Roni Mertenheimo

TIETOTURVAKÄYTÄNNÖT TURVALLISUUSSTRESSIN AIHEUTTAJANA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Mertenheimo, Roni
Tietoturvakäytännöt turvallisuusstressin aiheuttajana
Jyväskylä: Jyväskylän yliopisto, 2022, 83 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tietoturvakäytänteet muodostavat organisaatioiden tietoturvan ja tietoturvakulttuurin perustan. Ne tukevat organisaatioiden liiketoimintatavoitteiden saavuttamista, ohjaavat henkilöstön tietoturvakäyttäytymistä ja toimivat tietoturvan kommunikointivälineenä. Tietoturvakäytänteet ja niiden noudattaminen voidaan kuitenkin kokea kuormittavaksi, josta aiheutuvaa stressiä kutsutaan turvallisuusstressiksi. Aikaisemmassa turvallisuusstressin ja tietoturvakäyttäytymisen tutkimuksessa IT-alan työntekijät ovat selvästi olleet aliedustettuina, sillä tutkimus on kohdistunut muihin ammattialoihin. Kirjallisuuskatsauksen perusteella aikaisemmassa tutkimuksessa ei myöskään ole tunnistettu, millaiset tietoturvakäytänteet työntekijät kokevat kaikista stressaavimmiksi. Tutkielman tavoitteena oli saada vastauksia näihin tutkimusaukkoihin ja parantaa ymmärrystä suomalaisten IT-alan työntekijöiden kokemasta turvallisuusstressistä. Työntekijöiden mielipiteitä ja kokemuksia tietoturvakäytänteiden stressaavuudesta selvitettiin laadullisten teemahaastatteluiden avulla ja aineiston analysointimenetelmänä toimi teemoittelu. Tuloksien mukaan työntekijät kokevat etenkin salasanoihin, tietoturvateknologioihin, arkaluonteiseen tietoon ja laitteisiin liittyvät tietoturvakäytänteet ylikuormittavina, sillä ne yhtäaikaisesti lisäävät runsaasti työmäärää ja vähentävät työtehtäviin käytettävissä olevaa aikaa. Osa stressaavista tietoturvakäytänteistä myös koettiin monimutkaisina, sillä niitä koskevat ovat puutteellisia, vaikeaselkoisia tai hankalia ymmärtää.

Asiasanat: tietoturvakäytänteet, tietoturvakäyttäytyminen, turvallisuusstressi, stressi

ABSTRACT

Mertenheimo, Roni
Information Security Policies as the Creator of Security-Related Stress
Jyväskylä: University of Jyväskylä, 2022, 83 pp.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

Information security policies form the foundation of organizations' information security and information security culture. They support organizations in achieving their business goals, guide the information security behavior of the employees, and function as a communication tool for information security. However, information security policies and complying with them can be experienced as straining and the stress caused by it is called security-related stress. The previous research on information security behavior and security-related stress has focused mainly on non-IT employees, leaving the IT employees underrepresented. Additionally, according to literature review, it has not been identified what kind of information security policies the employees experience as the most stressing. The goal of this thesis was to find out answers to these gaps in the previous research and gain better understanding in what the most stressing information security policies for Finnish IT employees in the IT sector are. The experiences and opinions of the employees regarding information security policies were investigated using qualitative theme interviews and the interview material was analyzed with thematic methods. It was found out that especially policies related to passwords, information security technologies, sensitive information, and devices are experiences as overloading because they simultaneously increase the amount of work and decrease available work time for other work tasks. Some of the stressing information security policies were also experiences as complicated because they are insufficient or hard to understand.

Keywords: information security policy, information security behaviour, security-related stress, stress

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Organisaatioiden tietoturvaan kohdistuva suurin riski on yleensä ihminen, eli yrityksen työntekijä, joka aiheuttaa tietoturvalle riskejä joko tahattomalla tai tahallisella toiminnallaan. Riskeillä voi toteutuessaan olla suuria haittavaikutuksia, kuten esimerkiksi organisaatiovastuun menettäminen tai taloudelliset vahingot. Tämän vuoksi organisaatiot suunnittelevat ja toteuttavat tietoturvakäytänteitä, joiden noudattamista yleensä myös valvotaan. Tietoturvakäytänteet ovat organisaatioiden luomia ja dokumentoimia sääntöjä, käytänteitä ja vastuita, joita työntekijöiden tulee noudattaa yrityksen tieto- ja teknologiaresurssien turvallisuuden varmistamiseksi. Tietoturvakäytänteet ehkäisevät organisaatioiden tietoturvaan kohdistuvia riskejä tarjoamalla toimintamalleja hyvistä tietoturvaan liittyvistä käytänteistä sekä kieltävät tietoturvaa uhkaavat toimintatavat. (Bulgurcu, Cavusoglu & Benbasat, 2010.) Tietoturvakäytänteet lisäksi ohjaavat organisaation työntekijöiden tietoturvakäyttäytymistä, tukevat organisaation strategiaa ja toimivat tietoturvakulttuurin perustana (Paananen, Lapke & Siponen, 2020).

Tietoturvakäytänteet ja niiden noudattaminen voivat kuitenkin aiheuttaa työntekijöille stressiä, mikäli ne tai niiden noudattaminen koetaan liian paljon aikaa vieväksi tai vaikeaselkoiseksi. Tietoturvakäytänteiden noudattamisesta aiheutuvaa stressiä kutsutaan turvallisuusstressiksi, jonka D'Arcy, Herath ja Shoss (2014) määrittelivät teknostressin määritelmän pohjalta. Turvallisuusstressillä on kolme stressitekijää, jotka ovat ylikuormitus, monimutkaisuus ja epävarmuus. Työntekijät saattavat joutua käyttämään ylimääräistä aikaa tietoturvakäytänteiden opetteluun toimiakseen tietoturvakäytänteiden mukaisesti, tai tietoturvakäytänteiden dokumentaatio ei ole selkeää esimerkiksi ammattisanaston tai jargonin takia. Tietoturvakäytänteet voivat myös muuttua usein, joka aiheuttaa työntekijöille stressiä niiden epävarmuuden takia. Tietoturvakäytänteiden noudattamisesta aiheutuva stressi voi altistaa työntekijät käyttämään erilaisia selviytymis- ja neutralisaatiomekaniikoita, joiden avulla he lieventävät kokemaansa stressiä. Tällainen käyttäytyminen johtaa usein tietoturvakäytänteiden noudattamatta jättämiseen tai niiden rikkomiseen. (D'Arcy ym., 2014.) Turvallisuusstressi voi myös aiheuttaa työntekijöissä turhautuneisuutta ja väsymystä (D'Arcy & Teh,

2019) tai joissain tapauksissa jopa loppuun palamista (Pham, Brennan & Furnell, 2019).

Turvallisuusstressin aihepiiristä on tehty vasta kourallinen tutkimuksia, joten aiemmasta tutkimuksesta voidaan tunnistaa joitakin tutkimusaukkoja. Turvallisuusstressiin liittyvässä kirjallisuudessa ei ensinnäkään vaikuttaisi olevan tunnistettu, millaiset tietoturvakäytänteet organisaatioiden työntekijät kokevat kaikista kuormittavimmiksi ja miksi. Toiseksi tietoturvakäyttäytymisen ja turvallisuusstressin tutkimuskohderyhmänä on ollut lähes poikkeuksetta muut ammattiryhmät, kuin IT-alan ammattiryhmät. Tämän vuoksi tutkielman kohderyhmäksi valittiin nimenomaan IT-alan työntekijät. Tutkielman tarkoituksena on saada vastauksia näihin kahteen tutkimusaukkoon laadullisin menetelmin, eli siis tutkia, millaiset tietoturvakäytänteet suomalaiset IT-alan työntekijät kokevat stressaaviksi. Tutkielma pyrkii myös selvittämään esille tulleiden turvallisuusstressiä aiheuttavien tietoturvakäytänteiden stressaavuuden syyt, eli miksi ne koetaan stressaaviksi. Tutkielmalle määritettiin kaksi tutkimuskysymystä tutkimusaukkojen pohjalta, jotka ovat:

1. *Millaiset tietoturvakäytänteet suomalaiset IT-alan työntekijät kokevat stressaaviksi?*
2. *Miksi ensimmäisen tutkimuskysymyksen tietoturvakäytänteet ovat stressaavia?*

Tutkielman aineistonkeruumenetelmäksi valittiin puolistrukturoidut teemahaastattelut ja aineisto analysoitiin teemoittelun avulla. Tutkielman tavoitteena on pyrkiä ymmärtämään paremmin IT-alan työntekijöitä stressaavia tietoturvakäytänteitä ja lisäksi tunnistamaan esille tulleiden tietoturvakäytänteiden stressaavuuden syitä. Tutkielman tuloksia voidaan hyödyntää IT-alan organisaatioissa tietoturvakäytänteiden kehittämisen tukena sekä tietoturvakoulutuksien suunnittelun apuna. Tuloksien hyödyntäminen tietoturvakäytänteiden ja tietoturvakoulutuksien suunnittelun tukena voi vähentää työntekijöiden kokemaa turvallisuusstressiä, joka puolestaan edistää organisaatioiden kokonaisvaltaista tietoturvaa ja vähentää tietoturvakäytänteiden noudattamatta jättämisen tai rikkomisen riskiä. Tutkielman tuloksista on hyötyä myös työntekijöille, sillä he voivat pohtia omaa tietoturvakäyttäytymistään tuloksiin pohjaten ja tunnistaa, millaiset tietoturvakäytänteet he kokevat stressaavimpina.

Tämä tutkielma sisältää yhdeksän lukua. Johdantoluvussa käydään läpi tutkielman taustaa sekä motivoidaan tutkimus kirjallisuudesta löytyneiden tutkimusaukkojen avulla. Luvussa esitellään myös tutkielman tutkimuskysymykset. Luvun lopussa selitetään vielä tutkielman rakenne, kirjallisuuden valintakriteerit sekä kirjallisuuden etsinnässä käytetyt hakusanat.

Tutkielman kolme seuraavaa päälukua kattavat tutkielman kirjallisuuskatsauksen, joissa tarkastellaan tutkielman kannalta relevanttia tutkimuskirjallisuutta. Toisessa luvussa käsitellään tietoturvaa, tietoturvakäytänteitä sekä tietoturvakäytänteiden kehitysmetodeja. Toisen luvun kirjallisuuden etsinnässä käytettyjä hakusanoja olivat ”information security”, ”information security policy”, ”information security policy development” ja ”ISP development”. Kolmannessa luvussa puolestaan käydään läpi työntekijöiden tietoturvakäyttäytymiseen

liittyviä asioita. Luvussa muun muassa esitellään tietoturvakäyttäytymisen tutkimuksessa yleisimmin käytetyt teoriat, tietoturvakäyttäytymiseen vaikuttavia tekijöitä sekä tietoturvakäyttäytymisen muuttumiseen liittyviä asioita. Kolmannessa luvussa käytetyt hakusanat olivat ”information security behavior”, ”information security policy compliance”, ”information security policy violation”, “ISP violation” ja “ISP compliance”. Neljännessä luvussa käydään läpi viimeinen teoriakokonaisuus, eli turvallisuusstressi. Luvussa esitellään ensin turvallisuusstressin määritelmä, jonka jälkeen tutustutaan sen tutkimuksessa käytettyihin yleisimpiin teorioihin ja viimeiseksi turvallisuusstressin tutkimuksen aikaisempiin tutkimustuloksiin. Luvussa käytetyt kirjallisuuden hakusanat olivat ””security-related stress”, ”SRS”, ”information security stress” ja ”information security policy stress”. Kirjallisuuskatsauksen teorialukuja seuraa viidennessä luvussa kirjallisuuskatsauksen yhteenveto, jossa käydään läpi kaikkien kolmen teemojen olennaisimmat asiat.

Kirjallisuuskatsauksen tutkimuskirjallisuutta haettiin pääasiassa tietojärjestelmätieteen tutkimuskirjallisuuden tunnetuista tietokannoista ja julkaisupaikoista, kuten Elsevieristä, Emerald Insightista, SAGE Journalista ja myös satunnaisesti Google Scholarista. Kirjallisuuskatsauksessa hyödynnettiin eniten laadukkaita tieteellisiä artikkeleita, mutta myös joitakin konferenssipapereita, kirjoja ja standardeja. Tutkimuskirjallisuuden tärkeimpänä valintakriteerinä oli laatu, joten kirjallisuuden valintaan vaikutti erityisesti julkaisija. Tutkimuskirjallisuutta valittiin tietojärjestelmätieteen laadukkaista ja arvostetuista lehdistä, kuten MIS Quaterly, Computers & Security, Information Systems Journal ja European Journal of Information Systems. Tutkimuskirjallisuuden laadun varmistamiseksi hyödynnettiin Julkaisufoorumin luokitusta 1–3, joihin valitun kirjallisuuden tuli kuulua. Valitun kirjallisuuden tuli olla myös vertaisarvioitua laadun varmistamiseksi. Toisena valintakriteerinä oli kirjallisuuden sisällön sopivuus kirjallisuuskatsauksen aiheisiin. Sisältö varmistettiin lukemalla ensin artikkeleiden tiivistelmät ja artikkelin aiheen ja näkökulman ollessa sopiva luettiin artikkeli kokonaisuudessaan.

Kuudennessa luvussa perehdytään tutkielman empiiriseen osaan eli tutkimusmenetelmien lukuun, jossa kerrotaan tutkielman tutkimusmenetelmän valinnasta, aineistonkeruumenetelmästä sekä aineiston analysointimenetelmästä. Luvussa käsitellään myös tutkimuksen reliabiliteettiin ja validiteettiin liittyviä tekijöitä. Seitsemäs luku sisältää tutkimuksen tulokset, joka alkaa haastateltavien taustatietojen esittelyllä. Luvussa esitellään haastateltavilta saadut vastaukset tutkielman tutkimuskysymyksiin nähden. Kahdeksannessa luvussa, eli johtopäätökset-luvussa, vastataan tutkielman tutkimuskysymyksiin, mietitään tutkielman kontribuutioita sekä tutkimukselle että käytännölle ja pohditaan tutkielman rajoitteita ja jatkotutkimusaiheita. Viimeinen luku on yhteenveto, jossa käydään läpi tutkielman olennaisimmat asiat. Lähdeluettelo sekä haastatteluissa käytetty haastattelurunko löytyvät tutkielman lopusta.

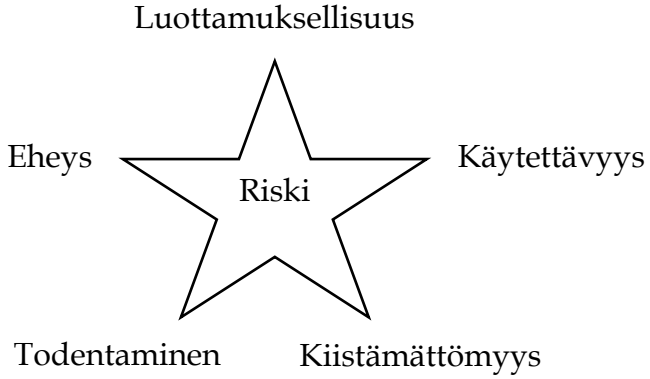
2 TIETOTURVAKÄYTÄNTEET

Tässä luvussa käydään läpi kirjallisuuskatsauksen ensimmäinen osa-alue, eli tietoturvakäytänteet. Luku on jaettu kolmeen alalukuun, joista ensimmäisessä käydään läpi tietoon ja tietoturvaan liittyviä asioita, kuten tiedon ominaisuudet. Toisessa alaluvussa tarkastellaan tietoturvakäytänteitä, niiden määritelmiä ja eri funktioita organisaatioissa. Viimeisessä alaluvussa käydään läpi tietoturvakäytänteiden kehittämistä ja luvussa esitellään kolme erilaista tietoturvakäytänteiden kehitysmetodia.

2.1 Tieto ja tietoturva

Tieto on määritelty tietoturvan kontekstissa yrityksen tärkeäksi omaisuudeksi, jota voidaan tallentaa sekä digitaalisen tallentamisen lisäksi myös muilla keinoilla (Calder & Watkins, 2010). Tietoturvalla puolestaan tarkoitetaan tiedon ja teknologiaresurssien suojaamista erilaisilta uhilta, kuten väärinkäytöltä, muuntelulta ja tuhoamiselta. Tietoturvaan liittyy olennaisesti CIA-kolminaisuuden käsite, joka tarkoittaa tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Nämä kolme tiedon ominaisuutta tulee aina täyttyä, jotta yritys voi saavuttaa tietoturvatavoitteensa. (Cabrera, Reyes & Lasco, 2020.) Tiedon luottamuksellisuus liittyy siihen, että tieto voi olla saatavilla vain valtuutetuille henkilöille, ja tiedon eheydellä tarkoitetaan tiedon tarkkuutta ja ettei se ole pirstaloitunutta. Tiedon saatavuudella tarkoitetaan puolestaan sitä, että tieto on saatavilla valtuutetuille henkilöille tarpeen tullen. (Calder & Watkins, 2010.) Tiedon ominaisuuksia voidaan kuvata myös tietoturvatähdellä (kuvio 1), joka on laajennettu versio CIA-kolminaisuudesta. Se ottaa huomioon saatavuuden, eheyden ja luottamuksellisuuden lisäksi myös tiedon aidoksi todistamisen ja kieltämättömyyden, sekä tähden ytimessä on riskit. Aidoksi todistamisella tarkoitetaan sitä, että tietoon pääsyä tavoittelevan henkilön identiteetti pystytään varmistamaan. Kieltämättömyys puolestaan viittaa siihen, että tiedon lähettäjä ja vastaanottaja ei voi kieltää osallistumistaan tiedon siirtotapahtumaan. Tietoturvatähden ytimessä olevilla

riskeillä kuvataan tietoon kohdistuvia riskejä, jotka liittyvät tähden sakaroiden viiteen tiedon ominaisuuteen. (Raggad, 2010.)



KUVIO 1 Tietoturvatähti (Raggad, 2010, s. 22)

2.2 Tietoturvakäytänteet

Tietoturvakäytänteet (engl. *information security policy, ISP*) ovat kokoelma sääntöjä ja vastuita, joilla yritykset pyrkivät turvaamaan tieto- ja teknologiaresurssinsa tietoturvan (Bulgurcu ym., 2010). Baskervillen ja Siposen (2002) mukaan tietoturvakäytänteille on useita erilaisia määritelmiä, joista osassa itse tietoturvakäytänteet ja niiden valvontamekanismit on eroteltu toisistaan. Toisissa määritelmissä puolestaan tietoturvakäytänteillä tarkoitetaan nimenomaan yleisiä sääntöjä tietoturvan varmistamiseksi, jotka eivät sisällä varsinaisia tietoturvaan liittyviä teknisiä ratkaisuja. Tietoturvakäytänteiden määritelmien suuren määrän vuoksi Baskerville ja Siponen (2002) ehdottivat tietoturvakäytänteiden kolmitasoista jaottelua, joka sisältää korkean tason käytänteet, matalan tason käytänteet ja metakäytänteet. Korkean tason käytänteet viittaavat yleisiin tietoturvakäytänteisiin, joista esimerkkinä ovat organisaatioiden johtoa ja työntekijöitä koskevat vastuut ja säännöt tietoturvan varmistamiseksi. Matalalla tasolla tarkoitetaan konkreettisimpia metodeja, jotka ohjaavat yrityksen tietoturvapäätöksiä. Matalan tason tietoturvakäytänteet sisältävät yrityksien tunnistamiin riskeihin liittyviä käytänteitä, kuten esimerkiksi salasanoihin ja niiden vaatimuksiin liittyvät tietoturvakäytänteet. Metakäytänteillä puolestaan tarkoitetaan olemassa olevien tietoturvakäytänteiden kehitykseen ja ylläpitoon liittyviä käytänteitä. Ne sisältävät myös tietoturvakäytänteiden käyttöönottoon ja niiden valvontaan liittyvät suunnitelmat. Metakäytänteiden hyödyntäminen korkean ja matalan tason tietoturvakäytänteiden rinnalla on oleellisen tärkeää tietoturvakäytänteiden yksilöimiseksi yrityksen tietoturvatarpeisiin ja -tavoitteisiin. (Baskerville & Siponen, 2002.)

Organisaatiot hyödyntävät toiminnassaan usein sertifiointeja ja standardeja laadukkaan toiminnan takaamiseksi. Tietoturvakäytänteisiin liittyy olennaisesti International Organization for Standardizationin (2018) (suom. *kansainvälinen*

standardoimisjärjestö) julkaisema standardi ISO/IEC 27001, joka määrittelee tietoturvan toteuttamiseen liittyvät vaatimukset. Standardi painottaa erityisesti tietoturvariskien hallintaa. Standardin pykälä 5.2 käsittelee tarkalla tasolla tietoturvaan olennaisesti liittyviä tietoturvakäytänteitä ja niiden vaatimuksia, ominaisuuksia sekä niihin liittyviä hyviä käytänteitä. Tietoturvakäytänteiden päätehtävänä on edistää ja suojata yrityksen tiedon ja siihen liittyvän omaisuuden luottamuksellisuus, eheys ja saatavuus. Tietoturvakäytänteiden tulee ensinnäkin määritellä yrityksen strategiset lähtökohdat, joihin yrityksen tietoturvatavoitteet perustetaan. Niiden tulee ottaa huomioon yrityksen tieto- ja teknologiaresurssien lisäksi myös liiketoiminnalliset piirteet. Yrityksen johdon on lisäksi arvioitava ja hyväksyttävä suunnitellut tietoturvakäytänteet. Yrityksen henkilöstöllä tulee olla vähintäänkin perustason ymmärrys tietoturvakäytänteiden käytännön soveltamisesta omassa työssään, jotta he pystyvät toimimaan niiden mukaisesti päivittäin sekä tietoturvarikkeen tapahtuessa. Standardi myös korostaa tietoturvakäytänteiden uudelleenarvioimisen tärkeyttä. Käytänteet tulee uudelleenarvioida vähintään vuosittain, mutta tilanteen vaatiessa ne voidaan uudelleenarvioida myös useammin. Kaikista tietoturvakäytänteiden muutoksista tulee informoida yrityksen henkilöstöä. (Calder & Watkins, 2010.)

Tietoturvakäytänteillä on organisaatioissa lukuisia tärkeitä tehtäviä ja toimintoja. Paananen, Lapke ja Siponen (2020) kokosivat yhteen tietoturvakäytänteiden piirteitä ja toimintoja tutkimusartikkelinsa kirjallisuuskatsausosiossa (taulukko 1). Tietoturvakäytänteiden piirteet ja toiminnot on luokiteltu kolmeen kategoriaan, joista ensimmäinen on organisaation ohjaus. Tietoturvakäytänteet ensinnäkin tukevat organisaatioiden liiketoimintatavoitteita määrittelemällä organisaatioille sopivat tietoturvaan liittyvät tavoitteet ja strategian. Niillä pystytään myös hallitsemaan henkilöstön tietoturvakäyttäytymistä ohjeistamalla organisaation työntekijöitä muun muassa erilaisiin tietoturvaprosesseihin ja teknologian käyttöön liittyvissä asioissa. Tietoturvakäytänteet myös määrittelevät organisaation teknologian ja informaation käyttöön liittyviä sääntöjä tietoturvan varmistamiseksi. Säännöt ja ohjeistukset toimivat työntekijöiden tehokkuuden ja tietoturvakäytänteiden noudattamisen mittaamisen perustana, ja tietoturvakäytänteiden tulisikin olla suunniteltu niin, että niiden noudattamista voidaan mitata. (Paananen ym. 2020.)

