiemmin yhdessä korkeakoulussa suoritettu tietoturvatesti hyväksiluettaisiin toisiin korkeakouluihin, eikä kunkin korkeakoulun tietoturvatestiä tarvitsisi suorittaa.

Käytännössä tietoturvakoulutusten ja -testien käytöllä pyritään parantamaan kunkin korkeakoulun omaa tietoturvaa sen tunnistamien riskien pohjalta. Vestman (2020, 144) toteaa, että kunkin organisaation johto määrittelee organisaatiota koskevat strategiset linjaukset, joiden varaan tietoturvakin rakentuu. Vaikka korkeakoulut ovat pitkälti toistensa kaltaisia makrotasolla katsottuna, niiden turvattavat tiedot ja toimintatavat vaihtelevat, jonka myötä myös tietoturvan tarve, merkitys ja toteutustavat ovat organisaatiokohtaisia. Kukin organisaatio arvioi millaisia tietoturvariskejä se sietää ja millainen on riittävä tietoturvan taso.

Käytännössä tietoturvakoulutusten ja -testien hyväksiluku edellyttää, että koulutuksille ja testeille on käytössä yhteinen minimitaso, joka kelpaa kaikille, ja myös kattaa riittävästi kaikille yhteisiä tietoturvariskejä. Koska kaikilla ei ole samanlaisia tietojärjestelmiä ja tietoturvariskejä, yhteisestä pohjasta voi tulla turhan laaja, jolloin siinä on myös epärelevantteja aiheita, tai liian suppea, jolloin se ei kata riittävästi riskejä. Tietoturvatesteistä ei myöskään kannata tehdä monitasoista, koska erojen takia on järkevämpää suorittaa tarvittavat roolipohjaiset koulutukset kussakin korkeakoulussa. Myös koulutusten ja testien suoritusväli pitäisi saada sovittua yhtenäiseksi.

Osa luvussa 3 käsitellyistä vaatimuksista edellyttää myös tietoturvaosaamisen osoittamista. Näiden kannalta toisessa organisaatiossa suoritettua tietoturvatestiä tuskin pidetään arvioitavan organisaation tietoturvan ja riskien kannalta vaatimukset täyttävänä osoituksena organisaation panostuksesta tietoturvakoulutukseen. Nämä aspektit huomioiden korkeakouluja parhaiten palvelee sen oman tietoturvakoulutuksen ja/tai -testin käyttö, joka huomioi paikalliset tietoturvariskit, toimintatavat ja ohjeet.

Suoritustietojen siirtäminen

Mikäli tietoturvatestien hyväksiluvussa löydetään yhteinen pohja, pitää tieto suorituksesta saada myös siirrettyä toisiin korkeakouluihin. Käytännössä tiedonsiirron pitäisi olla automaattista ja tämä on helpointa toteuttaa federoidun kirjautumisen yhteydessä, jossa voidaan siirtää palvelujen edellyttämiä käyttäjätietoja

erilaisissa attribuuteissa. Tiedon tietoturvakoulutuksen tai -testin suorituksesta voi luovuttaa esimerkiksi eduPerson-skeeman eduPersonEntitlement-attribuutin yhteisesti sovittuna arvona (REFEDS 2022). Korkeakouluilla on myös mekanismeja toisissa korkeakouluissa suoritettujen opintosuoritusten siirtoon, kuten VIRTA-opintotietopalvelu (CSC n.d.). Ne eivät kuitenkaan lähtökohtaisesti sovellu henkilökunnan suorittamien henkilöstökoulutusten siirtämiseen, koska henkilökunnan koulutussuorituksia ei tyypillisesti hallita opiskelijoiden tapaan opintojärjestelmissä. VIRTA-opintotietopalvelun käyttäminen edellyttää myös oppijanumeron hankkimista henkilökunnalle.

Tietojärjestelmiin on mahdollista rakentaa tuki paikallisen tietoturvakoulutuksen ja/tai -testin suorittamiseksi myös federoidun kirjautumisen kautta tuleville käyttäjille, jos näiden kirjautumistiedoissa ei tule mukana tietoa voimassa olevasta suorituksesta. Sama ratkaisu pitää ottaa käyttöön kaikissa korkeakoulun federoitua kirjautumista käyttävissä tietojärjestelmissä, jotta tieto paikallisista suorituksista on käytössä eri tietojärjestelmien välillä.

Tietoturvakoulutusten edellyttäminen federoiduissa tietojärjestelmissä ei estä tunkeutumista vuotaneilla tunnuksilla. Federoidun kirjautumisen väärinkäytön riskejä voidaan vähentää edellyttämällä monivaiheisen kirjautumisen käyttöä sekä tilanteeseen sopivaa henkilöiden tunnistustasoa (REFEDS 2023). Hakassa ja eduGAIN:ssa on käytössä myös vapaaehtoinen SIRTFI v2 -luottamuskäytäntö, jossa edellytetään kyvykkyyttä tunkeutumisten havaitsemiseen ja ilmoittamaan näistä toisille organisaatioille (SIRTFI v2 2022). Korkeamman tietoturvatason järjestelmiin voidaan sallia pääsy vain SIRTFI-luottamuskäytäntöön sitoutuneista organisaatioista.

Korkeakoulujen väliset erot hankaloittavat yhteisen tietoturvakoulutusmateriaalin käyttämistä. Mutta vaikka koulutuksille ja testeille ei saataisi sovittua yhteistä minimitaso ja sisältöpohjaa, korkeakouluilla on kuitenkin monilta osin samoja käytäntöjä ja yhteisesti käytössä olevia järjestelmiä, joiden pohjalta koulutusmateriaalia voidaan luoda ja jakaa yhteisesti käytettäväksi (Gynther 2023).

6 Ehdotus ihmislähtöiseen tietoturvaan

Tavoitteena on vähentää yliopiston tietoturvariskejä kokonaisuutena, jolloin tietoturva on osa tietotekniikan normaalia käyttöä, eikä erikseen huomioitava asia. Jotta tietoturvariskit vähenisivät niin ihmisten, teknologian kuin prosessien osalta, yliopiston tietoturvaa kannattaa kehittää ihmislähtöisesti, myös muut osa-alueet huomioiden. Ihminen on osa kokonaisuutta ja siten muutoksilla on vaikutus ihmisiin tavalla tai toisella.

6.1 Suunnitelman luonti

Ihmislähtöiselle tietoturvaohjelmalle tarvitaan alustava suunnitelma, jossa kuvataan tavoitteet ja keinot niiden saavuttamiseen. Apuna kannattaa käyttää kattavaa NIST:n SP 800-50r1: Building a Cybersecurity and Privacy Learning Program -ohjeistusta. Ohjelman tavoitteeksi kannattaa ottaa esiteltyjen kypsyysmallien taso 3, jolla riskitaso alkaa laskemaan ihmiskeskeisten riskien hallinnan ja käyttäytymisen muutosten myötä (SANS 2025; Carpenter & Roer 2022). Aikataulun on hyvä olla rauhallinen, koska muutosten hyötyjen ilmenemisessä menee oma aikansa. Suunnittelua kannattaa tehdä henkilöstöosaston kanssa, koska he hoitavat käytännössä koulutusten sovittamisen yliopiston muiden henkilöstökoulutusten joukkoon.

Johdon tuki suunnitelmalle ja sitoutuminen sen toteuttamiseen ovat kriittisen tärkeitä, koska organisaatiossa pyritään tekemään isoa muutosta, johon pitää sitoutua pitkällä tähtäimellä. Johdon näyttämää esimerkkiä tarvitaan myös positiivisen kulttuurin edistämiseen.