Toisena piirre- ja toimintokategoriana on toimija ja omaisuus, joka sisältää tietoturvakäytänteiden piirteinä subjektien ja objektien määrittelyn. Tässä kategoriassa siis määritellään, keille tietoturvakäytänteet on tarkoitettu noudatettavaksi ja minkä yritysomaisuuden tietoturvaa pyritään suojaamaan tietoturvakäytänteillä. Tietoturvakäytänteiden subjektien määrittelyistä selviää myös työntekijöiden vastuut ja toimivalta tietoturvan osalta. Osalla työntekijöistä voi olla tietoturvaan liittyviä erikoisvastuita ja -oikeuksia, kuten tietoturvakäytänteiden muuttaminen tai muiden työntekijöiden toimien hyväksyminen. Tietoturvakäytänteiden ei tulisi olla liian teknologiapainotteisia, mutta niiden tulisi antaa yleiskuva organisaatioiden informaatioon liittyvästä omaisuudesta, joka voi sisältää tietojärjestelmien, informaation ja datan kuvaukset. (Paananen ym., 2020.)

Kolmas kategoria, eli tietoturvaongelmiin valmistautuminen, kattaa useita osa-alueita riskien määrittelystä tietoturvakulttuurin rakentamiseen. Tietoturvakäytänteet toimivat kokonaisvaltaisena suunnitelmana organisaation tietoturvaan liittyvissä asioissa ja ne tarjoavat määrittelyiden ja ohjeistuksien avulla perustan yrityksen tietoturvaturvalliselle toimintaympärille. Ne myös määrittelevät tietoturvaan kohdistuvat riskit, jotka pohjautuvat tiedon ominaisuuksiin, eli siis CIA-kolminaisuuteen ja tietoturvatähteen. Tietoturvakäytänteet voivat myös toimia elpymissuunnitelmana tietoturvariskin realisoituessa, jolloin niistä selviää tietoturvaongelman vaikutusten ehkäiseminen ja riskien estäminen tulevaisuudessa. Tietoturvakäytänteet toimivat myös tietoturvan kommunikointivälineenä työntekijöille ja todistavat tietoturvaohjelman olemassaolon. (Paananen ym., 2020.)

TAULUKKO 1 Tietoturvakäytänteiden piirteet ja tehtävät (Paananen, Lapke & Siponen, 2020, s. 3)

	Tietoturvakäytänteiden piirteet	**Tietoturvakäytänteiden toiminnot**
Organisaation ohjaus	Tietoturvatavoitteiden ja tietoturvastrategian määrittely	Liiketoimintatavoitteiden tukeminen
	Ohjaaminen ja ohjeistaminen	Hallinta
	Sääntöjen määrittely	Tehokkuuden mittaamisen perusta
Toimija ja omaisuus	Subjektien määrittely	Määrittelee vastuut ja toimivallan
	Objektien määrittely	Antaa yleiskuvan yrityksen informaatio-omaisuudesta
Tietoturvaongelmiin valmistautuminen	Kokonaisvaltainen suunnitelma	Tietoturvakulttuurin perusta
	Osoittaa riskit	Estää tiedon katoamista ja väärinkäyttöä
	Elpymissuunnitelma	Varmistaa jatkuvuuden
	Kommunikointiväline	Tietoturvaohjelman olemassaolon todiste

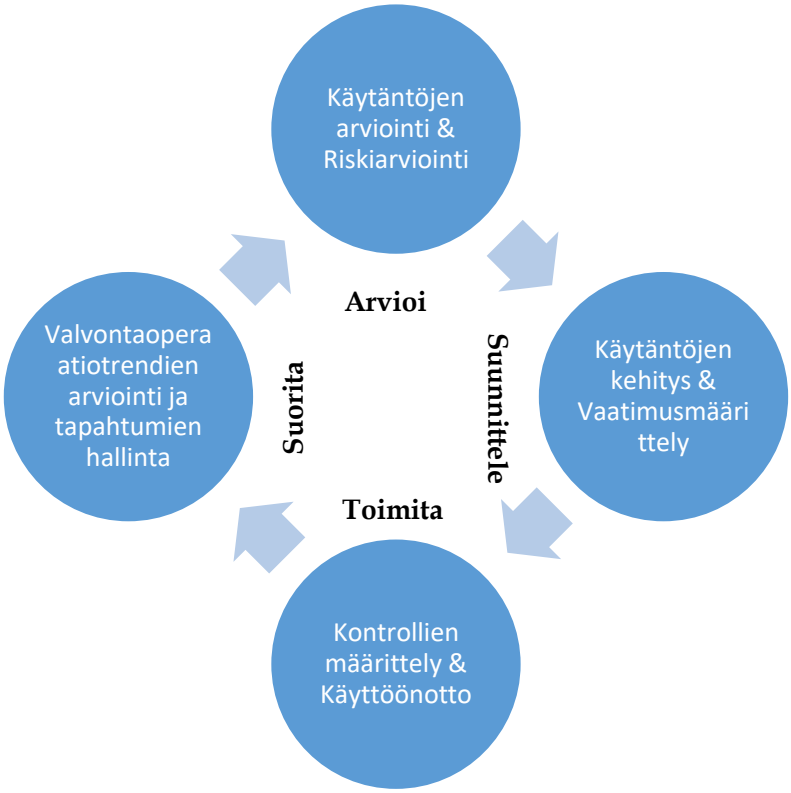
2.3 Tietoturvakäytänteiden kehittäminen

Tietoturvakäytänteiden suunnittelemiseen ja kehittämiseen on vuosien saatossa laadittu erilaisia prosesseja ja metodeja. Alaluvussa esitellään seuraavaksi kolme erilaista tietoturvakäytänteiden kehitysmallia, jotka ovat Wardin ja Smithin (2002) viisivaiheinen kehitysprosessi, Baskervillen ja Siposen (2002) nelivaiheinen metakäytänteisiin perustuva kehitysmalli ja viimeiseinä Reesin, Bandyopadhyayn ja Spaffordin (2003) PFIRES-malli. Wardin ja Smithin (2002) viisivaiheisessa kehitysprosessissa ensimmäinen vaihe on projektin aloitus, jossa tietoturvakäytänteiden kehitystä varten asetetaan projektitiimi ja sen ohjausryhmä. Sitä seuraa itse tietoturvakäytänteiden kehitysvaihe, jossa käytänteitä kehitetään yrityksen tietoturvatavoitteiden kannalta oleellisia asioita varten ja tarpeellisiksi katsottuja

sidosryhmiä konsultoiden. Kolmantena vaiheena on konsultaatio ja hyväksyntä, jossa tietoturvakäytänteille haetaan hyväksyntä organisaation johdolta. Neljäs vaihe kattaa kehitettyjen tietoturvakäytänteiden kommunikoinnin ja koulutuksen henkilöstölle, ja viimeisessä vaiheessa tietoturvakäytänteet levitetään koko organisaation saataville. (Ward & Smith, 2002.)

Baskerville ja Siponen (2002) metakäytänteihin perustuvassa kehitysmallissa on neljä vaihetta, jotka ovat käytänteiden vaatimukset, suunnittelu, käyttöönotto ja testaus. Ensimmäinen vaihe pitää sisällään tietoturvasubjektien ja objektien tunnistamisen sekä niiden luokittelu. Organisaatio siis määrittelee henkilöstön ja esimerkiksi sidosryhmät, jotka ovat tietoturvakäytänteiden noudattamisen piirissä. Samalla myös määritellään suojattava omaisuus, kuten fyysiset dokumentit tai tietojärjestelmät. Lopuksi vielä määritellään subjektien tarvitsemat käyttöoikeudet ja pääsy objekteihin. Suunnitteluvaiheessa luodaan itse korkean ja matalan tason tietoturvakäytänteet sekä metakäytänteet. Tässä vaiheessa määritellään myös tietoturvakäytänteiden tarkkuustaso sekä kuinka niiden noudattamista tullaan valvomaan. Käyttöönottovaiheessa suunnitellut ja toteutetut tietoturvakäytänteet otetaan käyttöön organisaatiossa ja testausvaiheessa tarkastellaan, millaisia vaikutuksia tietoturvakäytänteillä on ollut ja tarvitseeko niitä suunnitella uudelleen. (Baskerville & Siponen, 2002.)

Reesin ym. (2003) esittelemä Policy Framework for Interpreting Risk in E-Business Security -malli (PFIRES) (kuvio 2) tietoturvakäytänteiden kehitykseen koostuu neljästä vaihekokonaisuudesta, joista jokainen sisältää alavaiheita. Vaiheista ensimmäinen, eli arviointivaihe, alkaa tietoturvakäytäntöjen arvioinnilla ja riskiarvioinnilla. Organisaatiolla voi olla jo olemassa olevat tietoturvakäytännöt, joita mallin avulla aletaan uudelleensuunnittelemaan ja PFIRES-mallia voidaan myös hyödyntää silloinkin, kun organisaatiolla ei vielä ole käytössä olevia tietoturvakäytäntöjä. Tietoturvakäytäntöjen arvioinnilla tarkoitetaan niiden suunnittelua muun muassa organisaation toimintaympäristön kannalta ja suosituskäytäntöjen luomisella. Riskiarvioinnissa organisaatio tunnistaa kohteet, joita tietoturvakäytäntöjen tulisi suojata. Vaiheessa määritellään organisaation tärkeimmät omaisuudet ja niiden suojaamisen kustannukset. Suunnitteluvaiheessa tarkoituksena on tarkastella organisaation tietoturvastrategiaa ja luoda niiden pohjalta tietoturvakäytännöt. Tässä vaiheessa määritetään ja päivitetään vaatimukset tietoturvakäytännöille. Toimitusvaihe koostuu kontrollien, eli tietoturvariskejä ehkäisevien toimenpiteiden ja prosessien, määrittelemisestä ja niiden käyttöönotosta. Viimeisen vaiheen tarkoituksena on suorittaa tietoturvakäytänteitä, eli valvoa kolmannessa vaiheessa käyttöönotettujen kontrollien toimintaa ja noudattamista. Vaihe käynnistyy tietoturvakäytäntöjen käyttöönoton jälkeen. (Rees ym., 2003.)



KUVIO 2 Policy Framework for Interpreting Risk in e-Business Security (PFIRES) (Rees ym., 2003, s. 102)

3 TYÖNTEKIJÖIDEN TIETOTURVAKÄYTTÄYTYMINEN

Useiden tutkimuksien mukaan suurin osa organisaatioiden sisäisistä tietoturvauhkista ja -vuodoista johtuu työntekijöiden tietoturvakäyttäytymisestä. Tämä johtuu siitä, että työntekijät voivat erinäisistä syistä jättää tietoturvakäytänteitä noudattamatta tai rikkoa niitä, eivätkä työntekijät ole aina tietoisia tietoturvakäytänteistä tai niiden merkityksestä. (Bulgurcu ym., 2010; Rao, Dominic, Ali, Rehman & Sohail, 2021.) Tässä luvussa käydään läpi kirjallisuuskatsauksen toinen teoreettinen aihepiiri, eli tietoturvakäyttäytyminen organisaatiokontekstissa. Luku on jaettu kolmeen alalukuun, joista ensimmäisessä tarkastellaan tietoturvakäyttäytymisen tutkimuksessa useimmiten hyödynnettyjä teorioita sekä annetaan esimerkkejä niistä tietoturvakäyttäytymisen kontekstissa. Samassa alaluvussa myös esitellään Moodyn, Siposen ja Pahnilan (2018) luoma tietoturvakäyttäytymisen yhtenäismalli, jonka tarkoituksena oli selkeyttää teorioiden roolia tietoturvakäyttäytymisen tutkimuksessa yhdistämällä käytetyimmät teoriat ja niiden vaikutukset yhdeksi tietoturvakäyttäytymistä kuvaavaksi malliksi. Toinen alaluku kattaa tietoturvakäyttäytymiseen vaikuttavien tekijöiden läpikäynnin. Alaluvussa käydään läpi ensin tietoturvakäytänteiden noudattamiseen vaikuttavia tekijöitä, jonka jälkeen tarkastellaan päinvastaisesti niiden rikkomiseen vaikuttavia tekijöitä. Viimeisessä alaluvussa käydään läpi tietoturvakäyttäytymisen muuttumisen tutkimusta, joka on suhteellisen tuore näkökulma tietoturvakäyttäytymisen tutkimuksessa.

3.1 Teoriat tietoturvakäyttäytymisen tutkimuksessa

Organisaatioiden työntekijöiden tietoturvakäyttäytymistä on tutkittu yleensä kriminologian, psykologian tai sosiaalitieteiden aloilla alun perin kehitettyjen teorioiden avulla. Yleisimmin käytettyihin teorioihin tutustuminen auttaa yleiskuvan saamisessa tietoturvakäyttäytymisen tutkimusaihepiiriin, jonka vuoksi tämä teorialuku alkaa näiden teorioiden läpikäymisellä. Yleisimpiin käytettyihin

teorioihin lukeutuvat esimerkiksi perustellun toiminnan teoria, suunnittelun käyttäytymisen teoria, suojelumotivaatioteoria, peloteteoria, neutralisaatioteoria ja rationaalisen valinnan teoria. Nämä teoriat löytyvät alla olevasta taulukosta esimerkkeineen tietoturvakäyttäytymisen kontekstissa (taulukko 2) ja niitä tarkastellaan seuraavaksi yksitellen.

TAULUKKO 2 Käytetyimpiä teorioita tietoturvakäyttäytymistutkimuksessa

Teoria	**Esimerkki tietoturvakäyttäytymisen kontekstissa**
Perustellun toiminnan teoria (engl. *theory of reasoned action, TRA*)	Aikomus noudattaa tietoturvakäytänteitä johtaa tietoturvakäytänteiden todelliseen noudattamiseen (Siponen ym., 2014).
Suunnitellun käyttäytymisen teoria (engl. *theory of planned behavior, TPB*)	Ulkoisilla tekijöillä muokattavissa olevat asenteet, subjektiiviset normit ja minäpystyvyys vaikuttavat tietoturvakäyttäytymiseen (Bulgurcu ym., 2010).
Suojelumotivaatioteoria (engl. *protection motivation theory, PMT*)	Tietoturvakäytänteiden rikkomisen kokeminen uhkana ja kuinka minäpystyvyys motivoi välttämään niiden rikkomista (Siponen ym., 2014).
Peloteteoria (engl. *deterrence theory*)	Tietoturvakäytänteitä ei rikota, jos niiden rikkomisesta aiheutuvat seuraamukset koetaan varmoiksi, vakaviksi ja ne toimeenpannaan nopeasti (Siponen & Vance, 2010; Chen ym., 2020).
Neutralisaatioteoria (engl. *neutralization theory*)	Tietoturvakäytänteiden rikkoja järkeistää tekonsa itselleen neutralisointitekniikoilla (Siponen & Vance, 2010).
Rationaalisen valinnan teoria (engl. *rational choice theory, RCT*)	Työntekijä voi joko noudattaa tai rikkoa tietoturvakäytänteitä oman rationaalisen valintansa mukaan (Bulgurcu ym., 2010).

Perustellun toiminnan teorian mukaan aikomus käyttäytyä tietyllä tavalla vaikuttaa todelliseen käyttäytymiseen. Toisin sanoen, mitä vahvempi aikomus henkilöllä on käyttäytyä valitsemallaan tavalla, sitä varmemmin hän myös käyttäytyy todellisuudessa niin. Tietoturvakäyttäytymisen kontekstissa työntekijöiden aikomuksiin noudattaa tietoturvakäytänteitä vaikuttaa sosiaalisten normien lisäksi myös asenteet tietoturvakäytänteisiin. Normien ja asenteiden positiivinen vaikutus tietoturvakäytänteiden noudattamisaikomuksiin saa työntekijät lopulta noudattamaan niitä. (Siponen, Adam & Pahnila, 2014.)

Suunnitellun käyttäytymisen teoria kuvaa edellisen teorian tavoin henkilön aikomusta käyttäytyä tietyllä tavalla. Suunnitellun käyttäytymisen teoria voidaankin nähdä perustellun toiminnan teorian jatkoteoriana, joka täydentää aiempaa teoriaa. Suunnitellun käyttäytymisen teorian mukaan asenteet, subjektiiviset normit ja vaikutusvalta johonkin tilanteeseen vaikuttavat henkilön aikomuksiin ja lopulta todelliseen käyttäytymiseen merkittävästi. Asenteet, subjektiiviset normit ja vaikutusvalta tilanteeseen ovat muokattavissa ulkoisten vaikutusten

avulla, joilla tarkoitetaan esimerkiksi toisen henkilön vaikutusta. (Bulgurcu ym., 2010.)

Suojelumotivaatioteorian mukaan ihmiset arvioivat uhkatilanteessa sekä itse uhkan laadun sekä selviämismahdollisuutensa uhkasta. Uhka-arvioinnissa arvioidaan uhkasta aiheutuvan pelon määrää, johon vaikuttaa henkilön kokema haavoittuvuus tilanteessa sekä uhkasta aiheutuvien seuraamusten koettu vakavuus. Tietoturvakäyttäytymisen kontekstissa koettu haavoittuvuus voi olla esimerkiksi tietoturvakäytänteiden rikkomisen alttiutta ja uhkan koettu vakavuus puolestaan voi liittyä tietoturvarikkeistä aiheutuviin vahinkoihin organisaatiolle. Selviämisarviointi puolestaan kattaa minäpystyvyyden arvioinnin sekä vastatoimien tehokkuuden. Minäpystyvyydellä tarkoitetaan suojelumotivaatioteorian kontekstissa henkilön kykyä tunnistaa uhkasta selviämiseen liittyviä toimenpiteitä, ja vastatoimien tehokkuudella tarkoitetaan arviota toimenpiteiden tehokkuudesta uhkan estämisessä. Minäpystyvyyden, eli työntekijän vahvan uskon itseensä tietoturvakäytänteiden noudattamisen onnistumisessa, on todettu olevan varmin tietoturvakäyttäytymisen ennustaja. (Siponen ym., 2014.)

Kriminologiasta alun perin lähtöisin olevan peloteteorian mukaan henkilö päättää rikoksen tekemisestä arvioimalla rikollisen teon seuraamuksien todennäköisyyden ja vakavuuden. Jos teon seuraamuksien todennäköisyyden riski on suuri ja seuraamukset ovat ankaria, ei henkilö silloin teorian mukaan tee rikosta. Rikollisen teon seuraamuksia ovat esimerkiksi viralliset ja epäviralliset rangaistukset sekä häpeän tunne. Tietoturvakäytänteiden rikkomisen kontekstissa virallisia seuraamuksia voivat olla esimerkiksi varoitukset tai jopa työsuhteen päättäminen, kun taas epävirallisiin seuraamuksiin kuuluu muun muassa sosiaaliset seuraamukset, kuten kollegoiden paheksunta tietoturvakäytänteiden rikkojaa kohtaan. Häpeän tunne on verrattavissa virallisiin ja epävirallisiin seuraamuksiin, joten se voidaan lukea myös peloteteorian pelotteiden joukkoon. (Siponen & Vance, 2010.) Peloteteoriaan sisältyy myös seuraamuksien toimeenpanon nopeus, mutta tätä peloteteorian osa-aluetta on tietoturvakäyttäytymisen tutkimuksessa hyödynnetty harvoin (Chen, Zhen, Dong & Xie, 2020). Seuraamuksien koetulla tai oletetulla todennäköisyydellä ja vakavuudella voi myös olla tehokkaampi vaikutus kuin niiden todellisella varmuudella ja ankaruudella. Tämä johtuu siitä, että työntekijän muodostamaan mielikuvaan seuraamusten vakavuudesta ja todennäköisyydestä vaikuttaa suorat ja epäsuorat kokemukset henkilökohtaisista tai kollegojen kohtaamista rangaistuksista. Tämän vuoksi esimerkiksi kollegan välttäessä tai kohdatessa ankaria seuraamuksia tietoturvakäytänteiden rikkomisesta, mielikuva seuraamuksien vakavuudesta ja todennäköisyydestä voi muuttua. (Son, 2011.)

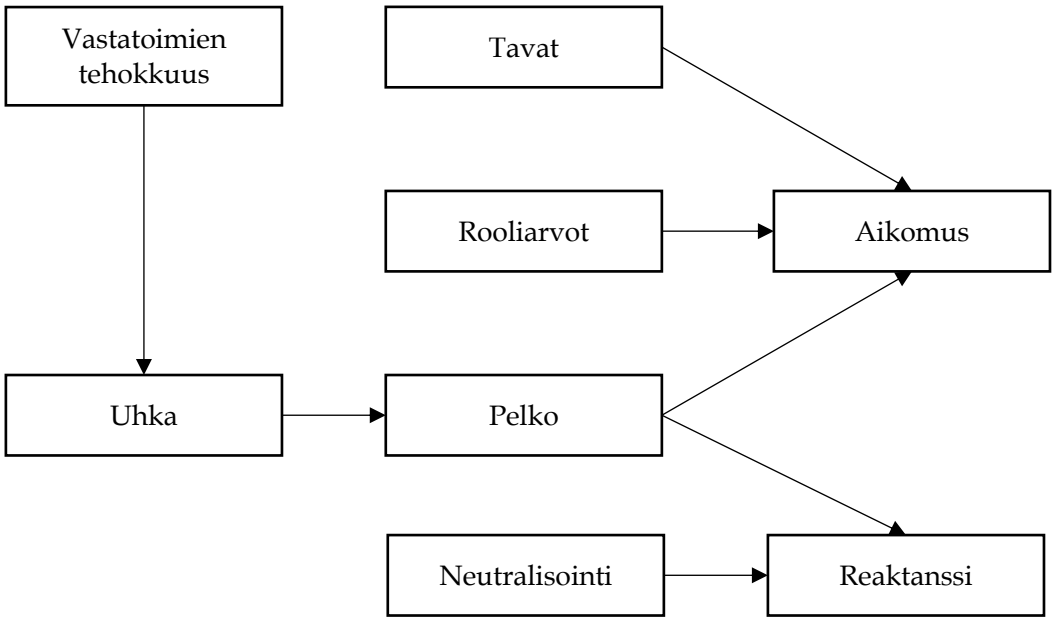
Sykesin ja Matzan (1957) esittelemä neutralisaatioteoria kuvaa vahingollisen tai poikkeavan käytöksen oikeutukseen käytettävät viisi neutralisaatiotekniikkaa, joilla yksilö voi järkeistää ja oikeuttaa käytöksensä itselleen. Teoria kattaa viisi eri neutralisaatiotapaa, jotka ovat vastuun kieltäminen, vahingon kieltäminen, uhrin kieltäminen, tuomitsijoiden tuomitseminen, ja korkeampiin lojaliteetteihin vetoaminen. (Sykes & Matza, 1957.) Vastuun kieltämisellä henkilö siirtää tekojensa vastuun itsestään pois ja voi väittää, että teko johtuu itsestään

ulkopuolisista asioista. Vastuun kieltäminen voi esimerkiksi näkyä siten, että työntekijä kieltää olevansa vastuussa tietoturvakäytänteiden rikkomisesta sen takia, että niitä oli hankala ymmärtää. Vahingon kieltäminen puolestaan liittyy siihen, että henkilö tunnistaa tekonsa vääryyden tai vahingollisuuden, mutta kokee, ettei teosta ole harmia kenellekään tai millekään. Työntekijä voi jättää noudattamatta tietoturvakäytänteitä kokiessaan, ettei se vahingoita muita työntekijöitä. Uhrin kieltämisellä teoria tarkoittaa sitä, että vahingollisesti käyttäytyvä yksilö kokee teon kohteena olevan henkilön ansaitsevan sen, eikä teossa ole uhria. Tätä neutralisaatiotekniikkaa ei ole juurikaan käytetty tietoturvakäyttäytymisen tutkimisessa, sillä tietoturvakäytänteiden rikkomiseen liittyvä uhri on hankala määrittää. Neljäs neutralisaatiotekniikka, eli tuomitsijoiden tuomitseminen, tarkoittaa sitä, että vahingollisesti käyttäytyvä henkilö syyttää hänen käyttäytymisensä tuomitsevia henkilöitä tai teon kohdetta. Työntekijä saattaa tietoturvakäytänteitä rikkoessaan esimerkiksi syyttää organisaatiota liian rajoittavista tietoturvakäytänteistä. Viimeiseinä tekniikkana oleva korkeampiin lojaliteetteihin vetoaminen tarkoittaa, että henkilö kokee tarpeelliseksi käyttäytyä normaalista poikkeavasti jonkin tavoitteen saavuttamiseksi. (Siponen & Vance, 2010.) Neutralisaatioteoriaa on Sykesin ja Matzan (1957) tutkimuksen jälkeen laajennettu useasti. Klockars (1974) lisäsi teoriaan tilikirjan metafora -neutralisaatiotekniikan ja Minor (1981) välttämättömyyden puolustamisen. Välttämättömyyden puolustamisella tarkoitetaan, että työntekijä puolustelee tietoturvakäytänteiden rikkomista välttämättömyydellä saada työtehtävät suoritettua ajoissa. Tilikirjan metafora -tekniikka puolestaan liittyy siihen, että jos työntekijä noudattaa tietoturvakäytänteitä pääsääntöisesti, niin hän voi satunnaisesti myös rikkoa niitä. (Siponen & Vance, 2010.) Viimeisempänä lisäyksenä, eli kahdeksantena neutralisointitekniikkana, on yleisyyden puolustaminen. Sillä tarkoitetaan sitä, ettei tietoturvakäytänteiden rikkomisesta tarvitse kokea syyllisyyttä, sillä niiden rikkominen on hyvin yleistä. (Rao ym., 2021.)