SANS:n (2024) mukaan kaksi suurinta hidastetta tietoisuusohjelman menestymiselle ovat ajan ja henkilöstön riittämättömyys, joten SANS:n (2025) suosituksen mukaisesti kehittämisohjelmaan kannattaa pyrkiä dedikoimaan henkilö. Psykologian aiheet ovat itsessään monimutkaisia ja edellyttävät uusia taitoja, joita ei perinteisillä tietoturva-asiantuntijoilla ole (Hielscher ym. 2023, 2311, 2323).

6.2 Riskien ja puutteiden kartoitus

Tiedonhallintalain 4:13 mukaisesti organisaation pitää selvittää olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet niiden mukaan (Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906). Ilman selvitystä voidaan keskittyä vääriin asioihin, jotka eivät laske riskitasoa. Kunkin yliopiston kannattaa tehdä oma selvitys, koska muiden riskejä ja puutteita ei kannata kopioida itselle, vaikka yhteisiä prosesseja ja teknologioita onkin käytössä.

Kuten kappaleessa 5.1 kerrottiin, selvitys kannattaa tehdä hyökkääjän näkökulmasta tehdyllä tunkeutumistestauksella, mahdollisimman laajana niin Internetistä kuin sisäverkosta käsin.

Tunkeutumistestauksen yhteydessä tarjottaneen kalastelusimulaatioiden käyttöä ihmisten tietoturvaosaamisen arviointiin, vaikka niiden siihen on kyseenalaista, kuten kappaleessa 4.4 kerrottiin. Sähköpostiin liittyvien riskien osalta kannattaa arvioida roskapostisuodatuksen tehokkuutta yleisesti, liitetiedostojen käsittelyn sekä toimitusjohtajahuijausten osalta, kalastelusuojattujen MFA-menetelmien käyttöastetta ja MFA:n käyttölaajuutta, sekä tapoja raportoida kalasteluviestejä organisaation CSIRT-yksikölle ja sen käsittelyprosesseja.

Yliopiston kaltaisessa monimuotoisessa ympäristössä voi olla vaikea ennakoida kaikkien yksiköiden tietoturvariskejä. Tätä varten kannattaa tehdä avoin kysely suoraan henkilöstölle, jossa pyydetään kommentteja asioista, joiden tietoturvallisuutta pitäisi kehittää tai muuten parantaa (Beyer ym. 2015, 9).

6.3 Riskien hallinta

Tuloksista kannattaa priorisoida teknisten heikkouksien ja haavoittuvuuksien korjaaminen helpoimmin hyväksikäytettävistä alkaen. Tekniset puutteet kannattaa ensisijaisesti eliminoida päivityksillä ja kovennuksilla. Turvattomat järjestelmät kannattaa mahdollisuuksien mukaan poistaa, koska niiden kompensointi prosesseilla tai ihmisten työpanoksella ei poista virheiden mahdollisuutta, ja vaatii resursseja niin kauan kuin puutteet ovat olemassa. Varsinkin ihmisiltä

huomion vaatiminen toteutettavissa olevien parannusten sijaan turhauttaa ja altistaa turhaan riskeille.

Tunkeutumistestauksessa voi löytyä tietojärjestelmiä tai -palveluja, jotka kaipaavat uusimista tai kehittämistä. Näiden kanssa kannatta huomioida tietoturvallinen käyttökokemus alusta alkaen, miettimällä minkälaisia ohjeistuksia nykyinen järjestelmä tarvitsee, ja voiko ohjeistuksia vähentää järjestelmää kehittämällä.

Riskejä kannattaa hallita jäljelle jäävien haavoittuvuuksien ja puutteiden osalta luvussa kolme esiteltyjä viitemalleja hyödyntäen. Riskien osalta kannattaa pyrkiä tilanteeseen, jossa laajan vaikutuksen riskit eivät ole mahdollisia yksittäisen tavallisen käyttäjän oikeuksilla. Tietoturvakäytännöillä joudutaan usein tasapainottelemaan käytettävyyden ja tietoturvan vahvuuden välillä, ja ihmisten näkökulmaa pitää muistaa huomioida, jotta tietoturvakäytännöistä ei tule työntekoa haittaavia (NCSC 2017).

Harjoittelukoulujen toimintaa kannattaa eriyttää mahdollisuuksien mukaan yliopiston muuhun toimintaan liittyvistä järjestelmistä.

Jäljelle jääneitä riskejä pitää huomioida tietoturvakoulutuksia ja tietoisuuden kehittämistä suunnitellessa, jotta jäännösriski pienenee ihmisten osaamisen kautta.

6.4 Roolipohjaisten koulutusten luonti

Roolipohjaisten tietoturvakoulutusten luonti henkilöstölle ja muille yliopistolle työskenteleville, eli kumppaneiden ja toimittajien yliopistolle työskentelevälle henkilöstölle, edellyttää roolien määrittelyä. Roolit pitää pystyä kuvailemaan ja käyttämään myös teknisesti attribuuteilla tai ryhmäjäsenyyksillä, jotta niitä voidaan soveltaa koulutusten, käyttöoikeuksien ja viestinnän kohdentamisessa.

Aluksi täytyy kartoittaa missä kaikissa työntekijärooleissa riskiarvioiden mukaan tarvitaan omaa tietoturva- ja tietosuojakoulutusta. Tässä kannattaa aloittaa yliopiston toiminnalle tärkeissä tehtävissä työskentelevistä. Yksi tärkeä, mutta muusta henkilöstöstä poikkeava, ryhmä on tietoturvavastuita omaava henkilös-

tö, joka tarvitsee omaan rooliinsa sopivaa koulutusta, jotta he tuntevat uhkaympäristön, ymmärtävät hyökkäystekniikoita ja osaavat suojata yliopistoa niiltä.

Perusmuotoisessa tietoturvakoulutuksessa käydään läpi kaikkia koskevia yleisiä asioita, kuten tietoturvasäännöt ja -velvoitteet, yleiset tietoturvamenettelyt, mistä saa lisätietoa ja apua, oma vastuu koko yliopiston tietoturvalle, laitteiden turvallinen käyttö, sekä yliopistoa koskevia uhkia. Koulutusta kaipaavia asioita voidaan tunnistaa tunkeutumistestauksen, kyselyn, havaittujen poikkeamien kautta, sekä ajankohtaisia tapahtumia seuraamalla.

Tietoturvakoulutusten sisältöä kannattaa päivittää vähintään vuoden välein, jolloin huomioidaan uudet uhat ja riskit, poikkeamat, sekä muutokset yliopistoa koskevissa käytännöissä ja ohjeissa. Myös tekoälyn kaltaiset uudet teknologiat voivat edellyttää koulutuksessa huomiointia.

Yliopiston pitää myös linjata miten usein tietoturvakoulutus pitää suorittaa. Samalla on hyvä linjata muita tietoisuustoimien käyttöä, jotta uusien uhkien ja riskien osalta ihmisiä voidaan kouluttaa heti, eikä vasta määräaikaisen koulutuksen tullessa ajankohtaiseksi.

Tietoturvakoulutusten suunnittelussa kannattaa huomioida sekä itseopiskelu että interaktiiviset koulutustilaisuudet. Itseopiskelussa kannattaa hyödyntää yliopistolla käytössä olevaa oppimisalustaa. Mikäli koulutuksiin päädytään käyttämään jotain kaupallista ratkaisua, valinnassa täytyy huomioida yliopiston toimintaympäristö ja riskit, jotta koulutukset sopivat yliopistolle.

Koulutusten suorittamisen kirjanpito ei välttämättä onnistu oppimisalustalla eikä henkilöstön osalta perinteisissä opintojärjestelmissä, joten henkilöstökoulutusten kirjanpito ja suoritusten vienti oppimisalustalta on suunniteltava sopivaan tietojärjestelmään. Samaan järjestelmään on hyvä rakentaa mekanismit suoritusten seurantaan, sekä tiedotuskanavat tietoturvakoulutuksen seuraavasta ajankohdasta, ja myös esihenkilöille, jos henkilöstö ei ole suorittanut koulutusta määräajan lähestyessä.