Viimeisenä teoriana oleva rationaalisen valinnan teoria kuvaa henkilön käyttäytymistä tilanteessa, jossa on useita eri valintamahdollisuuksia. Käyttäytymisen valintaan vaikuttaa henkilön arvio valinnan hyödyistä ja kustannuksista. Henkilö siis arvioi tilanteen eri valintojen seuraamukset sekä niiden hyödyt ja kustannukset, ja muodostaa arviointien avulla päätöksen käyttäytyä valitsemallaan tavalla. Koska ihmisillä on erilaisia mieltymyksiä ja käsityksiä valinnan hyödyistä ja kustannuksista, valinta on teorian mukaan aina subjektiivinen ja siten myös henkilön näkökulmasta rationaalinen. (Bulgurcu ym., 2010.)

Edellä kuvaillut teoriat kuuluvat tietoturvakäyttäytymisen tutkimuksen yleisimmin käytettyihin teorioihin, mutta tutkimuksessa on käytetty myös muita teorioita. Tutkimukset ovat lisäksi aikaisemmin hyödyntäneet yleensä vain yhtä tai kahta teoriaa teoreettisena viitekehyksenä. Näiden tekijöiden takia tietoturvakäyttäytymisen tutkimus voi vaikuttaa sekavalta teorioiden viidakolta, eikä teorioita yhdistävää tutkimusta ole aikaisemmin ollut tarjolla. Tilanne kuitenkin muuttui, kun Moody, Siponen ja Pahnila (2018) loivat tutkimuksessaan tietoturvakäyttäytymisen yhtenäismallin. Tutkimuksen tarkoituksena oli kartoittaa aikaisemmassa tietoturvakäyttäytymistutkimuksessa käytetyt teoriat, vertailla

niitä keskenään ja luoda lopulta yhtenäinen malli kuvaamaan tietoturvakäyttäytymistä ja siihen vaikuttavia tekijöitä. Tutkimukseen valittiin kolmetoista teoriaa, joihin lukeutui muun muassa neutralisointiteoria, peloteteoria ja suojelumotivaatioteoria. Tutkimuksen tuloksena syntyi tietoturvakäyttäytymisen yhtenäismalli (engl. *the unified model of information policy compliance, UMISPC)*. Malli (kuvio 3) oli merkittävä kontribuutio sekä tutkimukselle että käytännölle, sillä se yhdisti ensimmäistä kertaa tietoturvakäyttäytymisen tutkimuksessa useimmin käytetyt teoriat toisiinsa ja loi niiden pohjalta mallin kuvaamaan tietoturvakäyttäytymiseen vaikuttavista asioista. Aikaisemmassa tutkimuksessa teorioita on yleensä tutkittu erikseen tai vain yhtä tai kahta kerrallaan, eikä useampaa teoriaa ole hyödynnetty yhdessä (Moody ym., 2018.)



KUVIO 3 Tietoturvakäyttäytymisen yhtenäismalli (Moody ym., 2018, s. 305)

Yhtenäismalli kuvaa eri teorioista johdettujen tekijöiden, kuten rooliarvojen, pelon ja neutralisoinnin vaikutuksia tietoturvakäyttäytymiseen. Mallissa on kaksi lopputulemaa, eli aikomus noudattaa tietoturvakäytänteitä tai tietoturvauhkan kieltäminen (reaktanssi). Aikomukseen noudattaa tietoturvakäytänteitä vaikuttivat työntekijän tavat, rooliarvot ja pelko, joista rooliarvoilla oli suurin merkitys. Niillä tarkoitetaan, että työntekijä kokee tietoturvakäytänteiden olevan reiluja ja oikeudenmukaisia hänen roolinsa ja työtehtävien näkökulmasta organisaatiossa. Tavoilla puolestaan tarkoitetaan työntekijän käyttäytymisessä esiintyviä tapoja, jotka ovat luonnostaan tietoturvakäytänteiden mukaisia. (Moody ym., 2018.)

Pelkoon reaktanssin ennustajana vaikuttavat uhkat, joihin puolestaan vaikuttaa ensin vastatoimien tehokkuus. Uhkalla tarkoitetaan työntekijän kokemaa alttiutta altistua uhkalle, kuten tietoturvariskille, sekä uhkan seuraamusten vakavuutta. Vastatoimien tehokkuudella puolestaan tarkoitetaan koettua käyttäytymisen tehokkuutta uhkan lievittämisessä. Reaktanssiin toisena vaikuttavana

tekijänä havaittiin myös olevan pelon lisäksi neutralisointi, eli poikkeavan käytöksen järkeistäminen itselleen. (Moody ym., 2018.)

Mallin validius testattiin empiirisellä tutkimuksella. Tulokset tukivat mallia ja osoittivat sen toimivan selittävänä mallina tutkituissa tietoturvaskenaarioissa, jotka olivat salasanojen jakaminen, USB-tietoturvarikkeet ja työasemien lukitsematta jättäminen. Kyseiset skenaariot ovat organisaatioissa tapahtuvia yleisimpiä tietoturvakäytänteiden rikkeitä, jonka vuoksi ne valittiin tutkimukseen. On kuitenkin huomioitava, että malli ei ole kaikenkattava, eikä se pysty välttämättä selittämään tietoturvakäyttäytymistä kaikkien tietoturvakäytänteiden rikkomisen kohdalla. (Moody ym., 2018.)

3.2 Tietoturvakäytänteiden noudattaminen ja rikkominen

Työntekijöiden tietoturvakäyttäytymistä on aikaisemmassa tutkimuskirjallisuudessa tutkittu sekä tietoturvakäytänteiden noudattamisen että rikkomisen näkökulmasta, joskin jälkimmäiseen liittyvää tutkimuskirjallisuutta esiintyy huomattavasti vähemmän. Työntekijöiden tietoturvakäyttäytymistä selittäviä ja ennustavia tekijöitä käsitellään kahdessa seuraavassa alaluvussa ja vaikuttavat tekijät on myös koottu alla olevaan taulukkoon (taulukko 3).

TAULUKKO 3 Tietoturvakäytänteiden noudattamiseen ja rikkomiseen vaikuttavia tekijöitä (Rao ym., 2021, s. 34 mukaillen)

Tekijä	**Tietoturvakäytänteiden noudattaminen vai rikkominen**
Sisäinen ja ulkoinen motivaatio	Noudattaminen
Suojelumotivaatiokäyttäytyminen	Noudattaminen
Tietoturvakulttuuri- ja -tietoisuuskäyttäytyminen	Noudattaminen
Organisaation johdon käyttäytyminen	Noudattaminen
Neutralisointi	Rikkominen
Arvokonfliktit	Rikkominen
Pelotteet	Rikkominen
Turvallisuusstressi	Rikkominen

3.2.1 Tietoturvakäytänteiden noudattaminen

Tietoturvakäytänteiden noudattamiseen vaikuttavia tekijöitä ovat sisäinen ja ulkoinen motivaatio, suojelumotivaatiokäyttäytyminen, tietoturvakulttuuri ja organisaation johdon käyttäytyminen (taulukko 4). Sonin (2011) mukaan sisäisellä ja ulkoisella motivaatiolla on havaittu olevan hyvin merkittävä vaikutus työntekijöihin tietoturvakäytänteiden noudattamisessa. Lisäksi sisäisellä motivaatiolla on huomattavasti merkittävämpi rooli tietoturvakäyttäytymisessä, kuin työntekijöiden ulkoisella motivaatiolla. Sisäisen motivaatiomallin osalta tutkimus keskittyi koetun legitimiteetin ja koetun arvoyhteensopivuuden arvioimiseen, ja ulkoisiin motivaattoreihin lukeutuivat tietoturvakäytänteiden rikkomisesta

aiheutuvien seuraamusten koettu todennäköisyys ja vakavuus. Koetulla legitimiteetillä tarkoitetaan sisäisessä motivaatiomallissa tietoturvakäytänteiden koettua asianmukaisuutta ja oikeudenmukaisuutta. Koettu arvoyhteensopivuus puolestaan viittaa siihen, kuinka paljon työntekijä kokee henkilökohtaistensa ja organisaationsa arvojen sopivan yhteen. (Son, 2011.)

TAULUKKO 4 Tietoturvakäytänteiden noudattamista edistäviä tekijöitä

Tekijä	**Esimerkki tietoturvakäyttäytymisessä**	**Tutkimukset**
Sisäinen ja ulkoinen motivaatio	Tietoturvakäytänteitä noudatetaan tietoturvakäytänteiden ollessa työntekijöiden näkökulmasta asianmukaisia ja reiluja.	Son (2011)
Suojelumotivaatio-käyttäytyminen	Koettu korkea minäpystyvyys sekä tietoturvauhkatilanteessa koettu haavoittuvuus edistävät positiivista tietoturvakäyttäytymistä.	Johnston & Warkentin (2010); Rajab & Eydgahi (2019); Hooper & Blunt (2020)
Tietoturvakulttuuri- ja tietoturvatietoisuus-käyttäytyminen	Organisaation vahva tietoturvakulttuuri sekä vahva työtyytyväisyys ja tietoturvatietoisuus edistävät tietoturvakäytänteiden noudattamista.	Hu ym. (2012); D'Arcy & Greene, (2014); Safa ym. (2015)
Organisaation johdon käyttäytyminen	Organisaation johdon sitoutuminen tietoturvakulttuurin rakentamiseen sekä organisaatiolta saatava tuki vaikuttavat myönteisesti tietoturvakäytänteiden noudattamiseen.	Han ym (2017); Sharma & Warkentin (2019); Koolang ym. (2020)

Vahva suojelumotivaatio edistää myös työntekijöiden tietoturvakäytänteiden mukaista käyttäytymistä (Johnston & Warkentin, 2010; Rajab & Eydgahi, 2019; Hooper & Blunt, 2020). Johnstonin ja Warkentinin (2010) tutkimuksessa käsiteltiin pelotteiden ja suojelumotivaation vaikutusta tietoturvakäyttäytymiseen, ja tulokset osoittivatkin, että molemmilla on tehokas positiivinen vaikutus työntekijöihin. Tutkimuksen mukaan sosiaalisella vaikutuksella, eli kollegojen tietoturvakäytänteiden noudattamisella, oli kuitenkin suurin merkitys tietoturvakäyttäytymisen ennustamisessa (Johnston & Warkentin, 2010). Rajabin ja Eydgahin (2019) tutkimus puolestaan painottui korkeakoulujen työntekijöihin, mutta totesi silti edellisen tutkimuksen tavoin suojelumotivaation toimivan erinomaisena tietoturvakäytänteiden noudattamiseen vaikuttavana tekijänä ja sen ennustajana. Etenkin suojelumotivaatioteorian kuvaama haavoittuvuus tietoturvauhkissa todettiin olevan tietoturvakäytänteiden noudattamisen vahvin ennakoija. Mitä vähemmän työntekijöillä oli vaikutusvaltaa organisaation informaatioon, ja mitä enemmän he kokivat organisaation olevan altis tietoturvahyökkäyksille, sitä varmemmin he noudattivat tietoturvakäytänteitä. (Rajab & Eydgahi, 2019.) Hooper ja Blunt (2020) tutkivat monesta muusta tietoturvakäyttäytymiseen liittyvästä tutkimuksesta poiketen nimenomaan IT-alan työntekijöiden tietoturvakäytänteiden noudattamista. Tulokset osoittivat, että tietoturvakäytänteiden noudattamisen koettu vaikutus ja työntekijän minäpystyvyys edistävät merkittävästi tietoturvakäytänteiden noudattamista. Koetulla vaikutuksella tutkimuksessa

tarkoitetaan, että mitä suuremmaksi työntekijät kokevat tietoturvakäytänteiden noudattamisesta aiheutuvat hyödyt organisaatiolle, sitä enemmän se motivoi heitä myös noudattamaan niitä. IT-alan työntekijöillä on yleensä muiden alojen työntekijöitä korkeampi IT-asioihin liittyvä minäpystyvyys, joten tutkimuksen mukaan on luontaista, että se myös vaikuttaa positiivisesti tietoturvakäytänteiden noudattamiseen ja sen tärkeyteen. (Hooper & Blunt, 2020.)

Useissa tutkimuksissa painotetaan laadukkaan tietoturvakulttuurin rakentamista organisaatioissa sekä tietoturvatietoisuuden lisäämistä tietoturvakäytänteiden noudattamisen edistämiseksi (Hu, Dinev, Hart & Cooke, 2012; D'Arcy & Greene, 2014; Safa, Sookhak, Von Solms, Furnell, Ghani & Herawan, 2015). Hun ym. (2012) mukaan organisaation johdon osallistuminen tietoturva-asioihin, jotka muokkaavat organisaation sisäistä kulttuuria, vaikuttaa positiivisesti työntekijöiden asenteisiin tietoturvaa kohtaan ja siten parantaa tietoturvakäytänteiden noudattamista. Myös D'Arcy ja Greene (2014) puoltavat organisaation tietoturvakulttuurin positiivista vaikutusta tietoturvakäytänteiden noudattamisessa ja totesivat lisäksi myös korkean työtyytyväisyyden vaikuttavan myönteisesti tietoturvakäyttäytymiseen. Tutkimus myös paljasti odotuksien vastaisesti, että organisaation vahva tuki tietoturva-asioissa heikentää tietoturvakäytänteiden noudattamista. Havainto voi olla selitettävissä sillä, että työntekijät kokevat korkean organisaation antaman tuen takia organisaation olevan itse vastuussa tietoturvastaan, jolloin yksittäiset työntekijät eivät koe omaa tietoturvakäyttäytymistään tärkeäksi. (D'Arcy & Greene, 2014.) Safa ym. (2015) tutkivat tietoturvakäyttäytymistä tietoisen välittämisen konseptin avulla. Tietoisella välittämisellä tarkoitetaan, että työntekijät pohtivat tietoturvakäyttäytymisensä seuraamuksia ennen teon suorittamista. Tietoiseen välittämiseen vaikuttaa tutkimuksen mukaan työntekijän tietoturvatietoisuus, kokemus tietoturva-asioista sekä erityisesti myös organisaation tietoturvakulttuuri. Subjektiivisilla normeilla havaittiin myös olevan myönteinen vaikutus tietoturvakäytänteiden noudattamiseen, eli työntekijän käsityksellä siitä, millainen tietoturvakäyttäytyminen muille työntekijöille on tärkeää. (Safa ym., 2015.)

Neljäntenä tietoturvakäytänteiden noudattamiseen liittyvänä teemana on organisaation johdon käyttäytyminen tietoturva-asioissa. Han, Kim ja Kim (2017) tutkivat tietoturvakäyttäytymistä organisaation johdon, kuten esimiesten, käyttäytymisen ja psykologisen sopimuksen näkökulmasta. Psykologinen sopimus viittaa työntekijän muodostamiin odotuksiin hänen ja organisaation välisestä suhteesta, jossa molemmilla osapuolilla on transaktionaalisia ja relationaalisia velvoitteita sekä vastaanottaa että antaa jotain toisilleen. Transaktionaaliset velvoitteet ovat ulkoisia tekijöitä kuten palkkaan liittyviä asioita, ja relationaaliset velvoitteet liittyvät esimerkiksi urakehitykseen. Tutkimuksen mukaan psykologisella sopimuksella ja etenkin tietoturvakäytänteiden noudattamisen koetuilla hyödyillä on merkittävä positiivinen vaikutus työntekijöiden tietoturvakäyttäytymiseen. Koetuilla hyödyillä ei tutkimuksessa viitata tiettyihin spesifisiin hyötyihin, vaan niillä tarkoitetaan enemmänkin yleisiä suotuisia vaikutuksia. Psykologisen sopimuksen havaittiin kuitenkin vaikuttavan eniten organisaation johtotason henkilöstöön eikä työntekijöihin, joka voi selittyä johtotason yleensä

pidempänä työkokemuksena ja siten psykologisen sopimuksen korkeampana arvostamisena. (Han ym., 2017.) Sharman ja Warkentinin (2019) tutkimus puolestaan käsitteli tietoturvakäyttäytymisen eroja vakituisissa ja määräaikaisissa työsuhteissa. Tutkimus osoitti, että vakituiset työntekijät noudattavat tietoturvakäytänteitä paremmin kuin määräaikaiset työntekijät, sillä tietoturvakäytänteiden noudattamisen koettujen kustannuksien arvioinnilla ei ole heihin yhtä suurta vaikutusta kuin määräaikaisiin työntekijöihin. Tietoturvakäyttäytymiseen vaikutti myös positiivisesti vahva sitoutuminen organisaatioon, jonka havaittiin olevan vahvempi vakituisissa työntekijöissä. Tutkimus myös löysi päinvastaisia tuloksia D'Arcyn ja Greenen (2014) tutkimukseen verrattaessa, sillä organisaation antamalla tuella todettiin olevan myönteinen vaikutus tietoturvakäytänteiden noudattamiseen. Kuten sitoutumisella organisaatioon, myös organisaation antaman tuen vaikutukset olivat vahvempia vakituisissa työntekijöissä. (Sharman & Warkentin, 2019.) Koohangin, Nowakin, Paliszkiewiczin ja Nordin (2020) tutkimus puolestaan käsitteli neljän eri tietoturvakäyttäytymiseen vaikuttavien tekijöiden merkittävyyttä tietoturvakäyttäytymisen ennustajana, jotka olivat organisaation johto, luottamus, rooliarvot ja tietoturvatietoisuus. Tutkimus osoitti, että kaikki neljä tekijää olivat tehokkaita tietoturvakäytänteiden noudattamisen ennustajia. Organisaation johdon sitoutuminen tietoturvakulttuurin rakentamiseen ja sen kommunikointi edisti selvästi tietoturvakäytänteiden noudattamista. Työntekijöiden luottamus organisaation johdon rakentamaan tietoturvakulttuuriin sekä rooliarvot, eli työntekijöiden muodostamat arvot omasta roolistaan organisaatiossa, todettiin myös tärkeäksi tietoturvakäyttäytymistä edistäväksi tekijäksi ja niihin voidaan vaikuttaa organisaation johdon käyttäytymisellä. Lisäksi vahva tietoturvatietoisuus vaikuttaa myönteisesti tietoturvakäytänteiden noudattamiseen, jota voidaan vahvistaa esimerkiksi tietoturvakoulutuksilla. (Koohang ym., 2020.)

3.2.2 Tietoturvakäytänteiden rikkominen

Tietoturvakäytänteiden rikkomiseen vaikuttavia tekijöitä ovat esimerkiksi neutralisointi, arvokonfliktit, pelotteet sekä turvallisuusstressi (taulukko 5). Tietoturvakäytänteiden rikkomiseen tai noudattamatta jättämiseen liittyvässä tutkimuksessa neutralisaatioteoria on ollut yksi suosituimmista käytetyimmistä teorioista. Neutralisaatio ja neutralisaatiotekniikoiden käyttämisen on todettu olevan vahvasti yhteydessä tietoturvakäytänteiden rikkomiseen tai aikomukseen rikkoa niitä (Siponen & Vance, 2010; Kim ym., 2014; Moody ym., 2018; Willison, Warkentin & Johnston, 2018). Siposen ja Vancen (2010) mukaan neutralisointi lisää selkeästi työntekijöiden alttiutta aikomuksiin rikkoa tietoturvakäytänteitä, mutta samalla painottavat, että aikomukset eivät kuitenkaan aina tarkoita todellista tietoturvakäytänteiden rikkomista. Kim ym. (2014) totesivat myös neutralisoinnin vaikuttavan negatiivisesti työntekijöiden aikomuksiin noudattaa tietoturvakäytänteitä. Tutkimuksen mukaan kaikki neutralisointitekniikat, pois lukien uhrin kieltäminen, vaikuttaa kielteisesti työntekijöiden aikomuksiin noudattaa tietoturvakäytänteitä (Kim ym., 2014). Myös Moody ym. (2018) löysivät neutralisoinnin olevan vahvasti yhteyksissä tietoturvakäytänteiden rikkomiseen.

Tutkimuksen mukaan kaikkia neutralisointitekniikoita ei välttämättä käytetä kaikkiin erilaisiin tietoturvakäytänteiden rikkomistapoihin, vaan tietynlaiset rikkeet voivat johtua tiettyjen neutralisointitekniikoiden käyttämisestä (Moody ym., 2018). Willisonin ym. (2018) mukaan neutralisoinnilla on vaikutusta aikomuksiin noudattaa tietoturvakäytänteitä vain silloin, jos tietoturvakäytänteiden noudattaminen aiheuttaa proseduraalista epäoikeudenmukaisuutta. Tämä tarkoittaa sitä, että jos tietoturvakäytänteiden noudattaminen koetaan epäreiluna tai epäoikeudenmukaisena, niin se johtaa useimmiten tietoturvakäytänteiden rikkomiseen (Moody ym., 2018).

TAULUKKO 5 Tietoturvakäytänteiden rikkomiseen vaikuttavia tekijöitä

Tekijä	**Esimerkki tietoturvakäyttäytymisessä**	**Tutkimukset**
Neutralisointi	Tietoturvakäytänteiden rikkominen järkeistetään neutralisaatiotekniikoilla.	Siponen & Vance (2010); Kim ym. (2014); Moody ym. (2018); Willison ym. (2018)
Arvokonfliktit	Tietoturvakäytänteiden noudattamisesta aiheutuva este työnteolle ja arvojen ristiriita aiheuttaa tietoturvarikkeitä.	Doherty & Tajuddin (2018); Kajtazi ym. (2018); Li ym. (2019)
Pelotteet	Tietoturvakäytänteiden rikkomisten vakavat ja varmat seuraamukset sekä niiden nopea toimeenpano ehkäisee tietoturvarikkeitä.	Cheng ym. (2013); Merhi & Ahluwalia (2019); Chen ym. (2020)
Turvallisuusstressi	Tietoturvakäytänteiden noudattaminen koetaan turhauttavaksi, mikä heikentää työntekijöiden aikomuksia noudattaa tietoturvakäytänteitä.	Rao ym. (2021)

Työntekijöiden arvoilla ja valintamieltymyksillä on myös havaittu olevan yhteys tietoturvakäytänteiden rikkomiseen (Doherty & Tajuddin, 2018; Kajtazi, Cavusoglu, Benbasat & Haftor, 2018; Li, Zhang & Siponen, 2019). Dohertyn ja Tajuddin (2018) mukaan tietoturvakäyttäytymiseen vaikuttaa organisaation tietoresurssien koettu arvo työntekijän näkökulmasta. Jos työntekijät eivät koe organisaation tietoa merkittäväksi tai tärkeäksi, niin työntekijät eivät usein myöskään noudata tietoa turvaavia tietoturvakäytänteitä. (Doherty & Tajuddin, 2018). Kajtazin ym. (2018) tutkimuksessa todettiin, että tietoturvaan ja työn tekemiseen liittyvien arvojen ristiriita voi johtaa tietoturvakäytänteiden rikkomiseen. Jos tietoturvakäytänteiden noudattaminen aiheuttaa esteen tai hidasteen työtehtävien suorittamiselle, niin työntekijät priorisoivat useimmiten työtehtävien suorittamisen tietoturvakäytänteiden rikkomisen kustannuksella. Työntekijöiden aikomuksiin rikkoa tietoturvakäytänteitä vaikuttaa lisäksi myös koettu hyöty niiden rikkomisesta, joka voi olla esimerkiksi työtehtävien loppuun suorittamisen mahdollisuus ilman tietoturvakäytänteiden noudattamisen aiheuttamaa estettä. (Kajtazi ym., 2018.) Li ym. (2019) puolestaan tutkivat sellaisia tietoturvakäytänteiden rikkomuksia, joista ei ole organisaatioille välitöntä vahinkoa. Tällainen rike voi olla esimerkiksi tietoturvallisesti heikon salasanan käyttäminen, vaikka

tietoturvakäytänteet ohjeistavat työntekijöitä käyttämään tietoturvallisesti vahvoja salasanoja. Heikon salasanan valitsemisesta itsestään ei koidu yritykselle välittömästi harmia, mutta salasana voi olla tulevaisuudessa helposti murrettavissa organisaatioon kohdistuvassa kyberhyökkäyksessä. Tutkimuksen tulokset osoittivat, että tietoturvakäytänteiden rikkomisen pitkäaikaisvaikutusten ymmärtäminen vähentää työntekijöiden aikomuksia rikkoa tietoturvakäytänteitä. Pitkäaikaisvaikutusten osalta etenkin jatkuvuudella, eli tietoturvarikkeiden jatkuvalla välttämisellä, havaittiin olevan suuri merkitys tietoturvakäytänteiden rikkomisen vähentämisessä. (Li ym., 2019.)

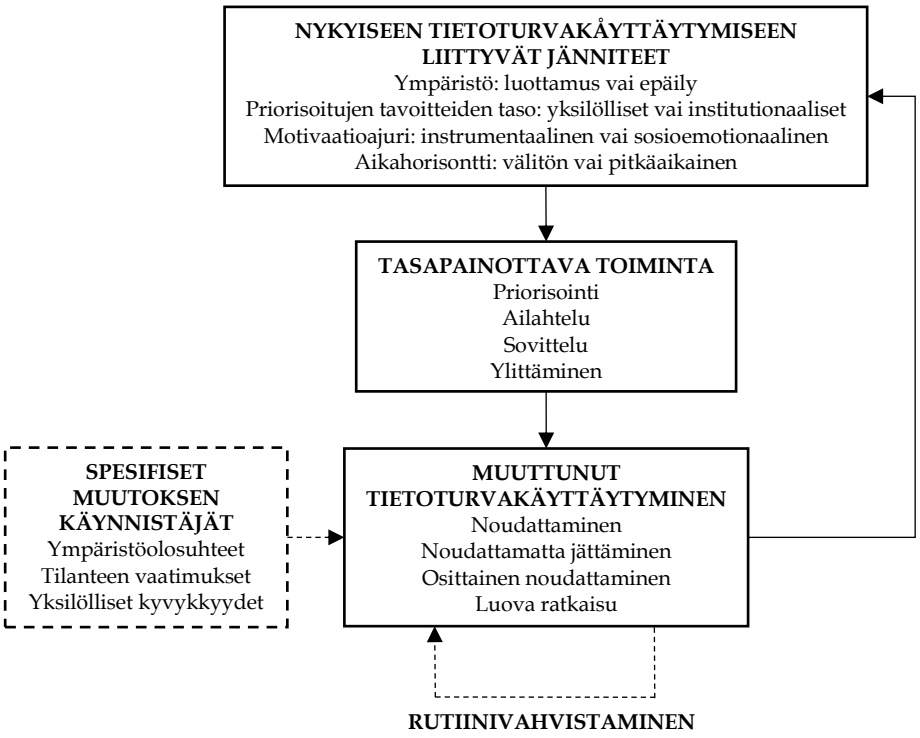
Kolmantena merkittävänä tietoturvakäytänteiden rikkomiseen liittyvänä teemana ovat pelotteet (Rao ym., 2021) ja niiden on havaittu olevan tehokas keino vähentää tietoturvakäytänteiden rikkomista (Cheng ym., 2013; Merhi & Ahluwalia, 2019; Chen ym., 2020). Chengin, Lin, Lin, Holmin ja Zhain (2013) mukaan virallisilla pelotteilla on suuri merkitys työntekijöiden tietoturvakäyttäytymisessä. Tietoturvakäytänteiden rikkomisen seuraamuksien suuri vakavuus vähensi merkittävästi työntekijöiden aikomuksia rikkoa tietoturvakäytänteitä, mutta toisaalta seuraamuksien korkea todennäköisyys ei vaikuttanut tietoturvakäyttäytymiseen (Cheng ym., 2013). Merhin ja Ahluwalian (2019) tutkimus käsitteli tietoturvakäytänteisiin liittyvää resistanssia ja pelotteita. Tietoturvakäytänteiden noudattaminen vaatii usein työntekijöitä tekemään muutoksia käyttäytymiseensä, jotta he eivät rikkoisi tietoturvakäytänteitä. Käyttäytymisen muuttaminen voi aiheuttaa työntekijöissä tietoturvakäytänneresistanssia, joka saa heidät toimimaan tietoturvakäytänteiden vastaisesti. Tietoturvarikkeistä aiheutuvat pelotteet puolestaan vaikuttivat tietoturvakäyttäytymiseen epäsuorasti vaikuttamalla ensin työntekijöiden deskriptiivisiin ja moraalisiin normeihin, jotka myöhemmin vähensivät työntekijöissä esiintyvää tietoturvakäytänneresistanssia. (Merhi & Ahluwalia, 2019.) Chengin ym. (2013) tutkimuksesta poiketen, Merhin ja Ahluwalian (2019) tutkimus osoitti, että seuraamuksien todennäköisyys vaikutti työntekijöiden deskriptiivisiin ja normeihin merkittävästi, kun taas seuraamuksien vakavuudella ei ollut juurikaan merkitystä. Tämä johtuu siitä, että moraalisiin normeihin vaikuttaa enemmän tapahtuman todennäköisyys kuin sen vakavuus (Merhi & Ahluwalia, 2019). Chen ym. (2020) tutkimus tietoturvakäytänteiden rikkomisesta käsitteli rikkeistä aiheutuvien seuraamusten vaikutusta erityisesti seuraamuksien toimeenpanon nopeuden näkökulmasta, jota on aikaisemmin tutkittu hyvin niukasti. Tutkimuksen mukaan toimeenpanon nopeudella on merkittävä positiivinen vaikutus tietoturvarikkeiden estämisessä, ja se parantaa lisäksi seuraamuksien todennäköisyyden tehokkuutta. Tietoturvarikkeistä aiheutuvien seuraamusten varmuus ja niiden nopea toimeenpano toimii työntekijöille pelotteena, jolloin he eivät todennäköisemmin tee tietoturvarikettä. Seuraamusten vakavuutta lisäämällä tietoturvakäyttäytyminen paranee entisestään, sillä tällöin työntekijät kohtaavat seuraamuksia jokaisesta tietoturvarikkeestä nopeasti, jota he pyrkivät välttämään. (Chen ym., 2020.)

Neljäs merkittävä tietoturvakäytänteiden rikkomiseen vaikuttava tekijä on turvallisuusstressi. Tietoturvakäytänteet voivat aiheuttaa esimerkiksi väsymystä ja turhautuneisuutta, jotka voivat johtaa tietoturvakäytänteiden rikkomiseen.

(Rao ym., 2021.) Turvallisuusstressiä ja siihen liittyvää tutkimusta käsitellään tarkemmin seuraavassa pääluvussa.

3.3 Tietoturvakäyttäytymisen muuttuminen

Karjalaisen, Sarkerin ja Siposen (2019) mukaan tietoturvakäyttäytymistä on lähes kaikissa aihepiirin aikaisemmissa tutkimuksissa tutkittu yleensä staattisena ja muuttumattomana ilmiönä, jota selittämään on käytetty erilaisia teorioita, kuten aiemmassa alaluvussa mainittuja pelote- ja suojelumotivaatioteoriaa. Dynaamisuuden ulottuvuuden puuttumisen takia he loivat tietoturvakäyttäytymisen dialektisen prosessimallin (kuvio 4), joka kuvaa työntekijöiden tietoturvakäyttäytymisen muuttumista organisaatiokontekstissa. Prosessimalli alkaa kuvaamalla työntekijän tilannetta työsuhteensa alkuvaiheessa, jossa hän tutustuu organisaation nykyisiin tietoturvakäytänteisiin. Organisaation nykyiset mutta työntekijälle uudet tietoturvakäytänteet voivat aiheuttaa erilaisia dialektisia jännitteitä, jotka toimivat tietoturvakäyttäytymisen muutoksen käynnistäjänä. Nämä jännitteet ovat ympäristö, priorisoitujen tavoitteiden taso, motivaatioajuri ja aikahorisontti, joista ensimmäinen liittyy työympäristön tietoturvariskien mahdollisuuteen. Työntekijän odotetaan suhtautuvan tietoturvallisuuden kannalta yhtäaikaisesti sekä epäilevästi työympäristöään kohtaan että luottamaan siihen organisaation normien vuoksi tasapainottelee työympäristöön luottamisen ja sen epäilemisen välillä, joka aiheuttaa tasapainottelua epäilemisen ja luottamisen välillä. Jännitteet voivat liittyä myös priorisoitujen tavoitteiden tasoon. Tietoturvakäyttäytyminen voi olla institutionaalista, jolloin tietoturvakäytänteitä noudatetaan organisaation sisäisten normien vuoksi. Niitä voidaan kuitenkin myös rikkoa esimerkiksi niiden noudattamisesta aiheutuneen kuormituksen takia, jolloin tietoturvatavoitteet muuttuvat yksilöllisiksi. Kolmantena jännitetyyppinä on instrumentaalinen ja sosioemotionaalinen motivaatio, jotka kuvaavat tietoturvakäytänteiden noudattamisen perustana olevaa motivaatiota. Instrumentaalinen motivaatio viittaa tietoturvakäytänteiden noudattamisen käsinkosketeltaviin hyötyihin, ja tällöin tunneside on heikko. Sosioemotionaaliseen motivaatioon liittyy vastavuoroisesti vahva tunneside, ja tietoturvakäytänteitä noudatetaan siitä aiheutuvien sosiaalisten ja emotionaalisten hyötyjen toivossa. Viimeinen jännitetyyppi on aikahorisontti, joka kuvaa tietoturvakäytänteiden noudattamisesta tai rikkomisesta aiheutuvia pitkäaikaisia ja välittömiä vaikutuksia. Tietoturvakäytänteiden rikkomisella työtehtävien nopeamman suorittamisen kannalta voidaan kokea olevan välittömämpiä hyötyjä niiden noudattamiseen verrattuna, mutta jokainen rike voi kuitenkin nostaa tietoturvariskien toteutumisen mahdollisuutta sekä yksilölle että organisaatiolle. (Karjalainen ym. 2019.)



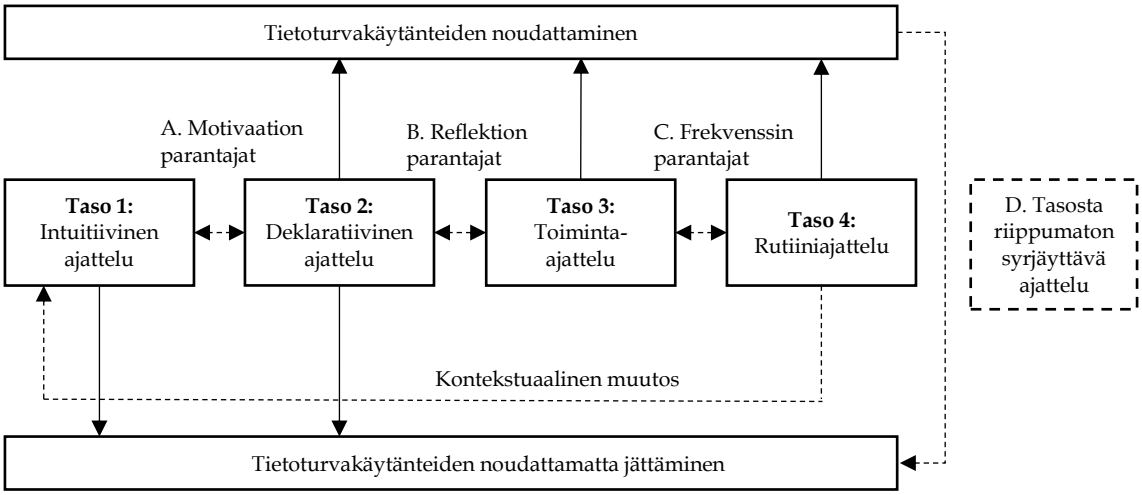
KUVIO 4 Tietoturvakäyttäytymisen dialektinen prosessimalli (Karjalainen, Sarker & Siponen, 2019, s. 692)

Edellä mainitut jännitteet käynnistävät tietoturvakäyttäytymiseen muuttumisen, sillä jännitteitä pyritään tasapainottamaan neljällä erilaisella kognitiivisella toiminnalla, jotka ovat priorisointi, ailahtelu, sovittelu ja ylittäminen. Priorisointi tarkoittaa jokaisesta neljästä jännitteestä toisen ääripään valitsemista hallitsevaksi tietoturvakäyttäytymiseen vaikuttavaksi tekijäksi. Ailahtelu puolestaan tarkoittaa tietoturvakäyttäytymisen muuttamista tilannekohtaiseksi, jolloin työntekijä voi vaihdella käyttäytymistään. Sovittelu viittaa vastaavasti jännitetyyppien molempien ääripäiden osittaiseen priorisointiin ja ylittäminen molempien ääripäiden korkeaan priorisointiin. (Karjalainen ym. 2019.)

Jännitteitä tasapainottava toiminta voi muuttaa työntekijöiden tietoturvakäyttäytymisen tietoturvakäytänteitä noudattavaksi, noudattamatta jättäväksi, osittain noudattavaksi tai luovien ratkaisujen keksijäksi. Priorisointi johtaa yleensä käyttäytymisen muuttumisen joko tietoturvakäytänteitä noudattavaksi tai noudattamatta jättäväksi, kun taas ailahtelu voi aiheuttaa vaihtelua noudattamisen ja noudattamatta jättämisen välillä. Sovittelutoiminta johtaa usein tietoturvakäytänteiden osittaiseen noudattamiseen, ja ylittäminen puolestaan luovien ratkaisujen keksimiseen. Muuttuneessa tietoturvakäyttäytymisessä pysyttely voi muuttua työntekijälle tavaksi, jos hän vahvistaa tietoturvakäyttäytymistään rutiininomaisesti. Tällöin tietoturvakäyttäytymistä aletaan toteuttaa ilman tasapainottavaa toimintaa. Muuttuneeseen tietoturvakäyttäytymiseen voi kuitenkin liittyä myös käyttäytymisspesifejä tietoturvakäyttäytymisen muutoksen käynnistäjiä, kuten äkilliset muutokset, jotka edelleen vaikuttavat ja muuttavat työntekijän tietoturvakäyttäytymistä. Näitä tekijöitä ovat esimerkiksi ympäristöolosuhteiden muuttuminen, tilanteen muuttuneet vaatimukset ja yksilöllisten

kyvykkyyksien muutos. Ympäristömuutoksiin lukeutuu esimerkiksi organisaation sisällä tapahtuvat muutokset, ja tilanteen vaatimusten muutoksia ovat puolestaan esimerkiksi sosiaaliset keskeytykset. Yksilöllisten kyvykkyyksien muutos liittyy esimerkiksi teknologiaan liittyvään tiedonjanoon ja oppimiseen. (Karjalainen ym. 2019.)

Toinen viimeaikainen kontribuutio tietoturvakäyttäytymisen muuttumisen tutkimuksessa on Karjalaisen, Siposen ja Sarkerin (2020) luoma tietoturvakäyttäytymisen kehittymisen tasomalli (kuvio 5), joka pyrki täyttämään tietoturvakäyttäytymisen muuttumiseen liittyvän tutkimuskirjallisuusaukon Karjalaisen ym. (2019) prosessimallin tavoin. Kuten Karjalainen ym. (2019) totesivat, että tietoturvakäyttäytymistä on yleensä tutkittu staattisena ilmiönä, myös Karjalainen ym. (2020) pitävät tietoturvakäyttäytymisen aikaisempia tutkimuksia ajattomina tilannekatsauksina tietyn hetken tietoturvakäyttäytymisestä.



KUVIO 5 Tietoturvakäyttäytymisen kehittymisen tasomalli (Karjalainen, Siponen & Sarker, 2020, s. 5)

Tasomalli pitää sisällään neljä tietoturvakäyttäytymiseen liittyvää ajattelun tasoa, ja tasojen välillä on tasolta seuraavalle siirtymiseen liittyviä tekijöitä. Ensimmäinen taso, eli intuitiivinen ajattelu, muodostuu työntekijän aikaisemmista tietoturvaan liittyvistä kokemuksista ja koulutuksesta. Tällä ajattelun tasolla olevilla työntekijöillä ei välttämättä ole vahvaa tietoturvaosaamista, jonka avulla he voisivat intuitiivisesti noudattaa organisaation tietoturvakäytänteitä. Päinvastoin työntekijöiden tietoturvakäyttäytyminen voi tällä tasolla olla tietoturvakäytänteiden vastaista, sillä tietoturvakäyttäytymiseen liittyviä päätöksiä tehdään henkilökohtaisten kokemuksien mukaan intuitiivisesti. Intuitiivisen tason työntekijät ovat siis yleensä tietämättään osaamattomia. Tason tyypilliseen tietoturvakäyttäytymiseen kuuluu myös erottelu, jolla tarkoitetaan vastuun siirtämistä tietoturvasta esimerkiksi IT-osastolle. Työntekijät eivät siis välttämättä ymmärrä olevansa myös itse vastuussa tietoturvasta, vaan uskovat vastuun kuuluvan ainoastaan organisaation IT-osastolle. Tietoturvataitojen yliarviointi ja tietoturvasta kuuluvan vastuun siirtäminen toimivat tietoturvakäyttäytymisen muuttumisen esteenä. (Karjalainen ym., 2020.)

Ensimmäiseltä tasolta siirtyminen toiselle tasolle on yleensä motivaatiokysymys ja siihen liittyy sisäisiä, ulkoisia ja organisatorisen hallinnan motivaatiotekijöitä. Tietoturvakäyttäytymisen ja siihen liittyvän ajattelun kehittymisen motivaatio on harvoin spontaania tai työntekijälähtöistä, joten sisäisellä motivaatiolla ei ole siinä yleensä vahvaa roolia. Tämä johtuu siitä, että tietoturvakäytänteiden noudattaminen ja työntekijän sisäinen motivaatio voivat olla ristiriidassa, jonka vuoksi tietoturvakäyttäytymisen kehittyminen vaatii yleensä ulkoisia ja organisatoriseen hallintaan liittyviä motivaatiotekijöitä. Ulkoisiin motivaatiotekijöihin lukeutuvat muun muassa media tai tietoturvatapauksissa mukana oleminen henkilökohtaisesti tai välillisesti. Organisatorisiin hallinnan motivaatiotekijöihin kuuluu esimerkiksi organisaation johdon tekemät toimenpiteet tietoturvaan liittyen. Sekä ulkoiset että organisatorisen hallinnan motivaatiotekijät voivat kehittää tietoturvakäyttäytymistä intuitiivisen ajattelun tasolta toiselle tasolle, eli deklaratiivisen ajattelun tasolle. (Karjalainen ym., 2020.)

Intuitiivisen ajattelun tason selittäessä vain tietoturvakäytänteiden noudattamatta jättämistä, deklaratiivinen taso voi selittää sekä tietoturvakäytänteiden noudattamista että niiden noudattamatta jättämistä. Deklaratiivisen ajattelun tasolla työntekijät pystyvät arvioimaan omaa tietoturvakäyttäytymistään opittujen asioiden pohjalta. Tasolla olevilla työntekijöillä ei kuitenkaan ole vielä kunnollista ymmärrystä tietoturvakäytänteiden tärkeydestä heille relevantissa organisaatiokontekstissa, joten he saattavat rikkoa niitä, myös tietoisesti. Tietoturvakäytänteitä yleensä rikotaan, mikäli rikkomisesta aiheutuva hyöty koetaan tietoturvakäytänteiden noudattamista tärkeämmäksi. Tietoturvakäytänteiden noudattaminen deklaratiivisella tasolla vaatii yleensä ulkoisia tekijöitä, kuten esimiehen käskyä tai muiden työntekijöiden tietoturvakäyttäytymisen seuraamista. (Karjalainen ym., 2020.)

Deklaratiiviselta tasolta toiminta-ajattelun tasolle siirtymiseen liittyy erilaisia reflektointitekijöitä, sillä tietoturvakäyttäytymisen parantuminen vaatii toisella tasolla olevalta työntekijältä itsereflektointia. Reflektiotekijöitä ovat kokemusperäinen oppiminen ja yhteisoppiminen, joista ensimmäisellä tarkoitetaan tietoturvarikkomuksien jälkeistä henkilökohtaista reflektointia, eli tietoturvakäyttäytymisen pohdintaa. Yhteisoppimisella puolestaan viitataan siihen, että esimerkiksi tietoturvakoulutuksien sijaan, joissa tieto siirtyy opettajalta työntekijälle, työntekijä voi osallistua muun muassa tietoturvakäytänteiden kehitykseen, jolloin aktiivista tietoturvaan liittyvän tiedon siirtymistä tapahtuu kahdensuuntaisesti. (Karjalainen ym., 2020.)