Koulutusten saaminen edellytykseksi henkilökuntaroolien tarvitsemille käyttöoikeuksille edellyttää kytköstä henkilökoulutusten kirjanpidon ja identiteetinhallintajärjestelmän välillä, johon pitää luoda henkilöstöroolia, suoritettua koulutusta ja määräaikaa yhdistelevä automaattisesti tuleva ja poistuva käyttöoikeus, jota voidaan käyttää yliopiston pääsynhallintajärjestelmissä. Kun käyttöoikeudet ovat käytettävissä, niitä pitää käyttää relevanteissa tietojärjestelmissä, joissa pääsyä halutaan rajata. Tietoturvakoulutuksiin sidotut käyttöoikeudet pitää huomioida myös yliopiston tietoturvapolitiikassa ja IT-käyttösäännöissä.

Tietoturvakoulutuksen suorittamisesta kannattaa tehdä pakollinen tietoturvapoikkeamissa osallisina olleille, ja tällöin pitää muistuttaa sen olevan toimenpide tietoturvallisuuden varmistamiseksi – ei rangaistus.

Opiskelijoille ja muille vastaavan tason rajoitetuille käyttäjille riittää kaikkia koskevien politiikkojen sekä IT-käyttösääntöjen hyväksyntä, palvelujen ohjeistus, sekä yleiset tietoturvatietoisuustoimet. Opiskelijoille kannattaa luoda digitaitoja opettava kurssi, joka käy läpi myös tietoturva- ja tietosuoja-asioita.

Riskit Haka- ja eduGAIN-kirjautumisten osalta ovat rajatummat yliopiston tietojärjestelmien osalta, mutta samalla tietojärjestelmään pääsevien käyttäjätunnusten määrä on korkeampi. Riskiarvioiden perusteella vaihtoehtona on luottaa tietojärjestelmän tietoturvaan ja tietoturvatietoisuustoimiin, tai pyrkiä soveltamaan kappaleessa 5.4 kuvattuja tapoja federoitujen kirjautumisten tietoturvan ja luottamuksen parantamiseen.

6.5 Käyttäytymismuutosten edistäminen ja kulttuurin kehittäminen

Tietoturvatietoisuus alkaa ohjeistuksista, joiden on oltava helposti löydettävissä ja niin käytettäviä, että niihin viitataan yliopiston arjessa (NCSC 2024a, 30). Ohjeistuksissa kannattaa kuvata tietoturvalliset tavat toimia, jolloin yliopistolaiset voivat luottaa toimivansa oikein noudattaessaan ohjeita.

Tietoturvatietoisuustoimien suunnittelussa, erityisesti uusien riskien osalta, kannattaa hyödyntää luvussa 4 kuvattuja tapoja. Viestien toisto sekä useiden kana-

vien hyödyntäminen on tärkeää, jotta asiat pysyvät ihmisten mielessä. Tietoisuustoimia kannattaa suunnitella akateemisen vuoden ajankohtiin, ja hyödyntää lokakuisen kyberturvallisuuskuukauden kaltaisia yleisiä tilaisuuksia. Tietoturvanäkökulmia kannattaa tuoda esiin yliopiston muissakin koulutuksissa.

Kaikkia kappaleessa 4.1 esiteltyjä COM-B-mallia hyödyntäviä menetelmiä voi soveltaa, kun ihmisten halutaan tekevän uusia asioita tietoturvan hyväksi, tai muuttavan käytöstään tietoturvallisemmaksi tunnistetuissa asioissa. Erityisesti ihmisten motivointi on tärkeää, koska sillä on suurin vaikutus käyttäytymisen muutokseen. Dialogi henkilöstön kanssa on tärkeä, jotta tietoturvatoimia suunnittelevat ymmärtävät, miten yliopistolla työskennellään, ja miten tietoturva toteutuu käytännössä. Keskustelussa voidaan ohjata ihmisiä tietoturvallisempiin toimintatapoihin.

Positiivisen tietoturvakulttuurin luomisessa on tärkeää ylläpitää positiivista suhtautumista tietoturva-asioihin ja kertoa miten ihmiset voivat auttaa yliopiston tietoturvan toteutumisessa. Tässä esihenkilöt sekä IT- ja tietoturvahenkilöstö ovat avainasemassa, koska heidän oma esimerkkinsä sekä reaktionsa erilaisiin tekoihin ja tapahtumiin määrittelevät ihmisten kokemusta.

Esihenkilöille sekä IT- ja tietoturvahenkilöstölle on tärkeää kertoa miten oikeudenmukaisessa toimintakulttuurissa ei syyllistetä, vaan asioita käsitellään molemmin puolin parantamismahdollisuutena, ja ilmoitukset käsitellään asianmukaisesti. Tietoturvailmoituksiin liittyvät prosessit on hyvä kuvata avoimesti, jotta ihmiset voivat tietää, miten poikkeamia käsitellään ja miten päätöksiä tehdään. Tietoturvailmoituksia ja -poikkeamia pitää analysoida juurisyiden löytämiseksi, jotta korjaavat toimet kohdistetaan ongelman varsinaiseen lähteeseen, oli se sitten ihmisestä, prosessista tai teknologiasta johtuva.

Tietoturvakäyttäytymisen kehittämiskohteiden selvittämiseen kannattaa käyttää kappaleessa 4.4 kuvattua Security Culture Surveytä. Tietoturvatietoisuuden ja tietoturvakulttuurin kypsyystason kehittymisessä kannattaa hyödyntää SANS:n Security Awareness Maturity Modelin (2025; liite 4, Taulukko 10) People Indicatoreita ja tietoturvariskien kehittymisessä taulukon Metrics-osiota.

7 Lopuksi

Opinnäytetyön tavoitteena oli kartoittaa yliopistoja koskevia tietoturvavaatimuksia sekä selvittää, miten ihmisiä voidaan huomioida yliopistojen tietoturvaa kehittäessä, jotta ihmisiin liittyvät tietoturvariskit vähenisivät. Vaatimuksia kartoitettiin lainsäädännöstä sekä tietoturvan viitemalleista, ja ihmiskeskeistä tietoturvaa analysoitiin tutkimustiedon avulla. Tuloksia vertailtiin yliopistoissa käytettäväksi ehdotettuun tietoturvatestauksen malliin.

Tietoturvatestiä on Hielscherin ym. (2023) löydösten mukaisesti ehdotettu nopeana ja helppona ratkaisuna monimutkaiseen ongelmaan. Ehdotettu kerran vuodessa tehtävä, kaikille samanlainen tietoturvakoulutus tai -testi ei täytä tiedonhallintalain ja tietosuoja-asetuksen yliopistoille asettamia tietoturvavaatimuksia. Koska alimman kypsyystason tietoturvatietoisuustoimet eivät juuri muuta ihmisten käyttäytymistä tietoturvallisemmaksi, ja siten vähennä riskialtista käytöstä, pakosta suoritettava koulutus voi olla jopa haitallinen sen antaessa väärän kuvan riskien hallinnasta (SANS 2025).

Vaatimusten täyttämiseksi yliopistojen pitää kouluttaa henkilöstöä tietoturva- ja tietosuoja-asioista heidän omiin työtehtäviinsä liittyen. Opiskelijoiden osalta vastaavaa vaatimusta ei ole, joten yliopistot voivat kouluttaa heitä oman riskienhallintansa mukaan. Tietoturvatietoisuuden, tietoturvallisen käyttäytymisen muutoksen edistämisessä kannattaa hyödyntää tietoturvaan sovellettuja psykologisia malleja, joilla saadaan motivoitua muutosta. Henkilöstö kannattaa ottaa mukaan prosessien ja teknologian tietoturvaa suunnitteluun mukaan, jotta todelliset työskentelytavat tulevat huomioiduksi. Tietoturvatietoisuusohjelmaa käynnistäessä kannattaa huomioida, että ihmiskeskeisen tietoturvan kehittämisessä kannattaa hyödyntää ihmistieteiden osaajia (NPSA 2023, 5).

Tässä opinnäytetyössä on tehty rajauksia käytettävien tutkimusten suhteen, koska ihmiskeskeistä tietoturvaa on tutkittu pitkään ja tutkimusala on laajentunut viime vuosina. Aihetta kannattaisi jatkaa organisaatioissa sovellettavien valmiiden toimintamallien kehittämisellä, koska yksittäisten tieteellisten tutkimusten tuloksia on vaikea soveltaa laajoihin organisaatioihin. Tällaisten kehittämisessä

tarvitaan osaajia muun muassa digitaitojen, erilaisten oppimistapojen ja digitaalisten oppimisympäristöjen osalta. Tässä tietoturva-asiantuntijoiden yhteistyö psykologien, sosiologien ja kasvatustieteilijöiden kanssa on avainasemassa.

Lähteet

Aarnio, E. 2001. TCB-tuomio luo suuntaviivat oikeuskäytännölle. Digitoday. Viitattu 29.5.2024. https://www.is.fi/digitoday/art-2000001335512.html

Aittasalo, M. 2024. Terveys- ja liikuntakäyttäytyminen. UKK-instituutti. Viitattu 8.3.2025. https://ukkinstituutti.fi/elintapaohjaus/kayttaytymisen-muutos/terveys-ja-liikuntakayttaytyminen/

Aittasalo, M.; Hankonen, N.; Nupponen, R. & Seppälä, T. 2017. Käyttäytymisen muutospyörä. UKK-instituutti. Viitattu 2.3.2025. https://ukkinstituutti.fi/elintapaohjaus/edistamismallit/kayttaytymisen-muutospyora/

Aivio, L.; Keinänen, K.; Martikainen, J.; Sjöblom, P. & Wilson I. 2022. Työryhmäraportti: Tietoturvallinen tunnistautuminen yliopisto-opiskelussa. UNIFI ry. Viitattu 2.6.2024. https://tt.eduuni.fi/sites/kity/publicAAPAFUCIOdocs/UNIFI_Opiskelijan_tietoturvallinen_tunnistautuminen_työryhmän_loppuraportti.pdf

Ammattikorkeakoululaki 14.11.2014/932

Baker, K. 2022. History of Ransomware. Viitattu 29.5.2024. https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/

Beyer, M.; Ahmed, S.; Doerlemann, K.; Arnell, S.; Parkin, S.; Sasse, A. & Passingham, N. 2015. Awareness is only the first step: A framework for progressive engagement of staff in cyber security. Viitattu 13.4.2025. https://web.archive.org/web/20170312170258/https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

Biedalak, K. & Woźniak, P. 2017. Did Ebbinghaus invent spaced repetition? Viitattu 26.5.2025. https://www.supermemo.com/en/blog/did-ebbinghaus-invent-spaced-repetition

Blythe, J. M.; Gray, A. & Collins, E. 2020. Human Cyber Risk Management by Security Awareness Professionals: Carrots or Sticks to Drive Behaviour Change? HCI for Cybersecurity, Privacy and Trust. Lecture Notes in Computer

Science, vol 12210, Springer, Cham. https://doi.org/10.1007/978-3-030-50309-3_6

Candrick, W.; Addiscott, R.; Walls, A. & Michaels, A. 2023. Security Awareness Efforts Fall Short! Now What? (Survey Results Analysis). Gartner. Viitattu 17.8.2024. https://www.gartner.com/document/4118799?ref=solrAll&refval=404498637

Carpenter, P. & Roer, K. 2022. The Security Culture Playbook: An Executive Guide to Reducing Risk and Developing Your Human Defense Layer. Hoboken: John Wiley & Sons Inc.

Center for Internet Security. 2024. CIS Critical Security Controls Version 8.1. Viitattu 31.12.2024. https://www.cisecurity.org/controls

CERT NZ. 2022. Cyber Change: Behavioural insights for being secure online. Viitattu 31.3.2025. https://www.cert.govt.nz/assets/resources/cert-nz-cyber-change-behavioural-insights-2022-online-version.pdf

Chin, M. 2021. File not found. The Verge. Viitattu 10.6.2024. https://www.theverge.com/22684730/students-file-folder-directory-structure-education-gen-z

CSC. 2024. Haka-käyttäjätunnistusjärjestelmä. Viitattu 9.6.2024. https://wiki.eduuni.fi/display/CSCHAKA/Luottamusverkosto

CSC. n.d. VIRTA-opintotietopalvelu. Viitattu 29.5.2025. https://wiki.eduuni.fi/spaces/CSCVIRTA/pages/75754013/VIRTA-opintotietopalvelu

Cyber Citizen. 2024. Cyber Citizen -hanke. Aalto-yliopisto. Viitattu 10.6.2024. https://cyber-citizen.eu

CySec4Psych. 2023. COM-B Model. Viitattu 4.4.2025. https://cysec4psych.eu/psych-cyber-concept/com-b-model/

CySec4Psych. n.d. Psychological Theory and Construct Finder. Viitattu 10.5.2025. https://cysec4psych.eu/psychological-theory-and-construct-finder/

eduGAIN. 2024. The eduGAIN interfederation service. Viitattu 9.6.2024. https://edugain.org

Euroopan parlamentin ja neuvoston asetus 2014/376. Euroopan parlamentin ja neuvoston asetus (EU) N:o 376/2014, annettu 3 päivänä huhtikuuta 2014 , poikkeamien ilmoittamisesta, analysoinnista ja seurannasta siviili-ilmailun alalla, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 996/2010 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2003/42/EY, komission asetusten (EY) N:o 1321/2007 ja (EY) N:o 1330/2007 kumoamisesta

Euroopan parlamentin ja neuvoston asetus 2016/679. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

Euroopan parlamentin ja neuvoston direktiivi 2022/2555. Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi)

FUCIO. 2023. Tietoturvakoulutus- ja testauskysely 2023: Tuloksia.

FUCIO. 2024. Suomalaisten korkeakoulujen tietohallintojohtajien IT-barometri 2024. Viitattu 29.5.2024. https://tt.eduuni.fi/sites/kity/publicAAPAFUCIOdocs/FUCIOAAPA-2024-IT-barometri.pdf

GÉANT. 2024a. GÉANT Security Baseline 1.2.1. Viitattu 6.1.2025. https://security.geant.org/wp-content/uploads/2024/11/GEANT-Security-Baseline-v1.2.1.pdf

GÉANT. 2024b. Join us for the second GÉANT Security Awareness Community Workshop on 12 November – Online. Viitattu 29.5.2025. https://connect.geant.org/2024/10/11/join-us-for-the-second-geant-security-awareness-community-workshop-on-12-november-online

Gynther, V. 2023. Tietoturvakoulutuksen kehittämisen tilanne. Viitattu 29.5.2024. https://www.it2023.fi/puhujat/#vesa-gynther

Hakkarainen, J. 2018. Helsingin yliopistoa riivaa poikkeuksellisen suuri kalaste-luviestien tulva – satoja ihmisiä on haksahtanut antamaan tietonsa rikollisille.