Kolmannella tasolla, eli toiminta-ajattelun tasolla, tietoturvakäyttäytyminen muuttuu itseohjautuvaksi ja työntekijä on tietoisesti kykeneväinen noudattamaan tietoturvakäytänteitä. Tällä tasolla oleva työntekijä pystyy arvioimaan tietoturvakäyttäytymisestään aiheutuvia tietoturvariskejä ja tietoturvakäytänteiden tehokkuutta riskien pienentämisessä. Vaikka toiminta-ajattelun tasolla työntekijät yleensä noudattavat tietoturvakäytänteitä hyvin, voi tasosta riippumaton syrjäyttävä ajattelu kuitenkin aiheuttaa tietoturvakäytänteiden noudattamatta jättämistä. (Karjalainen ym., 2020.)

Tasosta riippumattomalla syrjäyttävällä ajattelulla tarkoitetaan työntekijöiden tietoturvakäyttäytymiseen vaikuttavia tilannekohtaisia ja kontekstuaalisia rajoitteita, joihin lukeutuu työympäristö, oikaiseminen, sosiaalinen paine ja opportunismi. Työympäristö rajoitteena tarkoittaa, että työntekijät luottavat teknisiin tietoturvateknologioihin ja toisiin työntekijöihin niin paljon, etteivät usko tietoturvariskien realisoitumisen mahdollisuutta. Työntekijät saattavat siis tunnistaa esimerkiksi tietokoneen lukitsematta jättämisen olevan tietoturvariski, mutta päättävät jättää sen lukitsematta turvalliseksi koetun työympäristön takia. Toinen rajoite, eli oikaisu, liittyy tietoturvakäytänteiden rikkomiseen tai noudattamatta jättämiseen esimerkiksi kiireen tai stressin takia. Tietokone saatetaan jättää lukitsematta silloin, kun sen ääreltä poistutaan vain hetkeksi. Kolmantena rajoitteena oleva sosiaalinen paine voi olla sisäistä tai ulkoista. Sisäisellä sosiaalisella paineella tarkoitetaan esimerkiksi tietokoneen lukitsematta jättämistä toisten työntekijöiden ollessa läsnä, sillä se voitaisiin kokea nolona. Ulkoinen sosiaalinen paine puolestaan tarkoittaa arkaluonteisen tiedon paljastamista uhattuna olemisen kokemisen takia. Viimeisenä rajoitteena oleva opportunismi viittaa tietoturvakäytänteiden rikkomiseen henkilökohtaisen edun tavoittelun vuoksi. Työntekijä voisi siis rikkoa tietoturvakäytänteitä tietoisesti esimerkiksi taloudellisen hyödyn vuoksi. (Karjalainen ym., 2020.)

Kolmannen ja neljännen tason väliin liittyy frekvenssin parantajia, joiden tarkoituksena on tehdä kolmannen tason toiminta-ajattelusta ja tietoturvakäytänteitä noudattavasta tietoturvakäyttäytymisestä rutiininomaista vahvistamalla oikeanlaista käytöstä. Jos vahvistusta ei tapahdu, niin työntekijät eivät välttämättä ymmärtämään tietoturvakäytänteiden noudattamisen tärkeää merkitystä, eikä tietoturvakäytänteiden noudattamisesta tule rutiininomaista. Tietoturvakäyttäytyminen voi siis muuttua tietoturvakäytänteitä noudattamatta jättäväksi, mikäli työntekijä ei koe tietoturvakäytänteitä noudattavasta tietoturvakäyttäytymisensä suotuisia vaikutuksia. Neljännellä tasolla, eli rutiiniajattelun tasolla, tietoturvakäytänteitä noudatetaan rutiininomaisesti ja vakiintuneesti, eikä niiden noudattaminen vaadi enää huomattavaa kognitiivista työmäärää. Taso riippumattoman syrjäyttävän ajattelun vaikutus ei ole enää neljännellä tasolla yhtä vahva kuin edeltäville tasoilla, eikä siis heikennä tietoturvakäyttäytymistä yhtä helposti. (Karjalainen ym., 2020.)

4 TURVALLISUUSSTRESSI

Tässä luvussa käydään läpi kirjallisuuskatsauksen viimeinen teoreettinen osa-alue, eli turvallisuusstressi. Luku on jaettu neljään alalukuun, joista ensimmäisessä käydään läpi lyhyesti teknostressin ilmiö. Toisessa alaluvussa käydään läpi tämän tutkielman tärkein teoria, eli turvallisuusstressi ja sen stressitekijät. Kolmannessa alaluvussa kartoitetaan turvallisuusstressin tutkimuksessa useimmiten käytettyjä teorioita ja miten ne soveltuvat tutkimusaiheen tutkimukseen. Viimeisessä alaluvussa käydään läpi turvallisuusstressin aiempi tutkimus ja tärkeimmät tutkimustulokset.

4.1 Teknostressi ilmiönä

Teknostressi määriteltiin ensimmäisen kerran 1980-luvulla stressiksi, joka aiheutuu teknologiasta ja sen käytöstä. Teknostressiä aiheuttaa kyvyttömyys sopeutua käyttämään teknologiaa (Brod, 1982). Teknostressiä on sittemmin tutkittu runsaasti lisää, mutta yhdeksi suosituimmaksi tutkimukseksi on muodostunut Tarafdarin, Tun, Ragu-Nathanin ja Ragu-Nathanin (2007) tutkimus, jossa teknostressille määriteltiin viisi eri kuormittajatyyppiä organisaatiokontekstissa (taulukko 6). Teknostressin kuormittajatyypit ovat ylikuormitus, invaasio, monimutkaisuus, turvattomuus ja epävarmuus. Ylikuormituksella tarkoitetaan, että informaatiota tulee useista eri lähteistä niin paljon, ettei sitä pystytä enää hallitsemaan. Informaatiotulva pakottaa työntekijät työskentelemään enemmän ja nopeammin, joka aiheuttaa stressiä. Invaasio tarkoittaa esimerkiksi työn ja vapaa-ajan rajan heikentymistä kokoaikaisen saavutettavuuden takia, jolloin työntekijät kokevat, että he ovat aina yhteydessä teknologiaan. Monimutkaisuus stressitekijänä on monimutkaisen teknologian käytön ja siihen liittyvän vaikeaselkoisen sanaston aiheuttamaa stressiä, jolloin itse teknologia ja sen käyttö koetaan hyvin monimutkaisena. Turvattomuudella puolestaan tarkoitetaan teknologian käytön kyvyttömyyden tunteesta aiheutuvaa pelkoa siitä, että työntekijä korvataan toisella työntekijällä, jolla on paremmat teknologiataidot. Epävarmuudella

tarkoitetaan teknologian jatkuvasta kehittymisestä ja muuttumisesta aiheutuvaa stressiä, jolloin työntekijät joutuvat jatkuvasti vastaavasti myös opettelemaan uuden teknologian käyttöä. Teknostressillä on havaittu olevan useita negatiivisia vaikutuksia, joista yhtenä esimerkkinä on heikentynyt työtehokkuus. (Tarafdar ym., 2007.)

TAULUKKO 6 Teknostressin stressitekijät (Tarafdar ym., 2008)

Teknostressin stressitekijä	**Selitys**
Ylikuormitus (engl. *techno-overload*)	Teknologia pakottaa työskentelemään nopeammin ja pidempään.
Invaasio (engl. *techno-invasion*)	Aina saavutettavissa olemisen tunne teknologian vuoksi sekä työn ja vapaa-ajan raja heikentyminen
Monimutkaisuus (engl. *techno-complexity*)	Teknologian monimutkaisuus aiheuttaa osaamattomuuden tunnetta ja pakottaa opettelemaan teknologian käyttöä.
Turvattomuus (engl. *techno-insecurity*)	Pelko työpaikan menettämisestä paremmat IT-taidot omaavalle työntekijälle.
Epävarmuus (engl. *techno-uncertainty*)	Epävarmuuden tunteen aiheutuminen jatkuvasti muuttuvasta teknologiasta.

4.2 Turvallisuusstressi ilmiönä

Turvallisuusstressin (engl. *security-related stress, SRS*) tutkimus käynnistyi vuonna 2014, kun D'Arcy, Herath ja Shoss (2014) määrittelivät turvallisuusstressin olevan organisaatioiden turvallisuusvaatimuksista ja niiden noudattamisesta työntekijöille aiheutuvaa stressiä. Turvallisuusvaatimuksilla tarkoitetaan yrityksen käyttämiä tietoturvakäytänteitä. Turvallisuusstressin stressitekijöiden määrittelyssä hyödynnettiin jo olemassa olevia teknostressin stressitekijöitä, joista turvallisuusstressiä aiheutumista valittiin kuvaamaan ylikuormitus, monimutkaisuus ja epävarmuus (taulukko 7) (D'Arcy ym., 2014).

Turvallisuusstressin ylikuormituksella tarkoitetaan turvallisuusvaatimusten aiheuttamaa työmäärän lisääntymistä ja siitä johtuvan työtehtäviin käytettävissä olevan ajan vähentymisen aiheuttamaa stressiä. Organisaation turvallisuusvaatimukset voivat esimerkiksi määrätä tietokoneen käyttöoikeuksien lisäämisestä vain tarvittaessa, jolloin työtehtävien vaatiessa työntekijöiden täytyy käyttää niiden hakemiseen työaikaa. Tämän vuoksi työntekijöiden täytyy tehdä työtehtävänsä nopeammin turvallisuusvaatimusten noudattamisen vuoksi, jotta työtehtävät tulevan tehtyä ajoissa. Ylikuormitus voi näkyä myös esimerkiksi turvallisuusvaatimusten vaatimina tietokoneen tietoturvapäivityksinä, jotka voivat hidastaa tietokoneen käyttöä tai jopa kokonaan estää sen, joka lisää työtehtävien tekemisen aikapainetta. (D'Arcy ym., 2014.)

Monimutkaisuus stressitekijänä liittyy tietoturvakäytänteiden hankalaan ymmärrettävyyteen tai työntekijät kokevat ne monimutkaisina. Tietoturvakäytänteet voivat sisältää esimerkiksi työntekijöille vieraita termejä ja kieltä, jolloin

niiden ymmärtämiseen täytyy käyttää ylimääräistä aikaa. Työajan käyttäminen tietoturvakäytänteiden opetteluun on työntekijöiltä pois päivittäisten työtehtävien käytettävissä olevasta ajasta, jonka vuoksi ylimääräisen ajan käyttö voi aiheuttaa stressiä. (D'Arcy ym., 2014.)

TAULUKKO 7 Turvallisuusstressin stressitekijät (D'Arcy ym., 2014)

Turvallisuusstressin stressitekijä	**Selitys**	**Esimerkki**
Ylikuormitus	Tietoturvakäytänteet lisäävät työmäärää ja vähentävät työtehtävien tekemiseen käytettävissä olevaa aikaa.	Tietokoneen käyttöä hidastava tai kokonaan estävä tietoturvapäivitys.
Monimutkaisuus	Tietoturvakäytänteiden opetteluun on käytettävä aikaa niiden monimutkaisuuden tai epäselvyyden takia.	Tietoturvakäytänteissä käytettävä IT-alan ammattisanasto tai -slangia.
Epävarmuus	Tietoturvakäytänteet muuttuvat usein tai niiden muuttuminen on epävarmaa.	Uudet säädökset ja teknologiat aiheuttavat muutoksia tietoturvakäytänteisiin.

Kolmantena turvallisuusstressin stressitekijänä oleva epävarmuus tarkoittaa joko yrityksen sisäisistä tai ulkoisista tekijöistä aiheutuvia tietoturvakäytänteiden muutoksia. Yritys voi esimerkiksi joutua päivittämään tietoturvakäytänteitään esimerkiksi tapahtuneen tietoturvaonnettomuuden, uuden käyttöönotetun teknologian tai uusien lakien ja säädöksien vuoksi. Tietoturvakäytänteiden jatkuva muuttuminen voi aiheuttaa työntekijöissä epävarmuutta ja lopulta stressin muodostumiseen, sillä tietoturvakäytänteiden muuttuessa uudet käytänteet tulee myös opetella.

D'Arcyn ym. (2014) tutkimusartikkelissa turvallisuusstressiä tutkittiin selviämisteorian ja moraalisen irtautumisteorian näkökulmasta. Turvallisuusstressin aiheutumistapa ensinnäkin kuvattiin johtuvan selviämisteorian mukaisten primääri- ja sekundaariarvioiden yhteisvaikutuksesta. Työntekijät päätyvät yleensä käyttämään tunnekeskeistä selviytymistapaa silloin, jos he kokevat, etteivät voi vaikuttaa stressaavaan tilanteeseen välittömästi. Tämän vuoksi turvallisuusstressistä selviämistä tutkittiin nimenomaan tunnekeskeisen selviämistavan näkökulmasta, sillä työntekijöillä ei yleensä ole mahdollisuutta vaikuttaa suoraan stressin lähteeseen, eli tietoturvakäytänteisiin, sillä heidän edellytetään noudattavan niitä (D'Arcy ym., 2014).

D'Arcy ym. (2014) käyttivät tutkimuksensa teoreettisena viitekehyksenä selviämisteorian lisäksi myös moraalista irtautumisteoriaa, sillä selviämisteoria tai aikaisempi tutkimuskirjallisuus ei määrittele tunnekeskeisten selviämistapojen tarkkoja toimintatapoja. Moraalisen irtautumisteorian useat määritelmät vastaavat selviämisteorian tunnekeskeisen selviämistapojen määritelmiä, joten sen voidaan katsoa laajentavan ja tarkentavan selviämisteorian esittelemiä tunnekeskeisien selviämistapojen yleisiä periaatteita. Moraalista irrottautumisteoriaa voidaan lisäksi käyttää työntekijöiden epätoivotun käyttäytymisen ja sen järkeistämisen selittämiseen, joka toimii työntekijöille myös tunnekeskeisenä

selviämistapana. Moraalinen irtautuminen tarjoaa työntekijöille selviytymismekaniikan tietoturvakäytänteiden stressaavuutta vastaan, jolla työntekijät järkeistävät tietoturvakäytänteiden rikkomisensa. Tämän vuoksi tutkimuksessa johdettiin, että suurin osa tietoturvakäytänteiden rikkomisista tapahtuu hyväntahtoisten työntekijöiden toimesta, joiden tarkoituksena ei ole tahallaan rikkoa tietoturvakäytänteitä. Tutkimuksen tärkeimpänä tutkimustuloksena voidaan pitää tietoturvakäytänteistä ja niiden noudattamisesta aiheutuvan turvallisuusstressin aiheutumisen todistamista. Tutkimus myös osoitti turvallisuusstressin ja tietoturvakäytänteiden rikkomisen välisen yhteyden toteen. (D'Arcy ym., 2014.)

4.3 Teoriat turvallisuusstressin tutkimuksessa

Turvallisuusstressitutkimuksessa on käytetty varsin erilaisia teorioita kuin tietoturvakäyttäytymisen tutkimuksessa, ja ne painottuvat usein psykologiaan ja sosiaalitieteisiin. Yleisimpiä käytettyjä teorioita ovat muun muassa selviämisteoria, moraalinen irtautumisteoria ja rooliteoria. Kirjallisuuskatsauksen perusteella tunnistetut teoriat on koottu alla olevaan taulukkoon (taulukko 8).

TAULUKKO 8 Käytetyimmät teoriat turvallisuusstressitutkimuksessa

Teoria	**Esimerkki turvallisuusstressin kontekstissa**
Selviämisteoria (engl. *coping theory*)	Selviämisteoria tarjoaa selviämistavan turvallisuusstressiä kokeville. (D'Arcy ym., 2014)
Moraalinen irtautumisteoria (engl. *moral disengagement theory, MDT*)	Tietoturvakäytänteiden rikkomista vähättelevä puhetyyli. (D'Arcy ym., 2014.)
Henkilön ja organisaation yhteensopivuusmalli (engl. *person-organization fit model*)	Puutteelliset kyvykkyydet johtavat organisaation vaatimien tietoturvakäytänteiden noudattamisen rikkomiseen. (Lee ym., 2016)
Tunnepitoisten tapahtumien teoria (engl. *affective events theory, AET*)	Tunteet vaikuttavat merkittävästi tietoturvakäytänteiden noudattamisaikomukseen. (D'Arcy & Teh, 2019)
Rooliteoria (engl. *role theory*)	Koettu rooliepäselvyys voi aiheuttaa tietoturvakäytänteiden rikkomista. (Nasirpouri Shadbad & Biros, 2021)

Lazaruksen ja Folkmanin esittelemä (1984) selviämisteoria (engl. *coping theory*) kuvaa koetun stressin jälkeisiä vaikutuksia yksilöissä sekä käytöksellisiä ja kognitiivisia tapoja hallita stressiä. Teorian mukaan tilanteen stressaavuus arvioidaan kahdella yhtäaikaisesti tapahtuvalla arviolla, joista ensimmäisessä yksilö arvioi kyseessä olevan tilanteen merkittävyyden ja stressaavuuden, ja toisessa arviossa tarkastelee, kuinka paljon tilanteeseen voi itse vaikuttaa. (Lazarus & Folkman, 1984.) Turvallisuusstressin kontekstissa primääriarviointi tapahtuu, kun työntekijät kokevat tietoturvakäytänteistä aiheutuvaa ylikuormitusta, monimutkaisuutta tai epävarmuutta. Sekundaariarviossa työntekijät kokevat, etteivät voi itse vaikuttaa tietoturvakäytänteisiin, sillä heidän edellytetään niitä noudattavan.

Kaksi yleisintä tapaa turvallisuusstressistä selviämiseen ovat selviämisteorian kuvaamat tunnekeskeinen ja ongelmakeskeinen selviämistapa (D'Arcy ym., 2014). Tunnekeskeiseen selviämiseen liittyy kognitiivisia prosesseja, kuten käyttäytymisen järkeistämistä tai itsensä irrottaminen stressaavasta tilanteesta, joilla yksilö muuttaa stressaavaan tilanteeseen liittyviä asenteitaan stressin lievittämiseksi. Ongelmakeskeisessä selviämisessä puolestaan yksilö pyrkii muuttamaan stressaavan tilanteen vähemmän stressaavaksi. Selviämistapa tunnekeskeisen ja ongelmakeskeisen tapojen välillä valikoituu stressaavan tilanteen hallittavuuden perusteella – mitä hallittavammaksi tilanne arvioidaan, sitä todennäköisemmin selviämistapana on ongelmakeskeinen selviäminen. (Lazarus & Folkman, 1984.)

Banduran, Barbaranellin, Capraran ja Pastorellin (1996) esittelemä moraalinen irrottamisteoria (engl. *moral disengagement theory*) kuvaa kahdeksan mekanismia kolmessa laajemmassa kategoriassa, joilla yksilö kytkee pois päältä vahingollisen käyttäytymisen mahdollistavan moraalisen itsesäätelyn. Ensimmäinen kategoria, käyttäytymisen uudelleenrakentaminen, sisältää kolme mekanismia, jotka kohdistuvat suoraan vahingolliseen käyttäytymiseen. Moraalisessa oikeutuksessa yksilö tekee käyttäytymisestään sekä sosiaalisti että henkilökohtaisesti moraalisesti hyväksyttävää. Tämä voi näkyä esimerkiksi väkivaltaisen teon moraalisessa oikeuttamisessa oman maineen ylläpitämiseksi. Toisena mekanismina on kaunisteleva kielenkäyttö, jolla vahingollisesta teosta saadaan hyväksyttävä puhumalla siitä suotavaan sävyyn. Viimeisenä mekanismina on verrata omaa vahingollista käyttäytymistä johonkin toiseen vahingollisempaan käyttäytymiseen, jolloin oma käyttäytyminen vaikuttaa jopa hyödylliseltä tämän kontrastieron vuoksi. Näiden mekanismien käyttö vahingollisen käyttäytymisen järkeistämisessä on yksilöille kaikkein tehokkainta, sillä ne mahdollistavat käyttäytymisen itsehyväksynnän. (Bandura ym., 1996.)

Toinen moraalisen irrottamisteorian mekanismikategoria on seuraamuksien vähättely tai vääristely, joka sisältää vastuun siirtämisen, hajauttaminen ja seuraamuksien vääristämisen. Vastuun siirtämisessä yksilö katsoo vahingollisen käyttäytymisensä johtuvan muista ihmisistä tai sosiaalisesta paineesta ja näin siirtää vastuun itseltään pois. Vastuun hajauttaminen puolestaan tarkoittaa sitä, että yksilö katsoo myös muiden ihmisten olevan vastuussa vahingollisesta käyttäytymisestä, jolloin yksilön kokema oma vastuu käyttäytymisestä pienenee. Kolmantena mekanismina oleva seuraamuksien vääristäminen kuvaa toimintaa, jossa yksilö minimoi tai välttelee vahingollisesta toiminnastaan aiheutuvia seuraamuksia. (Bandura ym., 1996.)

Kolmannen kategorian mekanismit kohdistuvat vahingollisen käyttäytymisen kohteeseen ja sisältää epäinhimillistämisen ja syyttömyyden. Epäinhimillistämisellä tarkoitetaan, ettei yksilö katso vahingollisen käyttäytymisen kohteena olevaa henkilöä ihmisenä, jolloin häneen kohdistuva vahingollinen teko on yksilölle helpompi suorittaa. Syyttömyys puolestaan tarkoittaa sitä, että vahingollisesti käyttäytynyt yksilö kokee olevansa syytön uhri itsestään riippumattomaan tilanteeseen. (Bandura ym., 1996.)

D'Arcy ym. (2014) sovelsivat moraalisen irrottamisteorian mekanismeja turvallisuusstressin kontekstiin ja tunnistivat mekanismeja vastaavat työntekijöiden tietoturvakäytänteisiin liittyviä käyttäytymismekanismeja, jotka käyvät ilmi alla olevasta taulukosta (taulukko 9).

TAULUKKO 9 Moraalisen irtautumisteorian irtautumismekanismit tietoturvakäyttäytymisessä (D'Arcy ym., 2014, s. 293–294 mukaillen)

Mekanismi	**Tietoturvakäytänteiden konteksti**
Moraalinen oikeutus	Tietoturvakäytänteiden rikkominen työtehtävien tehokkaamman tekemisen tai työtehtävän määräajassa suorittamisen vuoksi.
Kaunisteleva kielenkäyttö	Tietoturvakäytänteiden rikkomista vähättelevä puhetyyli.
Suotuisa vertailu	Tietoturvakäytänteiden rikkomisen vertaaminen vakavimpiin rikkomuksiin, kuten organisaation omaisuuden varastamiseen.
Vastuun siirtäminen	Tietoturvakäytänteiden rikkominen suuren työmäärän vuoksi, jolloin rikkomisesta ei tarvitse olla vastuussa.
Vastuun hajauttaminen	Työntekijä kokee yrityksen johdon tai esimerkiksi IT-osaston olevan enemmän vastuussa tietoturvasta.
Seuraamuksien vääristely	Tietoturvakäytänteiden rikkomisella ei koeta olevan harmia yritykselle tai muille työntekijöille.
Epäinhimillistäminen	Tietoturvakäytänteiden rikkominen vaikuttaa ainoastaan epäinhimilliseen organisaatioon eikä muihin henkilöihin.
Syyttömyys	Tietoturvakäytänteiden rikkominen niiden liiallisen epäreiluuden tai tiukkuuden vuoksi.