Helsingin Sanomat. Viitattu 29.5.2024. https://www.hs.fi/pkseutu/art-2000005805242.html

Helsingin yliopisto. 2022. Lukkiutuiko käyttäjätunnuksesi? Syynä voi olla tekemätön yliopistolaisen tietoturvatesti. Viitattu 6.10.2024. https://helpdesk.it.helsinki.fi/uutiset/lukkiutuiko-kayttajatunnuksesi-syyna-voi-olla-tekematon-yliopistolaisen-tietoturvatesti

Helsingin yliopisto. 2021. Opiskelijan digitaidot -opintojakso. Viitattu 10.6.2024. https://blogs.helsinki.fi/opiskelijan-digitaidot/2021/05/28/materiaalin-lukuohje/

Hielscher, J.; Menges, U.; Parkin, S.; Kluge, A. & Sasse, M.A. 2023. “Employees Who Don’t Accept the Time Security Takes Are Not Aware Enough”: The CISO View of Human-Centred Security. 32st USENIX Security Symposium (USENIX Security 23). USENIX Association, Anaheim, CA. 2311–2328. https://www.usenix.org/system/files/usenixsecurity23-hielscher.pdf

Ho, G.; Mirian, A.; Luo, E.; Tong, K.; Lee, E.; Liu, L.; Longhust, C.; Dameff, C.; Savage, S. & Voelker, G. 2025. Understanding the Efficacy of Phishing Training in Practice. 2025 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, Los Alamitos, CA, USA. https://doi.ieeecomputersociety.org/10.1109/SP61157.2025.00076

Huoltovarmuuskeskus. 2018. Kyberturvallisuuden sanasto. Helsinki: Sanastokeskus TSK.

Hämäläinen, V-P. & Tuominen S. 2017. Joku julkaisi 16 000 suomalaisen henkilötunnukset netissä kuusi vuotta sitten – nyt niillä tehtaillaan tuhansia rikoksia vuodessa. Yle. Viitattu 29.5.2024. https://yle.fi/a/3-9914817

ISO/IEC 27001:2023. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardoimisliitto SFS.

ISO/IEC 27002:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Suomen Standardoimisliitto SFS.

ISO/IEC 27004:2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. Suomen Standardoimisliitto SFS.

Keuda. 2023. Keudan loppuraportti kyberhyökkäyksestä on valmistunut. Viitattu 29.5.2024. https://www.keuda.fi/2023/03/10/keudan-loppuraportti-kyberhyokkayksesta-on-valmistunut/

KnowBe4. n.d. Gain Insight Into Where Your Organization Stands With the Security Culture Maturity Model. Viitattu 21.4.2025. https://www.knowbe4.com/security-culture-maturity-model

Kondruss, B. 2024. Cyber attacks on universities. Viitattu 29.5.2024. https://konbriefing.com/en-topics/cyber-attacks-universities.html

Kruger, H. A. & Kearney, W. D. 2006. A prototype for assessing information security awareness. Computers & Security. Volume 25, Issue 4. 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kybermittari-arviointityökalu 2.1. Kyberturvallisuuskeskus. Viitattu 3.6.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittarin%20arviointityökalu_v2.1_20240507_web.xlsx

Kyberturvallisuuskeskus. 2024a. Kybermittari. Viitattu 1.6.2024. https://kybermittari.fi

Kyberturvallisuuskeskus. 2024b. Mitä NIS2-direktiivissä esitetyt kyberhygieniakäytännöt ovat? Viitattu 26.1.2025. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mita-nis2-direktiivissa-esitetyt-kyberhygieniakaytannot-ovat

Kyberturvallisuuskeskus. 2019. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Viitattu 4.6.2024. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri

Kärkkäinen, H. 2021. Sähköposti-isku Oulun yliopistoon, 900 salasanaa vääriin käsiin – ylläpidolta uhreille käsittämätön viesti. Digitoday. Viitattu 29.5.2024. https://www.is.fi/digitoday/tietoturva/art-2000008235534.html

Lain, D.; Kostiainen, L. & Čapkun S. 2022. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. IEEE Symposium on Security and Privacy. https://doi.org/10.48550/arXiv.2112.07498

Laki digitaalisten palvelujen tarjoamisesta 15.3.2019/306.

Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906.

Manninen, O.; Karjalainen M.; Levänen, M.; Pensar U. & Wennström J. 2013a. Henkilöstön tietoturvaopas. Viitattu 29.5.2024. https://tt.eduuni.fi/sites/kity/publicSECmaterial/henkiloston-tietoturvaopas.pdf

Manninen, O.; Karjalainen M.; Levänen, M.; Pensar U. & Wennström J. 2013b. Opiskelijan tietoturvaopas. Viitattu 29.5.2024. https://www.jyu.fi/digipalvelut/fi/ohjeet/tietoturva/lisatietoja-ja-linkkeja_opiskelijan-tietoturvaopas

Michie, S; van Stralen MM & West R. 2011. The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implement Science. Vol. 6, Article 42. https://doi.org/10.1186/1748-5908-6-42

NCSC. 2017. Growing positive security cultures. Viitattu 12.4.2025. https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

NCSC. 2018. Phishing attacks: defending your organisation. Viitattu 15.5.2025. https://www.ncsc.gov.uk/guidance/phishing

NCSC. 2019. You shape security: A positive security culture. Viitattu 4.4.2025. https://www.ncsc.gov.uk/collection/you-shape-security/a-positive-security-culture

NCSC. 2021. 10 Steps to Cyber Security: Engagement and Training. Viitattu 4.4.2025. https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training

NCSC. 2024a. Cyber Assessment Framework V3.2. Viitattu 9.11.2024. https://www.ncsc.gov.uk/files/Cyber%20Assessment%20Framework%20V3.2.pdf

NCSC. 2024b. Cyber Assessment Framework. Viitattu 6.1.2025. https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b6-staff-awareness-and-training

NIST. n.d. Glossary: Awareness. NIST Computer Security Resource Center. Viitattu 1.3.2025. https://csrc.nist.gov/glossary/term/awareness

NIST SP 800-50 Rev 1. 2024. Building a Cybersecurity and Privacy Learning Program. https://doi.org/10.6028/NIST.SP.800-50r1

NIST SP 800-53 Rev 5. 2020. Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5

NIST SP 800-63B Second Public Draft of Revision 4: Authentication & Authenticator Management. Viitattu 18.5.2025. https://pages.nist.gov/800-63-4/sp800-63b.html#password

NIST CSF 2.0. 2024. The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

NIST. 2024b. NIST CSF 2.0 Implementation Examples. Viitattu 3.6.2024. https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf

NPSA. 2023. Embedding Security Behaviours: using the 5Es. Viitattu 31.3.2025. https://www.npsa.gov.uk/system/files/documents/npsa-embedding-security-behaviours-using-5es_0_0.pdf

Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M. & Jerram, C. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, Volume 42. 165–176. https://doi.org/10.1016/j.cose.2013.12.003

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. Computers & Security. Volume 66. 40–51. https://doi.org/10.1016/j.cose.2017.01.004

REFEDS. 2022. eduPerson (202208) v4.4.0. Viitattu 10.5.2025. https://wiki.refeds.org/display/STAN/eduPerson+%28202208%29+v4.4.0

REFEDS. 2023. REFEDS Assurance Framework version 2.0. Viitattu 12.10.2024. https://refeds.org/wp-content/uploads/2023/12/RAF-2.0-Final-version.pdf

Reinfelder, L.; Landwirth, R. & Benenson, Z. 2019. Security Managers Are Not The Enemy Either. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 433. 1–7. https://dl.acm.org/doi/10.1145/3290605.3300663

Richter, S.; Straub, T. & Lucke C. 2018. Information Security Awareness – eine konzeptionelle Neubetrachtung. Viitattu 24.5.2025. https://www.researchgate.net/publication/323827248_Information_Security_Awareness_-_eine_konzeptionelle_Neubetrachtung

Saltzer, J. H. & Schroeder, M. D. 1975. The protection of information in computer systems. Proceedings of the IEEE. Vol. 63, no. 9, 1278–1308. https://doi.org/10.1109/PROC.1975.9939.

Salomaa, M. 2024. Helsingin yliopisto alkoi seuloa tohtori-opiskelijoita kaupallisella kyvykkyys-testillä – kanslerilta kovaa kritiikkiä. Helsingin Sanomat. Viitattu 21.5.2025. https://www.hs.fi/helsinki/art-2000010921090.html

SANS. 2024. SANS 2024 Security Awareness Report. Viitattu 17.8.2024. https://www.sans.org/mlp/ssa-2024-security-awareness-report/

SANS. 2025. SANS Security Awareness Maturity Model eBook. Viitattu 22.2.2025. https://www.sans.org/mlp/ssa-ebook-maturity-model/

Savonia. 2022. Savoniaan on kohdistunut tietoturvahyökkäys. Viitattu 29.5.2024. https://www.savonia.fi/uutiset/savoniaan-on-kohdistunut-tietoturvahyokkays/

Schneier, B. 2003. Beyond Fear: Thinking sensibly about security in an uncertain world. New York: Copernicus Books.

Seesto, T. 2023. Sähköposti. FUCIO:n pääsihteerin sähköposti 30.1.2023.

SIRTFI v2. 2022. A Security Incident Response Trust Framework for Federated Identity (Sirtfi) Version 2. REFEDS. Viitattu 9.6.2024. https://refeds.org/wp-content/uploads/2022/08/Sirtfi-v2.pdf

Snyder, J. 2022. Hyppönen's Law: If It's Smart, It's Vulnerable. Viitattu 1.6.2024. https://www.horangi.com/blog/hypponen-law-if-its-smart-its-vulnerable

Sophos. 2024. The State of Ransomware in Education 2024. Viitattu 12.10.2024. https://assets.sophos.com/X24WTUEQ/at/tq459xbt9qm8nm3t6q8px48/sophos-state-of-ransomware-education-2024-wp.pdf

Stikvoort, D.; Kossakowski K-P. & Maj M. 2023. SIM3 v2 interim – Security Incident Management Maturity Model. Viitattu 19.1.2025.

https://opencsirt.org/wp-content/uploads/2023/11/SIM3_v2_interim_standard.pdf

Stoll, C. 1990. The cuckoo’s egg: tracking a spy through the maze of computer espionage. New York: Pocket Books.

Petrosyan, A. 2024. Average duration of downtime after a ransomware attack at organizations in the United States from 1st quarter 2020 to 2nd quarter 2022. Statista. Viitattu 9.6.2024. https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-us/

Tampereen yliopisto. 2024. Käyttäjätunnus ja salasana. Viitattu 29.9.2024. https://www.tuni.fi/fi/it-palvelut/kasikirja/kayttajatunnukset-ja-salasanat/kayttajatunnus-ja-salasana#tietoturvakoulutus

Thomson, M.E. & von Solms, R. 1998. Information security awareness: educating your users effectively. Information Management & Computer Security. Vol. 6, No. 4, 167–173. https://doi.org/10.1108/09685229810227649

Tiedonhallintalaki 9.8.2019/906.

Tietoturva 24/7. 2024. Tietoturva 24/7 -verkkokurssi. Laurea-ammattikorkeakoulu. Viitattu 10.6.2024. https://www.laurea.fi/ajankohtaista/uutiset/tietoturva-247-verkkokurssi-heraa-tietoturvaan/

Traficom. 2022. Just culture - oikeudenmukainen kulttuuri. Viitattu 19.4.2025. https://www.traficom.fi/fi/liikenne/ilmailu/just-culture-oikeudenmukainen-kulttuuri

Traficom. 2025. Määräykset ja säädökset. Viitattu 16.2.2025. https://traficom.fi/fi/saadokset?group=kyberturvallisuus&kyberturvallisuus=initial&limit=20&offset=0&query=&saadoksentyyppi=%255B12%255D&sort=created

Traficom. 2024. Viestintä: Määräys teletoiminnan tietoturvasta. TRAFICOM/248815/03.04.05.00/2022. https://www.finlex.fi/fi/viranomaiset/normi/480001/50299

Turun yliopisto. 2024a. Opiskelijamäärien tilastot. Viitattu 2.11.2024. https://www.utu.fi/fi/opiskelutilastot/opiskelijamaarat

Turun yliopisto. 2024b. Vuosikertomus 2023: Hyvinvoiva yhteisö. Viitattu 2.11.2024. https://www.utu.fi/fi/yliopisto/vuosikertomus-2023/hyvinvoiva-yhteiso

Valtionvarainministeriö. 2023. Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri). http://urn.fi/URN:ISBN:978-952-367-458-5

Vestman, T. 2020. Kriittinen analyysi neutralisoimisteorian soveltamisesta tietojärjestelmätieteessä. Väitöskirja. Informaatioteknologian tiedekunta. Jyväskylä: Jyväskylän yliopisto. Viitattu 6.6.2024. http://urn.fi/URN:ISBN:978-951-39-8174-7

Vilander, J. 2021. Bridging the knowing-doing gap: The role of attitude in information security awareness. Maisterintutkielma. Informaatioteknologian tiedekunta. Jyväskylä: Jyväskylän yliopisto. Viitattu 8.3.2025. https://urn.fi/URN:NBN:fi:jyu-202105313312

Tietosuojalaki 5.12.2018/1050.

Ulkoministeriö. 2020. Katakri – tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 5.6.2024. https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Lantto, E. 2024. HE 57/2024 eduskunnalle NIS 2 -direktiivin täytäntöönpanoa koskevaksi lainsäädännöksi. Viitattu 26.1.2025. https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2024-AK-31375.pdf

Venables, P. 2024. Security Training & Awareness - 10 Essential Techniques. Viitattu 30.12.2024. https://www.philvenables.com/post/security-training-awareness-10-essential-techniques

Weinert, A. 2019. Your Pa$$word doesn't matter. Microsoft. Viitattu 15.5.2025. https://techcommunity.microsoft.com/blog/microsoft-entra-blog/your-paword-doesnt-matter/731984

Winkler, I & Brown T. 2021. You Can Stop Stupid: Stopping Losses from Accidental and Malicious Actions. Indianapolis: John Wiley & Sons Inc.

Yle. 2011. Itä-Suomen yliopiston henkilötietoja vuoti nettiin. Viitattu 29.5.2024. https://yle.fi/a/3-5449496

Yliopistolaki 24.7.2009/558

ZenGRC. 2024. Due Care vs Due Diligence: What Is the Difference? Viitattu 13.1.2025. https://www.zengrc.com/blog/due-care-vs-due-diligence-what-is-the-difference/

Åbo Akademi. 2024. IT help. Viitattu 29.9.2024. https://www.abo.fi/en/about-abo-akademi-university/it-help/#i-cant-log-in

Taulukko 7. NIST SP 800-53 Rev. 5: Awareness and training controls

CONTROL NUMBER	CONTROL NAME
AT-1	**Policy and procedures** a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and c. Review and update the current awareness and training: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Taulukko 7 (jatkuu).

Control Number	Control Name
AT-2	**Literacy training and awareness** a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes or following [Assignment: organization-defined events]; b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques]; c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.
AT-2(1)	Provide practical exercises in literacy training that simulate events and incidents.
AT-2(2)	Provide literacy training on recognizing and reporting potential indicators of insider threat.
AT-2(3)	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.
AT-2(4)	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].
AT-2(5)	Provide literacy training on the advanced persistent threat.

Taulukko 7 (jatkuu).

Control Number	Control Name
AT-2(6)	(a) Provide literacy training on the cyber threat environment; and (b) Reflect current cyber threat information in system operations.
AT-3	**Role-based training**
AT-3(3)	Provide practical exercises in security and privacy training that reinforce training objectives.
AT-3(4)	Suspicious communications and anomalous system behaviour. [Withdrawn: Moved to AT-2(4)]
AT-3(5)	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.
AT-4	**Training records** a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b. Retain individual training records for [Assignment: organization-defined time period].

Taulukko 7 (jatkuu).

AT-5	Contacts with security groups and associations. [Withdrawn: Incorporated into PM-15.]
AT-6	**Training feedback** Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].