Henkilön ja ympäristön yhteensopivuusmalli (engl. *person-environment fit model*) sisältää useita eri alamalleja, kuten henkilön ja työn yhteensopivuus, mutta turvallisuusstressitutkimuksessa sopivin alamalli on henkilön ja organisaation yhteensopivuutta kuvaava malli (engl. *person-organization fit model*). Se kuvaa työntekijän ja yrityksen välistä tasapainoa, joka järkkyessään aiheuttaa stressiä. Turvallisuusstressin näkökulmasta tämä voi näkyä esimerkiksi, kun yrityksen käyttämien tietoturvakäytänteiden noudattamisesta aiheutuva työmäärä ylittää työntekijän henkilökohtaiset kyvykkyydet. Toisin sanoen, jos henkilökohtaisten kyvykkyyksien avulla ei pystytä noudattamaan organisaation vaatimiin tietoturvakäytänteitä, niitä yleensä rikotaan. (Lee, Lee & Kim, 2016.)

Weissin ja Cropanzanon (1996) esittelemä tunnepitoisten tapahtumien teoria (engl. *affective events theory*, AET) käsittelee tunteisiin liittyviä tapahtumia työpaikalla. Se sisältää tunnepitoisten tapahtumien rakenteet, syyt ja seuraukset ja pitää niitä työntekijöiden tunnereaktioiden aiheuttajina. Teoria lisäksi huomioi keskeisesti ajan, sillä työntekijöiden kokemat tunnereaktiot vaihtelevat ajan kuluessa. Teorian kuvaamassa mallissa työympäristö vaikuttaa epäsuorasti työpaikalla tapahtuviin tapahtumiin sekä työntekijöiden asenteisiin työstä. Työpaikan tapahtumat aiheuttavat työntekijöissä tunnereaktioita, jotka vaikuttavat tunteista johtuvaan käyttäytymiseen sekä edelleen vaikuttavat työasenteisiin. Työasenteet puolestaan vaikuttavat työntekijöiden päätöksiin perustuvaan käyttäytymiseen. Tunnereaktiot vaikuttavat siis suoraan tunteisiin perustuvaan käyttäytymiseen, sekä työasenteiden vaikutuksien kautta päätöksiin perustuvaan

käyttäytymiseen. (Weiss & Cropanzano, 1996.) D'Arcy ja Teh (2019) totesivat tutkimuksessaan tunteiden olevan suuri vaikuttava tekijä työntekijöiden tietoturvakäytänteiden noudattamisessa.

Rooliteoria kuvaa ihmisten rooleja eri tilanteissa ja olettaa, että ihmisillä on omaan käyttäytymiseen ja muiden käyttäytymiseen liittyviä odotuksia. Teorialla on kolme keskeistä käsitettä, jotka ovat rooli, sosiaalinen paikka ja odotukset. Roolilla tarkoitetaan luonteenomaista käyttäytymistä, sosiaalisella paikalla roolin asemaa tai tehtäviä, ja odotuksilla käyttäytymistä. Rooliteorialla on viisi erilaista näkökulmaa: funktionaalinen, symbolinen vuorovaikuttaja, rakenteellinen, kognitiivinen ja viimeiseinä organisatorinen. Funktionaalisen rooliteorian kuvaa vakaata sosiaalista rakennetta ja ihmisten käyttäytymistä siinä. Ihmiset noudattavat opittuja sosiaalisia normeja ja tuomitsevat näistä normeista käytöksellään poikkeavat henkilöt. Funktionaalinen rooliteoria selittääkin siis sosiaalisen rakenteen vakautta ja rakenteen sosiaalisista normeista poikkeavaa käyttäytymistä. Symbolisen vuorovaikuttajan rooliteorian mukaan sosiaaliset normit ja roolit kehittyvät yksilöiden vuorovaikutuksen avulla. Sosiaalisia normeja ei kuvata tarkasti, vaan ne toimivat laajempina kokonaisuuksina, jotka yksilöt tarkentavat vuorovaikutuksella muiden kanssa. Symbolinen vuorovaikuttaja rooliteoria onkin omiaan kuvaamaan epäformaalia vuorovaikutusta ja rooleja. Rakenteellinen rooliteoria puolestaan keskittyy formaalimpien sosiaalisten rakenteiden kuvaamiseen. Sosiaalisen rakenne pitää sisällään saman käyttäytymismallin, eli roolin, omaavia ihmisryhmiä, jotka kohdistavat vuorovaikutuksen muihin ihmisryhmiin. Kognitiivinen rooliteoria liittyy odotuksien vaikutuksiin roolien käyttäytymiseen. Sen mukaan yksilön omat odotukset sekä ulkopuolelta tulevat odotukset ja sosiaaliset normit ohjailevat yksilön roolin käyttäytymistä. Viimeisenä, organisatorinen rooliteoria kuvaa hierarkkisia ja työtehtäviin keskittyviä sosiaalisia rakenteita. Organisatorisessa rooliteoriassa yksilöt kokevat usein roolikonflikteista aiheutuvaa kuormitusta, joka syntyy organisaation sisäisistä sekä yksilöiden omista sosiaalisista normeista, joita organisaatiossa sijaitsevat roolit pyrkivät noudattamaan. Organisatorisessa rooliteoriassa kuvatut roolikonfliktit tarkoittavat, että yksilö kokee roolissaan useita erilaisia odotuksia ja nämä eri odotukset saavat yksilön kyseenalaistamaan, kuinka hänen tulisi käyttäytyä. Useiden erilaisten odotuksien aiheuttama roolikonflikti synnyttää yksilössä kuormitusta, joka vaikuttaa usein negatiivisesti käyttäytymiseen. Roolikonflikteihin liittyy myös roolin monitulkintaisuutta sekä roolin ylikuormitusta. Roolin monitulkintaisuus tarkoittaa, että odotukset eivät ole tarpeeksi tarkkoja ohjaamaan käyttäytymistä, ja rooliylikuormitus liittyy siihen, että roolilla on liian paljon odotuksia, jotka aiheuttavat ylikuormitusta. (Bibble, 1986.)

4.4 Turvallisuusstressin aikaisempi tutkimus

Turvallisuusstressistä löydettiin kirjallisuuskatsausta tehdessä yhteensä yhdeksän tutkimusta, joihin D'Arcyn ym. (2014) turvallisuusstressin alun perin tunnistanut tutkimus myös lukeutuu. Seuraavaksi tehty tutkimus on Leen ym. (2016)

tutkimus, joka käsitteli stressitekijöiden vaikutuksia tietoturvakäytänteiden noudattamiseen erityyppisissä organisaatioissa. Tutkimuksen valitsemat tarkasteltavat stressitekijät olivat yksityisyyden menettäminen ja työylikuormitus, joista ensimmäisellä tarkoitetaan tietoturvakäytänteiden noudattamisen valvontaa. Organisaatioiden tulee valvoa tietoturvakäytänteiden noudattamista ja valvonta yltää aina sähköpostin valvonnasta eri laitteiden valvontaan. Työntekijät voivat kokea tämän valvonnan heidän yksityisyyttään loukkaavana. Toinen stressitekijä, eli työylikuormitus, tarkoittaa käytännössä samaa kuin D'Arcyn ym. (2014) turvallisuusstressin ylikuormitus, eli tietoturvakäytänteiden noudattamisesta aiheutuva lisääntynyt työmäärä. Tutkimuksen tuloksien mukaan molemmat stressitekijät vaikuttivat negatiivisesti työntekijöiden tietoturvakäytänteiden noudattamiseen. Lisäksi havaittiin, että ylikuormituksella on suurempi negatiivinen vaikutus teknispainotteisissa organisaatioissa, joissa tietoturvalla on keskeinen rooli. Tutkimuksessa myös havaittiin, että työntekijöiden asenteilla tietoturvakäytänteiden noudattamista kohtaan oli ylikuormitusta ja yksityisyyden menettämistä lieventävä vaikutus. Lieventävän vaikutuksen suuruuteen vaikutti työntekijöiden tietoturvaosaaminen. Tutkimuksen keskeinen johtopäätös on, että ylikuormituksesta ja yksityisyyden menettämisestä aiheutuva stressi tulisi ottaa huomioon tietoturvakäytänteiden suunnittelussa näiden stressitekijöiden minimoimiseksi. (Lee ym., 2016.)

Ho-Jin ja Cho (2016) tutkivat tietoturvakäytänteiden noudattamisen aiheuttaman lisätyömäärän vaikutuksia työntekijöiden työtyytyväisyyteen. Tutkimuksessa havaittiin, että etenkin tekniset tietoturvakäytänteet aiheuttivat turvallisuusstressiä, joka puolestaan heikensi työntekijöiden työtyytyväisyyttä. Tietoturvakäytänteiden stressaavuuden syyn havaittiin liittyvän tietoturvakäytänteiden valvontaan ja työtehokkuuden heikkenemiseen tietoturvakäytänteiden noudattamisen takia. (Ho-Jin & Cho, 2016).

D'Arcy, Herath, Yim, Nam ja Rao (2018) toistivat D'Arcyn ym. (2014) tekemän tutkimuksen erilaisessa kontekstissa tarkoituksenaan vahvistaa tutkimuksen aikasemmat tutkimustulokset uudessa ympäristössä. Toistotutkimuksen kohderyhmä vaihdettiin eri maassa sijaitsevaan organisaatioon, ja toistotutkimuksessa tutkittiin alkuperäisestä tutkimuksesta poiketen vain yhden organisaation työntekijöitä. Tutkimus onnistui ja osoitti turvallisuusstressin aiheuttavan moraalista irtaantumista tietoturvakäytänteiden noudattamisen aikomuksista, joka johtaa aikomukseen rikkoa tietoturvakäytänteitä. (D'Arcy ym., 2018.)

Hwang ja Cha (2018) tutkivat kuinka turvallisuusstressi ja siitä johdettu roolistressi vaikuttavat työntekijöiden tietoturvakäytänteiden noudattamisaikomuksiin. Tulokset osoittivat, että turvallisuusstressiä aiheuttavat tekijät heikentävät työntekijöiden sitoutuneisuutta yritykseen, joka vaikutti negatiivisesti tietoturvakäyttäytymiseen. Turvallisuusstressiä aiheuttavista tekijöistä löydettiin myös yhteyksiä roolistressiin, eli työntekijän kokemasta stressistä omasta roolistaan organisaatiossa. Lisäksi tutkimus osoitti, että ylennyksen tavoitteleminen vaikutti huomattavasti turvallisuusstressin aiheuttamiin vaikutuksiin. Vaikkakin turvallisuusstressi johtaa yleensä lisääntyneeseen turvallisuuteen liittyvään roolistressiin, niin ylennystä tavoittelevat työntekijät kokivat roolistressiä

huomattavasti vähemmän kuin sellaiset työntekijät, jotka eivät tavoitelleet ylennystä. Artikkeli esittää, että ylennyksen tavoittelu ja siitä seuraava palkinto hillitsee turvallisuusstressin kuormitustekijöiden ja roolistressin suhdetta, vähentää koettua roolistressiä, eikä koettu turvallisuusstressi johda yhtä usein tietoturvakäytänteiden rikkomiseen. (Hwang & Cha, 2018.)

D'Arcy ja Teh (2019) tutkivat tietoturvakäytänteiden ja turvallisuusstressin vaikutuksia koettuun turhautuneisuuteen ja väsymykseen sekä niiden vaikutuksia tietoturvakäytänteiden rikkomisten neutralisaatioreaktioihin. Turvallisuusstressillä havaittiin olevan selkeä yhteys etenkin lisääntyneeseen turhautuneisuuteen, mutta myös väsymykseen. Nämä tunteet lisäsivät työntekijöissä myös neutralisaatioreaktioita tietoturvakäytänteiden rikkomista kohtaan, jotka johtivat myös heikentyneeseen noudattamiseen. Tutkimuksessa myös todettiin, että mitä korkeampi oli tietoturvakäytänteistä aiheutunut turhautuneisuuden tai väsymyksen tunne, sitä useammin neutralisaatioreaktio johti todelliseen tietoturvakäytänteiden rikkomiseen. Voi siis olla, että jos koetut tunteet eivät ylitä työntekijän yksilöllistä rajaa, niin neutralisaatioreaktiot eivät todennäköisesti johda tietoturvakäytänteiden rikkomiseen, vaan tällöin henkilökohtaiset eettiset arvot estäisivät neutralisaatioreaktioiden muuttumisen tietoturvakäytänteiden rikkomiseksi. (D'Arcy & Teh, 2019.)

Pham ym. (2019) tutkivat tietoturvakäytänteiden noudattamisesta johtuvaa loppuun palamista sekä millaisilla yksilötason ja organisaatiotason tekijöillä loppuun palamista voi lievittää. Tutkimus tunnisti ensiksi kolme eri syytä tietoturvakäytänteistä aiheutuvan stressin syntymiseen. Ylikuormituksella tarkoitetaan sitä, että työntekijät kokevat olevansa paineen alla noudattaakseen turvallisuusvaatimuksia, eikä heillä ole tarpeeksi aikaa noudattaa kaikkia vaatimuksia. Toisena syynä oli hankala pääsy tietoturvakäytänteisiin, jolla tarkoitetaan sitä, että työntekijät eivät ymmärrä dokumentoituja tietoturvavaatimuksista tai miten heidän tulisi niitä noudattaa. Viimeisenä syynä oli uusien taitojen opettelusta aiheutuva stressi, eli työntekijät kokivat stressaavana sen, että heidän tuli opetella uusia taitoja noudattaakseen tietoturvavaatimuksia, joka vei myös paljon aikaa. Tuloksista havaittiin, että ylikuormituksella oli suurin vaikutus loppuun palamiseen, mutta uusien taitojen opettelu ei odotuksien vastoin lisännytkään koettua loppuun palamista. Organisaatiotason loppuun palamista lieventävillä tekijöillä ei tutkimuksen mukaan ollut ollenkaan vaikutusta loppuun palamiseen, ja yksilötason lieventävillä tekijöillä oli vain hyvin lievä vaikutus. (Pham ym., 2019.)

Nasirpouri Shadbad ja Biros (2021) tutkivat turvallisuusstressin ja roolistressin vaikutuksia tietoturvakäytänteiden noudattamiseen. Tutkimuksessa todettiin ensin roolistressin syntyvän kolmesta tekijästä, jotka ovat roolikonfliktit, rooliepäselvyys ja roolikuormitus. Roolikonflikteilla tarkoitetaan työntekijän roolin ja tietoturvakäytänteiden yhteensopimattomuutta. Tietoturvakäytänteiden noudattaminen saattaisi siis esimerkiksi vaatia työntekijää tekemään jotain, mikä estää hänen roolinsa työtehtävien suorittamisen. Rooliepäselvyys puolestaan viittaa siihen, että tietoturvakäytänteiden noudattaminen aiheuttaa epäselvyyttä tietyssä roolissa työskentelevälle työntekijälle. Työntekijälle voi olla epäselvää, kuinka hänen tulisi noudattaa kyseistä tietoturvakäytännettä roolissaan.

Viimeisenä rooliylikuormitus tarkoittaa, että tietoturvakäytänteiden noudattaminen ja työtehtävien suorittaminen koetaan ylivoimaisena, sillä tietoturvakäytänteiden noudattaminen vie liikaa aikaa muilta työtehtäviltä. Tutkimuksen mukaan nämä kolme tekijää vaikuttavat selkeästi kielteisesti tietoturvakäytänteiden noudattamisaikomuksiin, ja roolikonflikteilla havaittiin olevan suurin vaikutus. Työntekijöiden kokiessa joko roolien ylikuormitusta, epäselvyyttä tai konflikteja, he päättävät usein olla noudattamatta tietoturvakäytänteitä. (Nasirpouri Shadbad & Biros, 2021.)

Nasirpouri Shadbad ja Biros (2022) tutkivat teknostressin vaikutuksia tietoturvakäyttäytymiseen. Tutkimus laajensi tietoturvakäyttäytymisen tutkimusta yhdistämällä turvallisuusstressin kuormittajat teknostressin kuormittajiin, jolloin tietoturvakäytänteiden rikkomiseen vaikuttaviin tekijöihin luetaan mukaan myös esimerkiksi tietojärjestelmistä ja teknologiasta aiheutuva kuormitus. Tutkimustuloksina havaittiin, että turvallisuusstressin aiheuttamaa väsymystä tai uupumusta kokevat työntekijät ovat alttiimpia rikkomaan tietoturvakäytänteitä. Aikaisemmista tutkimuksista poikkeavana havaintona oli, että koettu kuormitus ja uupumus ei suoraan säätele työntekijöiden alttiutta rikkoa tietoturvakäytänteitä, vaan teknostressi ja turvallisuusstressi itsessään vaikuttaa työntekijöiden aikomuksiin rikkoa tietoturvakäytänteitä. (Nasirpouri Shadbad & Biros, 2022.)

5 KIRJALLISUUSKATSAUKSEN YHTEENVETO

Tutkielman kirjallisuuskatsaus koostui kolmesta pääluvusta, joista ensimmäinen käsitteli tietoturvaa, tietoturvakäytänteitä ja metodeja niiden kehittämiseen. Luvussa määriteltiin ensiksi tietoturvan käsite Raggadin (2010) tietoturvatähden avulla, joka sisältää viisi eri tiedon ominaisuutta. Ne ovat tiedon luottamuksellisuus, eheys, käytettävyys, todentaminen ja kiistämättömyys. Nämä viisi ominaisuutta liittyvät tieto- ja teknologiresurssien suojaamiseen erilaisilta tietoturvauhilta, ja niiden tulee täyttyä tietoturvatavoitteiden saavuttamista varten. (Raggad., 2010.), Tietoturvakäytänteet puolestaan ovat erilaisia tieto- ja teknologiaresurssien turvaamiseen liittyviä sääntöjä (Bulgurcu ym., 2010), jotka voidaan luokitella korkean tason, matalan tason ja metatason tietoturvakäytänteisiin (Baskerville & Siponen, 2002). Tietoturvakäytänteet on määritelty käsitteenä eri tutkimuksessa hyvin eri tavoin – osa määritelmistä painottaa niiden olevan teknisiä tietoturvaa varmistavia ratkaisuja ja osa puolestaan käsittää niiden olevan lähinnä toimintaohjeita ja -prosesseja työntekijöille tietoturvauhkien ehkäisemiseksi. Korkean tason tietoturvakäytänteet ovat matalan tason käytänteitä abstraktimpia käytänteitä, joilla tietoturvaa pyritään varjelemaan. Matalan tason tietoturvakäytänteet ovat korkean tason käytänteitä spesifimpiä ja niihin lukeutuvat esimerkiksi salasanoihin liittyvät tietoturvakäytänteet. Viimeisenä tietoturvakäytänteiden tyyppinä ovat metakäytänteet, jotka keskittyvät tietoturvakäytänteiden tarkasteluun ja niiden kehittämiseen. (Baskerville & Siponen, 2002.)

Korkean, matalan ja metatason tietoturvakäytänteillä on erilaisia piirteitä ja tarkoituksia. Ne ensinnäkin ohjaavat organisaatiota määrittelemällä yrityksen tietoturvatavoitteet ja tietoturvastrategian sekä toimivat tietoturvan mittaamisen perustana. Tietoturvakäytänteet määrittelevät lisäksi organisaatiossa vastuut ja toimivallan tietoturvan osalta, sekä ne antavat myös yleiskuvaa organisaation kokonaisvaltaisista informaatio- ja teknologiaresursseista. Tietoturvakäytänteet auttavat myös organisaatiota valmistautumaan tietoturvauhkiin toimimalla kokonaisvaltaisena tietoturvasuunnitelmana sekä tietoturvariskien määrittelemisellä. Tietoturvakäytänteet toimivat lisäksi organisaation tietoturvan kommunikointivälineenä ja organisaation sisäisen tietoturvakulttuurin perustana. (Paananen, Lapke & Siponen, 2020.)

Tietoturvakäytänteiden kehittämiseen on olemassa erilaisia malleja, joista yksi varsin tunnettu on PFIRES-malli. Jatkuvuuteen perustuva malli sisältää neljä vaihekokonaisuutta, joissa tietoturvariskit uudelleenarvioidaan, uudet tietoturvakäytännöt suunnitellaan ja toteutetaan, ja lopuksi aloitetaan uusien tietoturvakäytänteiden valvonta. Malli lähtee tämän jälkeen uudestaan käyntiin ensimmäisestä vaiheesta. (Rees ym., 2003.)

Tutkielman toinen kirjallisuuskatsauksen luku keskittyi tietoturvakäyttäytymiseen organisaatiokontekstissa. Työntekijöiden tietoturvakäyttäytymistä, eli usein joko tietoturvakäytänteiden noudattamista tai niiden rikkomista, on tutkittu laajalti sosiaalitieteiden ja muun muassa kriminologian alalta olevien teorioiden pohjalta. Eniten hyödynnettyihin teorioihin lukeutuvat neutralisaatioteoria, peloteteoria sekä suunnitellun käyttäytymisen teoria. Tutkimukset ovat painottuneet yleensä yhden tai kahden teorian käyttämiseen, eikä tietoturvakäyttäytymistä ole ennen viime vuosia tutkittu usean eri teorian yhteisvaikutuksen kautta. Tähän toivat muutoksen ensimmäisinä Moody ym. (2018), jotka vertailivat tietoturvakäyttäytymisen tutkimuksessa käytettyjä teorioita ja tekivät vertailun pohjalta tietoturvakäyttäytymisen yhtenäismallin. Yhtenäismalli ammentaa aikaisemmassa tutkimuksessa käytetyistä teorioista tietoturvakäyttäytymiseen vaikuttavia tekijöitä, kuten neutralisointireaktiot ja rooliarvot, ja esittää sitten näiden vaikuttavien tekijöiden johtavan lopulta joko aikomukseen noudattaa tai rikkoa tietoturvakäytänteitä. Toisena vaihtoehtona malli voi johtaa reaktanssiin, eli tietoturvauhkan olemassaolon kieltämiseen. (Moody ym, 2018.)

Tietoturvakäyttäytymisen tutkimuskirjallisuudessa on Moodyn ym. (2018) jälkeen tehty esimerkiksi Raon ym. (2021) kokonaisvaltainen kirjallisuuskatsaus tietoturvakäyttäytymiseen liittyvistä tekijöistä, jossa tekijät lajiteltiin tarkasteltujen tutkimuksien näkökulman mukaan joko tietoturvakäytänteiden noudattamiseen tai niiden rikkomiseen vaikuttavaksi tekijäksi. Tietoturvakäytänteiden noudattamiseen havaittiin kirjallisuuskatsauksen pohjalta vaikuttavan esimerkiksi työntekijän motivaatio, organisaation tietoturvakulttuuri sekä organisaation johdon käyttäytyminen tietoturvaan liittyvissä asioissa. Tietoturvakäytänteiden rikkomiseen vaikuttaviin tekijöihin lukeutuivat esimerkiksi turvallisuusstressi sekä työntekijän ja organisaation väliset arvokonfliktit. (Rao ym., 2021.)

Tietoturvakäyttäytymisen tutkimukseen viime aikoina tullut toinen muutos on se, että tietoturvakäyttäytymistä on alettu tarkastelemaan dynaamisena ja muuttuvana ilmiönä, kun aiemmin aihetta on tutkittu tietyssä hetkessä tapahtuvana staattisena ilmiönä. Karjalainen ym. (2019) loivat tähän liittyen työntekijän tietoturvakäyttäytymisen dialektisen prosessimallin, joka kuvaa tietoturvakäyttäytymiseen liittyvien jännitteiden aiheuttamaa tietoturvakäyttäytymisen muutosta. Malli lähtee liikkeelle nykyisiin tietoturvakäytänteisiin liittyvien jännitteiden aiheuttamasta tasapainottavasta toiminnasta, jonka seurauksena tietoturvakäyttäytyminen muuttuu esimerkiksi tietoturvakäytänteitä noudattavaksi tai niitä vain osittain noudattavaksi. Malli oli tiettävästi ensimmäinen tietoturvakäyttäytymisen muuttumista kuvaava malli. (Karjalainen ym., 2019.) Karjalainen ym. (2020) loivat myös tietoturvakäyttäytymisen tasomallin, joka dialektisen prosessimallin tavoin kuvaa tietoturvakäyttäytymisen muuttumista, mutta malli

kuvaa neljä eri tietoturvakäyttäytymisen ajattelun tasoa ja tasolta tasolle siirtymiseen vaikuttavia tekijöitä. Ensimmäisen taso liittyy työntekijän aikaisempiin kokemuksiin tietoturvakäyttäytymiseen vaikuttavina tekijöinä ja neljäs taso kuvaa rutiininomaista tietoturvakäyttäytymistä, joka ei vaadi työntekijältä suuria kognitiivisia ponnisteluja. (Karjalainen ym., 2020).