Taulukko 8. NCSC Cyber Assessment Framework, B6.a: Cyber Security Culture

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
People in your organisation don't understand what they contribute to the cyber security of the essential function(s). People in your organisation don't know how to raise a concern about cyber security. People believe that reporting issues may get them into trouble. Your organisation's approach to cyber security is perceived by staff as hindering the business of the organisation.	Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation. All people in your organisation understand the contribution they make to the essential function(s) cyber security. All individuals in your organisation know who to contact and where to access more information about cyber security. They know how to raise a cyber security issue.	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations. People in your organisation raising potential cyber security incidents and issues are treated positively. Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure. Your management is seen to be committed to and actively involved in cyber security. Your organisation communicates openly about cyber security, with any concern being taken seriously. People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.

Taulukko 9. NCSC Cyber Asessment Framework, B6.b: Cyber Security Training

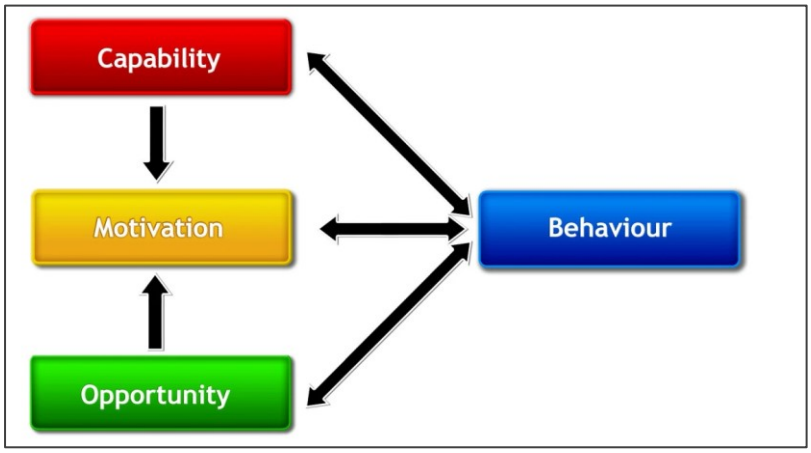
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
There are teams who operate and support your essential function(s) that lack any cyber security training. Cyber security training is restricted to specific roles in your organisation. Cyber security training records for your organisation are lacking or incomplete.	You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles. You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively. Cyber security information is easily available.	All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths. Each individuals cyber security training is tracked and refreshed at suitable intervals. You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective. You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.

Security Awareness Community Workshop – 12 November 2024

Task description

Brainstorm on an effective approach to encourage users to implement one of the key security behaviours below using the COM-B model for behavioural change:

- Creating secure passwords
- Using a password manager
- Using Multi Factor Authentication (MFA) for their accounts
- Locking their screen
- Reporting security incidents
-



Michie, S., van Stralen, M.M. & West, R. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Sci* **6**, 42 (2011). https://doi.org/10.1186/1748-5908-6-42

COM-B	
Motivation Why should the behaviour be changed?	
Capability Which skills are needed to implement the behaviour?	
Opportunity Which opportunities and tools support and prompt the behaviour?	

	Questions	Answers
Goal	What is to be achieved?	
Target group	Who is the target group?	
Key messages (motivation)	Why is this behaviour important?	
Benefit (What's in it for me?)	What advantages does the behaviour have for the target group? What are the consequences of non-compliance?	
Communication channels	Which channels are used to spread the message?	
Training measures (capability)	What training is offered to learn, repeat and consolidate the behaviour?	
Opportunities	What tools/processes are provided to facilitate behaviour?	

Taulukko 10. Security Awareness Maturity Modelin tasokuvaukset. (SANS 2025)

Security Awareness Maturity Model Indicators Matrix

This matrix details each of the stages of the maturity model, identifies which stage your organization is in, the value of the stage, and how to achieve the next stage. Leverage this matrix as a strategic planning guide for your approach to managing and measuring your organization's human risk. For more information and free resources, visit **sans.org/security-awareness-training**.

Maturity Level	Description	Program Indicators	People Indicators	Time to Achieve	Metrics	Steps to Next Level
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 of failing to meet 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.	N/A	None	• Identify the regulations or standards that you must adhere to. • Identify security awareness requirements for those standards. • Identify someone to roll out the required security awareness training. • Develop or purchase training that meets those requirements. • Deploy security awareness training. • Track and document who completes the training.
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 its human risk. In some circumstances this stage can be the most dangerous, as leadership perceives the organization is effectively managing its human risk, but it is not.**	• Program is led by someone who is only dedicated part-time to the security awareness efforts. • Security awareness reports to GRC, compliance, audit, legal or human resources. • 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. • There is little coordination or partnership with other departments, such as communications and human resources. • Leadership perceives security as purely a technical issue. • Training is primarily once a year, often mandatory. • 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 perceive security as something that the IT or security team takes care of—it's not their problem. • People feel security is something they have to do. • People have a negative perception of the security team, which is perceived as arrogant, too technical or perhaps even blockers. • People perceive security policies as confusing, difficult and as a blocker to their daily work responsibilities. • People often ignore policies and use their own solutions to get work done.	It depends on the standards, regulations or legal requirements you are attempting to adhere to. However, the overall effort is usually minimal, often requiring nothing more than annual training.	• Number/percentage of people that have completed training • Number/percentage of people that have signed Acceptable-Use Policy • Number of on-site training sessions in one year • Number/frequency of awareness materials distributed (newsletters, posters, webcasts, etc.)	• Identify and gain support of key leaders and stakeholders • Create Project Charter, identifying things such as scope, leadership, goals, objectives, assumptions, and constraints for the awareness program. • Identify who will be responsible for the awareness program. To ensure greatest success, that person should be dedicated full-time, have strong people skills, and report to and be part of the security team and report to the CISO. • Identify the top human risks you will need to manage. Coordinate with Incident Response team, Security Operations Center, and/or Cyber Threat Intelligence team to assist with this. This may also require some type of human risk assessment. • Identify the key behaviors that will mitigate and manage the top human risks. • Plan how you will communicate to, engage, and train your workforce on these key behaviors. • Develop, resource and/or purchase your training materials and platform to include Learning Management System or a Human Risk Management platform. • Create execution plan with milestones to include metrics.
STAGE 3 **Promoting Awareness and Behavior Change**	The program identifies the the top human risks to the organization and the behaviors that manage those risks. The program goes beyond just annual training and includes continual reinforcement throughout the year. More mature programs in this stage identify additional roles, departments, or regions that represent unique risks that require additional or specialized role-based training. Content is communicated in an engaging and positive manner that encourages behavior change. As a result, people understand their role in cybersecurity, follow organizational policies and exhibit key behaviors to secure the organization. **VALUE: Your organization is not only meeting its compliance requirements but is able to effectively identify, manage, and measure its human risk.**	• The program is led by someoned dedicated full-time to managing the security awareness program. In addition, this individual often has strong communication/people skills. • Security awareness reports to and is an integrated part of the security team. • Leadership understands and commits to the need for managing human risk. • There is a strategic plan that has identified the scope, goals, objectives, and justification for the program. • Through a risk assessment and in partnership with different security team members (DFIR, SOC, CTI), the security team has identified and can explain the organization's top human risks and the behaviors that most effectively manage those risks. • The program has sufficient leadership support to provide resources necessary and has an executive champion. • The Security Awareness team actively partners and collaborates with various departments within the organization, including communications, human resources, and help desk. • The program goes beyond just annual training and includes continuous reinforcement throughout the year. • More mature programs have identified different departments, roles, or regions that represent increased or unique risks to the organization and require specialized or additional training (role-based training). • The program works to positively engage the workforce. Engagement is not based on mandatory training but creating training that people want to consume.	• Employees understand that technology alone cannot protect them and they have a responsibility to protect themselves and the organization. • People are reporting incidents or suspected attacks. • When the security team pushes out information, people are asking them questions. • Employees are exhibiting the behaviors they are being trained on. • Employees begin to exhibit the same strong security behaviors at home and in their pesonal lives. • Employees are asking how their family can take the training.	Depending on the behaviors you are attempting to change, you can begin impacting behaviors organization-wide within 3–6 months. However, the more behaviors you are attempting to change, the longer it can take to change those behaviors organization-wide. This is one of the reasons it is so important to prioritize your top human risks, and the behaviors that manage those risks. The fewer behaviors you focus on, the more likely you can change those behaviors.	This stage is all about measuring the behaviors you care about and which behaviors are the most important to managing your risk. Some examples include: • Phishing simulation click rates, number of repeat clickers and report rates • Number of lost or stolen laptops or mobile devices • Adoption rate of Password Managers or MFA • Percentage of employee passwords that could be cracked • Percentage of workstations that are securely locked down at night • Percentage of mobile devices that are current and/or screenlocks enabled • Number of accidental data loss events, such as data loss due to auto-complete in email or insecure cloud accounts. **NOTE: See the interactive metrics matrix for more examples. These metrics are ultimately driven by what behaviors are the most important to managing your human risk.**	• Establish a process to give leadership regular updates on the awareness program. • Identify a specific date when the security awareness program is reviewed and updated every year. • During annual review and update, identify any new risks or behaviors required to manage human risk and new ways to communicate to, engage, and train your workforce. • The security awareness team should partner with audit, compliance, or GRC and actively assist with policy development to help ensure they are as simple as possible for the workforce. • The Security Awareness team should be actively assisting the Security team in any outreach, communication and engagement efforts to include any new tool rollouts. • Establish some type of formal incentive program to recognize individuals, groups, or departments excelling in cybersecurity and/or exhibiting key behaviors.
STAGE 4 **Long-Term Sustainment and Culture Change**	The program has the processes, resources, and leadership support in place for a long-term sustainment, including (at a minimum) an annual review and an update of the program. As a result, the program is an established part of the organization's culture and is current and engaging. The program has gone beyond changing behavior and is changing the workforce's shared attitudes, perceptions, and beliefs about cybersecurity. **VALUE: Your program has gone beyond impacting behavior and has started building a strong security culture. By security culture, we mean your workforce's shared attitudes, perceptions, and beliefs about cybersecurity. A strong security culture not only creates an environment where people are far more likely to exhibit secure behaviors, but promotes and helps ensure security is built into almost all operational aspects of the organization, exponentially increasing the overall security of the organization.**	• The program is led by someone dedicated full-time to managing the security awareness program and has a team of multiple full-time employees focusing on managing human risk. • Security awareness reports directly to the Chief Information Security Officer (CISO). • Program is actively reviewed and updated on an annual basis. • Leadership believes in and has invested in long-term support of the program. The program lead is regularly updating leadership on a monthly or quarterly basis. • Security team believes in investing in human controls equally as much as technical controls. There is a strong partnership between the security awareness team and different elements of the security team (SOC, DFIR, CTI, etc.). • The security ambassador champions the program and is run by a dedicated program manager. • The Security Awareness team is assisting in the development of security policies, processes, and procedures to ensure they are easier to understand and comply with. • The Security Awareness team is assisting the Security team with all organization-wide security communications or security tool roll-outs ensuring that expectations are simple to understand and easy to use.	• Good security practices are baked into who we are and what we do. • Employees educate others on good security behaviors. • Employees start providing ideas or suggestions on how to improve security in the organization. • Employees or departments actively reach out to and request assistance or briefings by the Security team. • Department leads and teams request security reviews/audits. • The Security team and their security efforts are perceived as approachable, collaborative, and helpful by the workforce. (e.g., people feel safe reporting an incident, even when they know they caused it).	Impacting your organizational culture takes much longer than impacting behavior. Impacting culture can take 3–10 years depending on the size, complexity, and age of your organization and its culture (John Kotter, Leading Change). For this stage, we recommend not focusing on changing your organization's culture, but embedding security into and aligning with your organization's existing culture.	• Survey people's attitudes, perceptions, and beliefs towards information security (this can be broken down by what people think about your security policies, your Security team and your security training). • Conduct focus groups or interviews for deep dives into people's attitudes, perceptions, and beliefs • A number of people/departments are requesting security briefings or updates. • A number of people engaging the security team with questions or submitting ideas on how to improve security.	• Create a metrics dashboard that combines all the information/measurements from the different maturity levels. • Identify and align with leadership's strategic priorities. • Identify and align with any key strategic security frameworks or models.
STAGE 5 **Strategic Metrics Framework**	The program has a robust metrics framework aligned with and supporting the organization's mission and business goals. The program is no longer just measuring and reporting on changes in behavior and culture, but ultimately how these changes are reducing risk and enabling leadership to achieve their strategic priorities. As a result, the program is continuously improving and able to demonstrate return on investment. **VALUE: Your program is aligned with and actively supporting your leadership's strategic priorities and your organization's business goals/mission.**	• The Security Awareness team works with business leaders to identify and align with their strategic business priorities. • Metrics are collected on a regular basis, often automated. • Metrics are provided to senior leadership demonstrating value at a business level and showing alignment with strategic business priorities. • Metrics are aligned with the security framework(s) that your leadership has committed to, such as NIST Cybersecurity Framework or CIS Critical Controls. • Different types of metrics are delivered to different target audiences. • You have the ability to benchmark your program's maturity against peer organizations in your industry.	Leadership actively requests and uses security awareness metrics to measure their organizational progress and/or compare departments across the organization.	This is a long-term effort aligned with your overall program, as you are continually updating and improving your ability to collect useful metrics that you can both act on and provide to leadership.	• A metrics dashboard that tracks the key metrics covered in the previous stages. In some cases, a Human Risk Management platform may be used to automate the collection and display of these metrics. • How these changes are impacting and reducing overall risk to the organization, which can be measured in strategic metrics such as: – Overall number of security incidents – Average time to detect an incident (attacker dwell time) – Average time to recover from an incident – Number of policy, audit, or compliance violations In addition, show leadership how the awareness program is aligned with and enabling strategic goals in any strategic security frameworks, like the NIST CSF.	SANS SECURITY AWARENESS SANS CYBERSECURITY LEADERSHIP

Taulukko 11. Security Culture Maturity Modelin tasoarviointiin käytetyt indikaattorit. (Carpenter & Roer 2022)

Security Awareness Training	**Phishing & Simulated Phishing Testing**	**Behavioral Data**	**Organizational Tone and Activities**	**Survey Data**	**Other Measurement Data**
Frequencency of training campaigns Delivery types (in person, online, mobile, etc.) Content types used Learning modules taken Measured areas of strength or weakness Customization/personalization for the organization and their unique risks Customization/personalization for the individual based on role/department	Opened Clicked Attachment open Data entered on a landing page Exploited: user clicked on an Exploit enabled test Macro enabled: macro on an attachment was enabled Replied Reported Accuracy of reporting Organizational patterns of use for phishing simulations (e.g., customization of templates, gamification, etc.)	Tracking & Reporting of simulated or real-world user behavior alerts Documented policies for user behavior failures (stick) or high performance in testing/self-reporting (carrot) Technology/Integration into real-world behavior alerts Gamification	Company-wide communications regarding security policies Executive-led discussion around security policies Presence/absence of Security Championship Program Reward and Contest regarding security behavior and culture including company-wide milestones, etc. Security-centric special events	Culture Survey Data • Attitudes • Behavior • Cognition • Communication • Compliance • Norms • Responsibility Proficiency Assessment Data • Passwords & Authentication • Email security • Internet use • Social media • Mobile devices • Incident reporting • Security Awareness Others as desired	Phish-prone percentage Industry Benchmarks Virtual Risk Officer information Email Exposure Check Data API integration with other tools