Kirjallisuuskatsauksen kolmas ja viimeinen pääluku käsitteli tietoturvakäytänteistä aiheutuvaa stressiä, eli turvallisuusstressiä. Turvallisuusstressin perustana on muutama vuosikymmen sitten ensimmäisen kerran määritelty teknostressi, joka on teknologiasta ja sen käytöstä aiheutuvaa stressiä. (Brod, 1982; Tarafdar ym., 2007). Turvallisuusstressin käsite määriteltiin ensimmäistä kertaa D'Arcyn ym. (2014) toimesta, ja sen aiheutumista valittiin kuvaamaan teknostressin kolme stressitekijää, jotka ovat ylikuormitus, monimutkaisuus ja epävarmuus. Turvallisuusstressistä on sittemmin ilmestynyt vajaa kymmenkunta tutkimusta, joissa jokaisessa tutkimuksen painopiste on ollut erilainen. Esimerkiksi Hwang ja Cha (2018) tutkivat turvallisuusstressin ja roolistressin vaikutuksia tietoturvakäytänteiden noudattamisessa, kun taas D'arcy ja Teh (2019) tutkivat turvallisuusstressin yhteyksiä turhautumiseen ja ärsyyntymiseen. Kuten tietoturvakäyttäytymisen tutkimuksessa, myös turvallisuusstressin aikaisemmassa tutkimuksessa on hyödynnetty muutamaa valittua teoriaa tutkimuksen teoreettisena viitekehyksenä. Suosituimpiin teorioihin lukeutuvat rooliteoria, selviämisteoria ja tunnepitoisten tapahtumien teoria. Turvallisuusstressin on todettu heikentävän työntekijöiden työtyytyväisyyttä (Ho-Jin & Cho, 2016) ja aiheuttavan turhautuneisuutta, ärsyyntymistä (D'Arcy & Teh, 2019) ja väsymystä (Nasispouri Shadbad & Biros, 2022). Lisäksi ylikuormituksen, eli tietoturvakäytänteiden noudattamisesta aiheutuvan lisätyömäärän, on havaittu olevan yksi suurin syy turvallisuusstressin aiheutumiselle (Lee ym., 2016; Pham ym., 2019).

6 TUTKIMUSMENETELMÄT

Tässä luvussa kuvataan tutkielman empiirisen osan toteutus. Luku on jaettu kuuteen alalukuun, joista ensimmäisessä selitetään tutkielman tutkimusmenetelmän valinta. Toinen alaluku sisältää aineistonkeruumenetelmän, jossa selitetään valitun aineistonkeruumenetelmän valintaan liittyneet seikat. Kolmannessa alaluvussa kerrotaan, mistä tutkimukseen löydettiin haastateltavia ja millaisilla kriteereillä heidät valittiin. Neljäs luku kattaa tutkimuksen toteutuksen, jossa kuvataan tutkielman käytännön toteutus. Viidennessä alaluvussa käsitellään tutkielmaan valittu aineiston analyysimenetelmä. Viimeisessä alaluvussa käydään läpi tutkimuksen reliaabeliuteen ja validiuteen vaikuttavia asioita.

6.1 Tutkimusmenetelmä

Tutkimuksen tavoitteena on selvittää, millaiset tietoturvakäytänteet eri organisaatioiden työntekijät kokevat stressaavimmiksi ja miksi juuri kyseiset tietoturvakäytänteet ovat stressaavia. Puusan, Juutin ja Aaltion (2020) mukaan laadulliset tutkimukset keskittyvät tarkastelemaan tutkimuskohteiden mielipiteitä ja subjektiivisia kokemuksia tutkittavasta kohteesta. Lisäksi Hirsjärven ja Hurmeen (2008) mukaan laadullinen tutkimus pyrkii ihmisten näkökulmien ymmärtämiseen ja tulkintaan, kun taas määrällinen tutkimus pyrkii yleensä ennustamaan ja yleistämään jotain ilmiötä. Tutkielmassa halutaan nimenomaan ymmärtää haastateltavien näkökulmia ja tulkita heidän kokemuksiaan. Tämän vuoksi tutkimuksen tutkimusmenetelmäksi valittiin laadullinen menetelmä, sillä tutkimuksessa haluttiin selvittää tutkittavien kokemuksia ja henkilökohtaisia ajatuksia tietoturvakäytänteiden stressaavuudesta.

6.2 Aineistonkeruumenetelmä

Tutkielman aineistonkeruumenetelmäksi valittiin puolistrukturoidut teemahaastattelut. Tutkielmaa ei päätetty toteuttaa strukturoidulla, lomakehaastattelumaisella aineistonkeruumetodilla sen takia, että haastateltavien kertomia esille tulleita asioita ei pystyttäisi tarkentamaan halutulla tavalla ja haastattelurungon kysymykset tulisi tällöin miettiä erittäin tarkkaan.

Hirsjärven ja Hurmeen (2008) mukaan haastatteluiden käyttämisessä aineistonkeruumenetelmänä on lukuisia etuja ja haittoja. Etuihin lukeutuu esimerkiksi haastateltavan näkeminen subjektina haastattelutilanteessa, jolloin hän voi kertoa asioista vapaasti. Haastatteluita käytettäessä myös tiedetään jo ennalta, että haastateltavat tulevat antamaan erilaisia vastauksia, joka lisää vastausten monipuolisuutta ja auttaa ymmärtämään tutkittavaa ilmiötä paremmin. Haastatteluissa voidaan lisäksi syventää haastateltavan antamia vastauksia esimerkiksi kysymällä häneltä perusteluita esittämälleen asialle. Näin asian käsittely ei jää pintapuoliseksi. (Hirsjärvi & Hurme, 2008.) Puusan ym. (2020) mukaan haastatteluiden käyttäminen aineistonkeruumenetelmänä laadullisessa tutkimuksessa on mielekästä siksi, että haastateltaviksi voidaan valita harkinnanvaraisesti sellaisia haastateltavia, joilla on henkilökohtaista kokemusta tutkittavasta aiheesta. He myös toteavat, että haastattelut ovat joustava aineistonkeruumenetelmä, sillä haastateltavia on mahdollista pyytää selittämään kertomaansa tarkemmin (Puusa ym., 2020). Teemahaastatteluiden tuoma vapaus haastattelutilanteessa koetaan hyödyksi myös tässä tutkielmassa, sillä tutkimuskysymyksien selvittäminen helpottuu huomattavasti, jos haastateltavat voivat kertoa kokemuksistaan avoimesti ja kattavasti. Myös haastateltavien vastauksien eroaminen toisistaan on tutkielman kannalta hyödyllistä, sillä näin saadaan kattavampi kuva stressaavista tietoturvakäytänteistä ja niiden syistä. Tietoturvakäytänteiden stressaavuus on jo toki lähtökohtaisesti henkilökohtainen asia, ja onkin odotettavissa, että haastateltavat tulevat antamaan ainakin jollain tasolla erilaisia vastauksia, sillä jokaisella haastateltavalla on varmasti erilaisia kokemuksia tietoturvakäytänteistä, niiden noudattamisesta ja niiden stressaavuudesta. Tutkielman haastatteluissa on erittäin tärkeää perusteluiden kysyminen haastateltavien vastauksiin, jotta esille tulleiden tietoturvakäytänteiden stressaavuuden syyt voidaan saada selville. Näiden seikkojen vuoksi haastattelut sopivat tutkielman aineistonkeruumenetelmäksi erinomaisesti.

Vaikka haastattelut vaikuttavat otolliselta aineistonkeruumenetelmältä, voi niillä kuitenkin olla jotain haittoja. Haastatteluiden haitoiksi Hirsjärvi ja Hurme (2008) esittävät ensiksikin, että haastatteluiden toteutus vie aikaa, sillä haastatteluaikojen sopiminen, haastateltavien etsiminen ja lopulta haastatteluiden litteroiminen ja analysointi on hyvin aikaa vievä prosessi. Haastattelut voivat myös sisältää virheitä, sillä haastateltavat saattavat antaa vastauksia, joita he ajattelevat haastattelijan haluavan kuulla. (Hirsjärvi & Hurme, 2008; Puusa ym., 2020). Lisäksi haastatteluaineiston analysointi voi olla työlästä, koska haastatteluiden analysointiin ei yleensä ole tarjolla valmiita malleja. (Hirsjärvi & Hurme, 2008).

Edellä mainitut haitat on otettu huomioon tutkielman aineistonkeruumenetelmää valittaessa ja haastatteluita suunniteltaessa. Tutkielman tekemiseen on ensiksikin varattu tarpeeksi aikaa, sekä haastatteluiden toteutus pyrittiin aloittamaan ajoissa. Haastatteluvirheiden vähentämiseksi haastatteluissa on pyritty luomaan mahdollisimman avoin ilmapiiri ja haastateltavien antamia vastauksia on pyydetty tarkentamaan pintapuolisten vastauksien ehkäisemiseksi. Puolistrukturoidut teemahaastattelut mahdollistavat vapaamman keskustelun, sillä haastattelun kulkua voidaan ohjata haastateltavan vastauksien mukaan (Puusa ym., 2020).

6.3 Haastateltavien valinta

Aikaisemmassa tietoturvakäyttäytymisen ja turvallisuusstressin tutkimuksessa IT-alan työntekijät ovat olleet varsin aliedustettuina. Tämän vuoksi tutkimuksen kohteeksi valittiin tässä tutkielmassa nimenomaan suomalaiset IT-alan työntekijät ja toimihenkilöt. Haastateltavat valittiin tutkielman tekijän omasta lähipiiristä sekä kontakteista. Potentiaalisilta haastateltavilta tiedusteltiin etukäteen ennen haastatteluita heidän kokemuksistaan tietoturvakäytänteistä ja niiden stressaavuudesta. Heille myös kerrottiin jo tässä vaiheessa, että turvallisuusstressi voi ilmetä esimerkiksi turhautuneisuutena tai väsymyksenä tietoturvakäytänteitä ja niiden noudattamista kohtaan. Tällä pyrittiin varmistamaan, että jokaisella haastateltavalla olisi kokemusta turvallisuusstressistä, ja että haastatteluista olisi mahdollista saada vastauksia tutkielman molempiin tutkimuskysymyksiin.

6.4 Tutkimuksen toteutus

Haastattelut toteutettiin vuoden 2022 kesän ja alkusyksyn aikana heinä-syyskuussa. Haastattelut aikataulutettiin haastateltavalle sopivalle ajankohdalle ja haastatteluun oli mahdollista osallistua kasvokkain tai internetin välityksellä Zoom-videoneuvottelupalvelussa. Suurin osa haastatteluista toteutettiin kasvokkain. Haastateltavat valittiin tutkimuksen tekijän omasta tuttavapiiristä ja kontakteista. Haastatteluissa ei tähdätty tiettyyn kestoon, vaan yksittäisiä haastatteluita jatkettiin aina niin kauan, kuin haastateltavilla oli sanottavaa asiasta. Keskustelua pyrittiin pitämään yllä ja jatkamaan lisäkysymyksien avulla ja tarkennuspyyntöjen avulla. Haastatteluihin valmistauduttiin tekemällä pari testihaastattelua, joiden pohjalta todettiin, että teemahaastattelurunko tuottaa toivotunlaisia vastauksia. Haastateltaville tuotiin esille haastatteluissa, että haastattelu on anonyymi eikä vastauksien perusteella ole mahdollista tunnistaa yksittäistä haastateltavaa. Haastateltaville kerrottiin haastatteluiden alussa myös haastattelun nauhoittamisesta, jotta saatu aineisto voidaan litteroida ja analysoida myöhemmässä vaiheessa. Haastatteluiden äänimateriaali nauhoitettiin haastattelutavan mukaan, joko tutkimuksen tekijän puhelimen sanelinohjelmistoon

kasvokkain tapahtuvan haastattelun tapauksessa tai Zoom-palvelun nauhoitusominaisuuden avulla tietokoneelle videoneuvotteluhaastattelun tapauksessa.

Tutkimuksessa toteutettiin yhteensä 15 haastattelua ja niiden kestot löytyvät alla olevasta taulukosta (taulukko 10). Lyhin haastattelu oli kestoltaan 6 minuuttia 55 sekuntia ja pisin haastattelu puolestaan 23 minuuttia 14 sekuntia. Haastatteluiden kestojen keskiarvo oli 12 minuuttia 26 sekuntia. Haastatteluiden kestoon vaikuttavat haastateltavien kokemukset tietoturvakäytänteistä ja niiden noudattamisesta aiheutuva stressin määrä ja laatu. Osalla haastateltavista oli paljonkin kokemuksia ja sanottavaa useista stressaavista hetkistä, kun taas osalla oli kokemusta vain yhdestä tai kahdesta stressiä aiheuttaneesta tietoturvakäytänteestä. Tämän vuoksi lyhyistäkin haastatteluista saatiin hyödyllisiä vastauksia, eikä joidenkin haastatteluiden lyhyttä kestoa nähty tutkimuksen laatua heikentävänä tekijänä. Jokaisesta haastattelusta tunnistettiin vastauksia molempiin tutkielman tutkimuskysymykseen.

TAULUKKO 10 Haastatteluiden kestot ja keskiarvo

Haastattelu	**Haastattelun kesto**
H1	6:55
H2	8:58
H3	12:15
H4	7:04
H5	8:06
H6	13:15
H7	16:12
H8	9:00
H9	12:00
H10	10:19
H11	19:08
H12	15:07
H13	23:14
H14	13:33
H15	14:06
Keskiarvo	12:36

Haastatteluiden perustana oleva teemahaastattelurunko (liite 1) laadittiin keväällä ennen haastatteluiden aloittamista. Hirsjärven ja Hurmeen (2008) mukaan puolistrukturoiduissa teemahaastatteluissa on merkityksellistä se, että kysymykset on valmisteltu ennakkoon. Vaikka haastattelurungon kysymykset ovat samat jokaisen haastateltavan kohdalla, ne voidaan kysyä eri järjestyksessä ja jatkokysymyksissä voi olla eroja haastateltavien välillä. (Hirsjärvi & Hurme, 2008). Haastattelut alkoivat kertomalla haastateltaville tutkimuksen tarkoituksesta ja tutkimuskysymyksistä sekä selitettiin, millaisia tuloksia tutkimus pyrkii tuottamaan. Taustatietoina haastateltavilta kysyttiin ikä, sukupuoli, koulutustaso ja työkokemus vuosissa nykyisissä tehtävissä. Haastateltaville kerrottiin seuraavaksi lyhyesti tietoturvakäytänteistä ja kysyttiin niihin liittyviä taustakysymyksiä. Haastateltavilta kysyttiin, ovatko he tutustuneet organisaationsa tietoturvakäytänteisiin,

ovatko he osallistuneet tietoturvakoulutukseen organisaatiossaan ja pyydettiin lopuksi arvioimaan osaamistaan ja ymmärrystään organisaationsa tietoturvakäytänteistä. Haastattelut etenivät seuraavaksi itse pääaiheeseen, eli tietoturvakäytänteiden stressaavuuteen. Haastateltaville kerrottiin lyhyesti turvallisuusstressistä ilmiönä ja sen syntytavoista. Haastatteluissa kysyttiin seuraavaksi, onko haastateltava kokenut stressiä tietoturvakäytänteistä ja niiden noudattamisesta. Haastattelurungossa olevista kysymyksistä valittiin sopivat kysymykset kysyttäväksi, eli jokaisessa haastattelussa ei kysytty jokaista teemahaastattelurungon kysymystä. Esille tulleista tietoturvakäytänteiden noudattamisen stressaavista tilanteista kysyttiin haastateltavilta tarkentavia kysymyksiä, kuten miksi kyseinen tietoturvakäytänne on haastateltavan mielestä stressaava ja millainen stressaava tilanne oli. Näin jokainen haastateltava esitti kokemuksensa perusteella stressaavan tietoturvakäytänteen ja syyn sen stressaavuudelle. Teemahaastattelurunkoon poimittiin myös muutamia apukysymyksiä D'Arcyn ym. (2014) tutkimuksesta, joita haastateltavilta kysyttiin tarvittaessa. Haastattelun lopuksi haastateltaville annettiin vielä mahdollisuus vapaaseen sanaan, eli kertoa mitä tahansa mieleen tulevaa aiheeseen liittyen.

6.5 Aineiston analyysimenetelmä

Haastatteluaineiston analysointiosuus käynnistyi haastatteluiden toteutuksen jälkeen haastatteluiden litteroinnilla. Hirsjärven ja Hurmeen (2008) mukaan litteroinnin tarkkuudelle ei ole tarkkaa ohjetta, vaan litteroinnin tarkkuus tulee määrittää tutkimuksen ja tutkimustavan perusteella. Tässä tutkielmassa halutaan saada selville haastateltavien kokemuksia ja mielipiteitä, joten erittäin tarkkaa litterointia ei nähty tarpeelliseksi. Litteroinnissa pyrittiin kirjoittamaan haastattelut sanasta sanaan, mutta ilman ylimääräisiä tai toistuvia täytesanoja tai huokauksia. Näin litterointityö nopeutui, mutta haastateltavien kertomat asiat kirjoitettiin niin, kuin he asiat tarkoittivatkin sanoa. Hirsjärvi ja Hurme (2008) suosittelevat tekemään aineistoon merkintöjä ja muistiinpanoja jo litterointivaiheessa, jotta itse varsinainen analysointivaihe olisi sujuvampi. Myös Puusan ym. (2020) mukaan laadullisissa tutkimuksissa aineistoa analysoidaan yleensä koko tutkimuksen ajan, myös litterointiaiheessa. Litterointivaihe suoritettiinkin suosituksen mukaisesti, ja aineistoon tehtiin muistiinpanoja merkittävistä ja oleellisista esille tulleista asioista ja litterointivaiheessa helpottamaan aineiston analysointia.

Laadullisissa tutkimuksissa on tärkeää selvittää, kuinka monta haastattelua tutkimukseen tulisi saada. Haastatteluiden sopivaan määrään liittyy olennaisesti saturaation käsite, jolla tarkoitetaan sitä, että haastatteluista ei tule enää esille uusia merkittäviä asioita (Hirsjärvi & Hurme, 2008). Haastatteluissa havaittiin saturoitumista jo ennen viidettätoista haastattelua, sillä haastatteluissa tuli pääosin esille hyvin samankaltaisia asioita. Haastatteluita päätettiin toteuttaa yhteensä viisitoista kappaletta, jotta haastatteluaineisto olisi tarpeeksi kattava ja antaisi mahdollisimman hyvän kuvan IT-alan työntekijöitä stressaavista tietoturvakäytänteistä.

Hirsjärven ja Hurmeen (2008) mukaan itse aineiston analyysiosuus on monivaiheinen prosessi ja sisältää aineiston kuvailun, luokittelun ja synteesin luomisen. Aineiston kuvailemisella tarkoitetaan kohteen piirteiden ja tapahtumien selvittämisen. On olennaista sijoittaa kuvaukset oikeaan kontekstiin, jotta kuvauksien merkitys voidaan ymmärtää oikein. Toisessa vaiheessa, eli aineiston luokittelussa, tarkoituksena on luokitella aineisto. Luokittelut tulee perustua empiiriseen aineistoon, jotta aineistoa voidaan vertailla toisiinsa. Luokittelun voi tehdä esimerkiksi perustamalla luokat tutkimusongelmaan, tutkimusalaan tai aikaisempiin teorioihin. Synteesivaiheessa tarkoituksena on löytää eroavaisuuksia ja samankaltaisuuksia luotujen luokitteluiden välillä. Synteesiä käytetään lopulta tulkintojen tekemiseen. Tulkintaa tehdäänkin laadullisissa tutkimuksissa yleensä koko tutkimuksen ajan. (Hirsjärvi & Hurme, 2008.) Tutkielman haastatteluaineisto sijoittuu organisaatiokontekstiin, jolloin vastaukset voivat olla erilaisia kuin esimerkiksi henkilökohtaista tietoturvakäyttäytymistä tarkastellessa. Tämä otettiin huomioon aineiston analyysivaiheessa. Haastatteluissa esitettyjä asioita myös liitettiin aikaisempaan tutkimuskirjallisuuteen, etenkin tietoturvakäytänteiden stressaavuuden syiden osalta. Niitä verrattiin turvallisuusstressin kolmen stressitekijän määritelmiin ja kuvauksiin. Haastatteluaineiston varsinainen analyysi tehtiin teemoittelun avulla. Hirsjärvi ja Hurme (2008) kuvaavat teemoittelua analysointitavaksi, jossa tunnistetaan haastatteluista esille tulevia samanlaisia piirteitä, eli teemoja, jotka pohjautuvat tutkijan tulkintaan haastatteluaineistosta. Esille nousseita teemoja vertaillaan toisiinsa esimerkiksi tyypittelyn avulla, jossa haastatteluissa havaittuja yhteisiä piirteitä ryhmitellään tiettyjen kriteerien perusteella. (Hirsjärvi & Hurme, 2008.) Haastatteluaineiston litteroinnin jälkeen haastatteluaineistosta tunnistettiin jokaista haastateltavaa stressanneet tietoturvakäytänteet ja ne merkittiin ylös. Kun kaikki haastattelut oli käyty läpi, samanlaiset tietoturvakäytänteet kerättiin yhteen ja ne luokiteltiin yhden yläkäsitteen alle. Tietoturvakäytänneluokkia muodostui yhteensä neljä kappaletta. Seuraavaksi tarkasteltiin tietoturvakäytänteiden stressaavuuden syitä, jotka yhdistettiin kerrottuihin tietoturvakäytänteisiin ja turvallisuusstressin stressitekijöihin D'Arcyn ym. (2014) tutkimuksen perusteella.

6.6 Tutkimuksen reliaabelius ja validius

Puusan ym. (2020) mukaan tutkimuksen reliaabelius ja validius ovat keskeisiä termejä yleensä määrällisissä tutkimuksissa, mutta ne soveltuvat myös laadullisien tutkimuksien luotettavuuden arviointiin. Hirsjärven ja Hurmeen (2008) mukaan tutkimuksen reliaabelius voidaan ajatella esimerkiksi niin, että sama henkilö antaa kahdella eri tutkimuskerralla saman tuloksen, tai että kaksi eri henkilöä päätyvät samanlaiseen tulokseen. He kuitenkin painottavat, että varsinkin muuttuvien ominaisuuksien kohdalla, kuten ihmisten ominaisuuksien, eri tuloksien saaminen ei välttämättä ole tutkimusmenetelmän vika, vaan muuttuneen tilanteen seuraus. Vastaavasti Puusa ym. (2020) painottavat laadullisen tutkimuksen reliaabeliuden osalta, että ihmisen käyttäytymisen kontekstisidonnaisuuden

vuoksi kaksi eri tutkijaa eivät välttämättä pysty pääsemään samaan lopputulokseen. Tutkimuksen validiuden he puolestaan määrittelevät tutkittavan ilmiön eheydeksi, jolloin tutkimuksen tuloksia pitää tarkastella nimenomaan tutkittavan ilmiön luonteen näkökulmasta (Puusa ym., 2020). Hirsjärvi ja Hurme (2008) puolestaan kertovat tutkimuksen validiuden olevan sitä, että valittu tutkimusmenetelmä mittaa sitä, mitä sen on tarkoitus mitata. Puusan ym. (2020) mukaan laadullisen tutkimuksen luotettavuus tulisi arvioida laajemmin, kuin ainoastaan validiuden ja reliaabeliuden avulla. Laadullisen tutkimuksen luotettavuutta voidaan arvioida esimerkiksi siirrettävyyden avulla, jolloin pohditaan, että voidaanko sama tutkimus toistaa jossain toisessa tutkimusympäristössä. Laadullisen tutkimuksen luotettavuuteen vaikuttaa erityisesti myös tutkimuksen raportoinnin läpinäkyvyys ja kattavuus: mitä kattavammin laadullisen tutkielman aineistonkeruu ja analysointi on raportoitu, sitä luotettavampana tutkimusta voidaan pitää. (Puusa ym., 2020.) Myös Hirsjärvi ja Hurme (2008) esittelivät tutkimuksen laadun ja luotettavuuden parantamisen keinoiksi esimerkiksi hyvän haastattelurungon laatimisen, haastattelijan koulutuksen ja aineiston pikaisen litteroinnin haastatteluiden jälkeen.

Tässä tutkielmassa tutkimuksen validiutta ja reliaabeliutta on pyritty parantamaan useilla eri tavoilla. Ensinnäkin tutkimuksen toteutukseen liittyvät asiat on pyritty tuomaan ilmi niin läpinäkyvästi ja kattavasti kuin mahdollista. Lukijalle pitäisi siis olla selvää, miten tutkimuksen aineisto kerättiin ja miten se analysointiin. Haastatteluissa käytetty haastattelurunko suunniteltiin huolella etukäteen ja siihen sisällytettiin myös turvallisuusstressin tutkimuskirjallisuudessa käytettyjä apukysymyksiä, joita kysyttiin tarvittaessa. Haastatteluiden avoimuus pyrittiin varmistamaan kertomalla haastateltaville vastauksien luottamuksellisuudesta ja siitä, että he voivat tuoda ilmi mitä tahansa heille tulee aiheesta mieleen. Haastatteluissa myös painotettiin, ettei haastateltavien pidä antaa tietynlaisia vastauksia vain haastattelijan miellyttämisen takia. Haastatteluissa pyrittiin myös keskustelemaan aiheesta niin pitkään, kuin haastateltavilla vain oli sanottavaa aiheesta, eikä haastatteluja kiirehditty. Jokaiseen esille tulleeseen asiaan tartuttiin tarkemmin ja haastateltavilta kysyttiin jatkokysymyksiä heidän vastauksiinsa perustuen. Haastattelut loppuivat, kun haastateltavilla ei ollut enää sanottavaa aiheesta eivätkä lisäkysymykset tuottaneet keskustelua. Hirsjärven ja Hurmeen (2008) suosituksen mukaisesti haastatteluaineisto litterointiin nopeasti ja huolellisesti haastatteluiden jälkeen, jotta jokainen haastattelu olisi vielä haastattelijan muistissa. Haastateltavia pyrittiin myös saamaan eri organisaatioista ja taustoista, jotta tutkimuksen kohderyhmä ei kohdistuisi ainoastaan yhteen organisaatioon tai tietynlaisiin haastateltaviin. Tällä pyrittiin parantavat tutkimuksen luotettavuutta. Yksi tutkimuksen luotettavuutta heikentävä tekijä voi olla, että tutkimukseen osallistuneet henkilöt olivat tutkijan omasta lähipiiristä. Tämä on voinut aiheuttaa toimenpiteistä huolimatta sen, että haastateltavat vastasivat sillä tavalla, miten he ajattelivat tutkijan haluavan kuulla.

7 TULOKSET

Tämä luku kattaa tutkimuksen keskeisten tuloksien läpikäynnin. Luku on jaettu neljään alalukuun, joista ensimmäisessä alaluvussa käydään läpi tutkimukseen osallistuneiden haastateltavien taustatiedot. Toisessa alaluvussa käydään läpi ensimmäiseen tutkimuskysymykseen liittyviä tuloksia, eli millaiset tietoturvakäytänteet haastateltavat kokivat stressaavaksi. Kolmas alaluvussa sisältää toisen tutkimuskysymyksen kannalta relevantit löydökset, eli miksi esille tulleet tietoturvakäytänteet koetaan stressaaviksi. Viimeinen alaluku kattaa koetun turvallisuusstressin muuttumiseen liittyviä havaintoja, joiden selittämisessä hyödynnetään kirjallisuuskatsauksen toisessa teorialuvussa esiteltyä Karjalaisen ym. (2020) tietoturvakäyttäytymisen tasomallia.

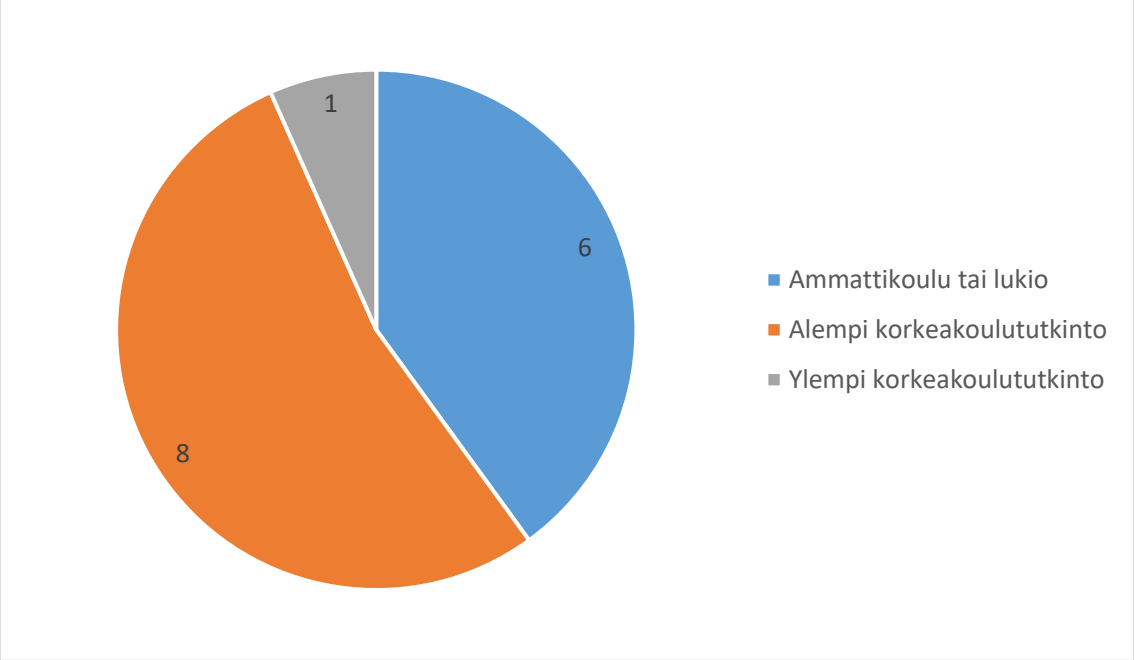
7.1 Haastateltavien taustatiedot

Haastateltavilta kysyttiin perustaustatietoja ja tietoturvakäytänteisiin liittyviä taustatietoja ennen varsinaisia tutkimusaihekysymyksiä (taulukko 11). Perustaustatietoina kysyttiin ikä, sukupuoli, koulutusaste ja työvuosien määrä nykyisissä tehtävissä. Iät sijoitettiin yleisesti tutkimuskäytössä hyödynnetylle viisiportaiselle ikäasteikolle, jonka asteet olivat 18–24 vuotta, 25–34 vuotta, 35–44 vuotta, 45–54 vuotta ja yli 65 vuotta. Koulutustaso määräytyi viimeisimmän suoritetun tutkinnon mukaan ja sen vaihtoehtoina olivat peruskoulu, ammattikoulu tai lukio, alempi korkeakoulututkinto ja ylempi korkeakoulututkinto. Myös työvuodet luokiteltiin viisiportaiselle asteikolle, jossa vaihtoehdot olivat alle yksi vuosi, 1–2 vuotta, 3–4 vuotta, 4–5 vuotta ja yli 5 vuotta. Haastateltavat olivat iältään 18–34-vuotiaita, painottuen enemmän 25–34 vuotiaisiin. Haastateltavista 18–24-vuotiaita oli 6/15 ja 2–34-vuotiaita oli 11/15. Haastateltavista miehiä oli 13 ja naisia 2. Kaikki haastateltavat olivat suorittaneet vähintään toisen asteen tutkinnon (kuvio 6). Toisen asteen tutkinnon suorittaneita oli 6 kappaletta ja alemman korkeakoulututkinnon suorittaneita 8 kappaletta. Vain yksi haastateltava oli suorittanut ylemmän korkeakoulututkinnon. Työvuosissa nykyisissä tehtävissä nähtiin

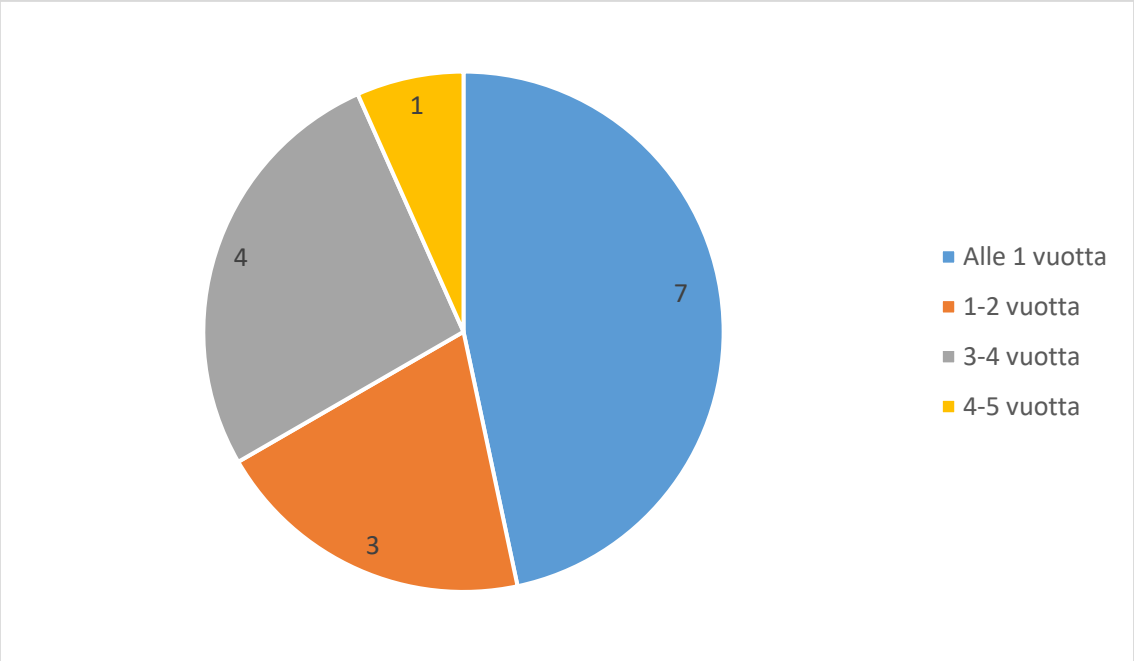
hieman suurempaa jakaumaa (kuvio 7). Alle 1 vuoden nykyisissä tehtävissä toimineita haastateltavia oli 7 kappaletta, 1–2 vuotta toimineita 3 kappaletta, 3–4 toimineita 4 kappaletta ja 4–5 vuotta toimineita 1 kappale.

TAULUKKO 11 Haastateltavien taustatiedot

	Ikähaarukka	Sukupuoli	Koulutustaso	Työkokemus
H1	25–34 vuotta	Mies	Alempi korkeakoulututkinto	Alle 1 vuosi
H2	18–24 vuotta	Mies	Alempi korkeakoulututkinto	Alle 1 vuosi
H3	18–24 vuotta	Mies	2. asteen tutkinto	3–4 vuotta
H4	18–24 vuotta	Mies	Alempi korkeakoulututkinto	Alle 1 vuosi
H5	18–24 vuotta	Mies	2. asteen tutkinto	Alle 1 vuosi
H6	18–24 vuotta	Mies	Alempi korkeakoulututkinto	Alle 1 vuosi
H7	25–34 vuotta	Mies	2. asteen tutkinto	3–4 vuotta
H8	25–34 vuotta	Mies	Alempi korkeakoulututkinto	4–5 vuotta
H9	18–24 vuotta	Nainen	Ylempi korkeakoulututkinto	Alle 1 vuosi
H10	25–34 vuotta	Mies	Alempi korkeakoulututkinto	1–2 vuosi
H11	25–34 vuotta	Mies	Alempi korkeakoulututkinto	2–3 vuotta
H12	25–34 vuotta	Mies	2. asteen tutkinto	1–2 vuosi
H13	25–34 vuotta	Mies	2. asteen tutkinto	3–4 vuotta
H14	25–34 vuotta	Mies	Alempi korkeakoulututkinto	4–5 vuotta
H15	25–34 vuotta	Nainen	2. asteen tutkinto	Alle 1 vuosi



KUVIO 6 Haastateltavien koulutustaso

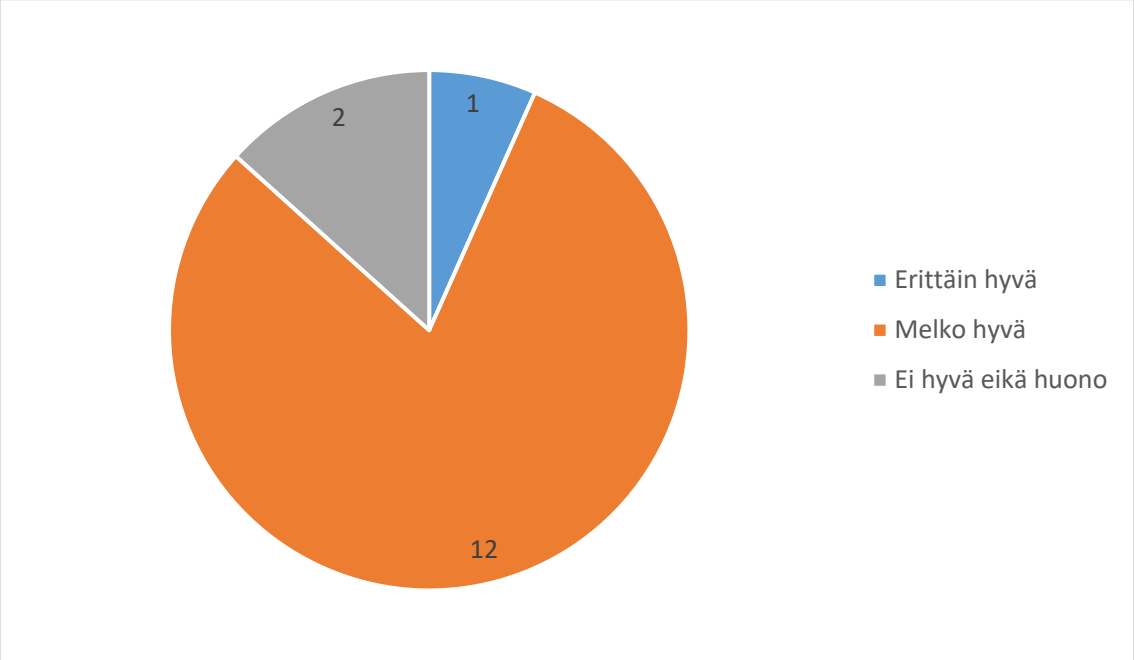


KUVIO 7 Haastateltavien työvuodet nykyisissä tehtävissä

Tietoturvakäytänteisiin liittyviä taustakysymyksiä oli kolme kappaletta (taulukko 12). Taulukossa ISP:llä tarkoitetaan tietoturvakäytänteitä (engl. *information security policy).* Ensimmäisenä taustatietokysymyksenä haluttiin selvittää, ovatko haastateltavat ylipäätään tutustuneet organisaatioidensa tietoturvakäytänteisiin. Toisena kysymyksenä kysyttiin, ovatko haastateltavat osallistuneet organisaatioissaan tietoturvakoulutukseen. Ensimmäiseen ja toiseen taustakysymykseen vastausvaihtoehtoina oli kyllä tai ei. Viimeisenä tietoturvakäytänteisiin liittyvänä taustakysymyksenä oli itsearvio haastateltavien oman organisaation tietoturvakäytänteiden ymmärtämisen tasosta, jossa käytettiin Likert-asteikkoa, eli viisiportaista vastausasteikkoa. Asteikon vaihtoehtoina olivat erittäin hyvin (5), melko hyvin (4), ei hyvin eikä huonosti (3), melko huonosti (2) ja erittäin huonosti (1). Haastateltavista jokainen kertoi tutustuneensa organisaationsa tietoturvakäytänteisiin. Lisäksi neljätoista haastateltavaa viidestätoista kertoi osallistuneensa organisaationsa järjestämään tietoturvakoulutukseen. Vastaukset kahteen ensimmäiseen taustakysymykseen olivat odotettuja, sillä varsinkin IT-alan organisaatioissa tietoturvalla ja tietoturvakäytänteillä on yleensä vahva ja merkittävä rooli, ja työntekijöille järjestetään tietoturvakoulutuksia vähintäänkin työsuhteen alussa. Tietoturvakäytänteiden ymmärryksen itsearviossa puolestaan havaittiin pientä jakaumaa (kuvio 8). Suurin osa haastateltavista kertoi ymmärtävänsä organisaationsa tietoturvakäytänteet melko hyvin (4), mutta kaksi haastateltavaa arvioi osaaminensa olevan keskitasolla (3) ja vain yksi haastateltava koki omaavansa erinomaisen (5) ymmärryksen organisaationsa tietoturvakäytänteistä.

TAULUKKO 12 Haasteltavien taustatiedot liittyen tietoturvakäytänteisiin

	Onko tutustunut ISP?	Osallistunut ISP-koulutukseen?	Itsearvio ISP ymmärryksestä?
H1	Kyllä	Kyllä	Melko hyvä
H2	Kyllä	Ei	Melko hyvä
H3	Kyllä	Kyllä	Melko hyvä
H4	Kyllä	Kyllä	Melko hyvä
H5	Kyllä	Kyllä	Melko hyvä
H6	Kyllä	Kyllä	Melko hyvä
H7	Kyllä	Kyllä	Melko hyvä
H8	Kyllä	Kyllä	Melko hyvä
H9	Kyllä	Kyllä	Melko hyvä
H10	Kyllä	Kyllä	Erittäin hyvä
H11	Kyllä	Kyllä	Melko hyvä
H12	Kyllä	Kyllä	Melko hyvä
H13	Kyllä	Kyllä	Melko hyvä
H14	Kyllä	Kyllä	Ei hyvä eikä huono
H15	Kyllä	Kyllä	Ei hyvä eikä huono



KUVIO 8 Haastateltavien tietoturvakäytänteiden ymmärryksen itsearvio

Haastatteluiden alussa haastateltavilta kysyttiin heidän yleisiä mielipiteitään ja asenteitaan tietoturvakäytänteisiin ja niiden noudattamiseen liittyen (kuvio 9). Suurin osa haastateltavista koki tietoturvakäytänteiden olevan tärkeitä ja he ymmärsivät, miksi tietoturvakäytänteitä tulee noudattaa.

> No siis kyllä mä niinkun ymmärrän, että ne [tietoturvakäytänteet] on tärkeitä ja on pakko olla tiukat käytännöt ja niitä on pakko noudattaa, tai voi tulla isojakin vahinkoja. Hyvä asia ja on tärkeä noudattaa. (H1)

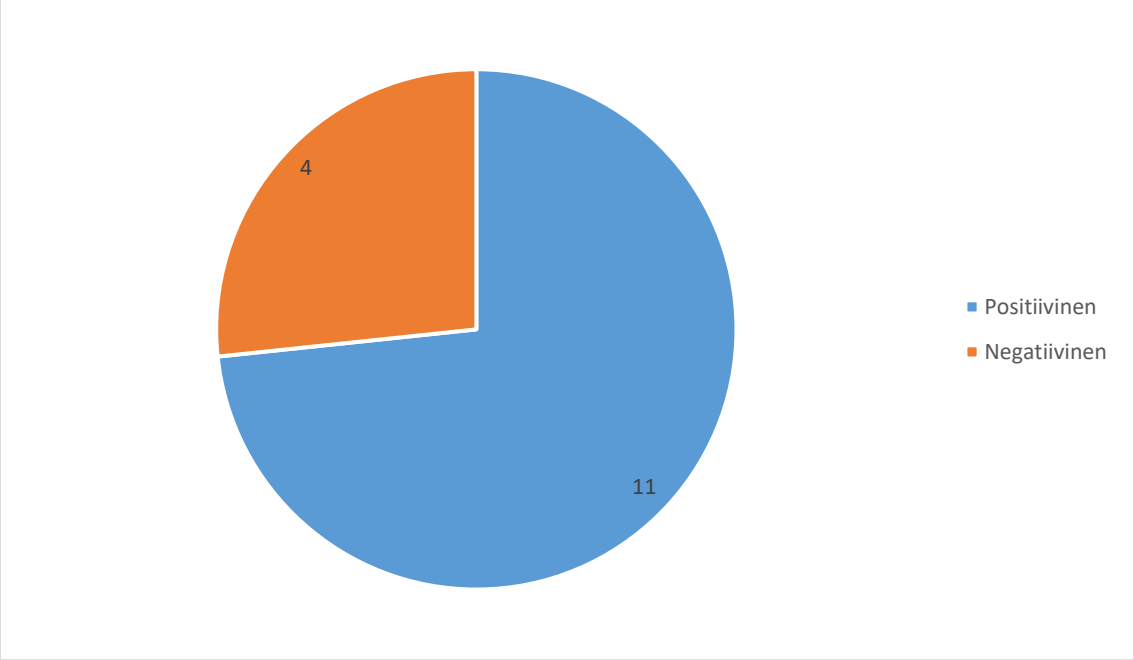
[IT-]Alalla kun ollaan, niin monet noista käytännöistä tuntuu semmosilta niin kuin aika maalaisjärjen omaisilta, tavallaan itsestäänselvyyksiltä. (H2)

Hyvin positiivisia, kun mä tykkään, että niin on tietynlaiset tietoturvakäytänteet ja se että kaikki noudattaa niitä, koska se oikeesti parantaa kaikkien turvallisuutta ja sitä, että ei vuoda tietoja nettiin. Ei se voi olla silleen, että ollaan kuin villissä lännessä tässä hommassa, että totta kai pitää ne ottaa huomioon, kun mekin käsitellään tosi sensitiivistä dataa. Sitä pitää käsitellä oikein. (H3)

No kyllä ne mun mielestä tuo semmosta varmuuden ja turvallisuuden tunnetta, on hyvä, että niitä on olemassa. Kaikille tehdään tavallaan selväks, että mikä on ok ja mitä pitäisi sitten noudattaa. Positiivisia tunteita siis oikeestaan aika pitkälti. (H4)

Mun mielestä ne on tärkeää olla olemassa, varsinkin mitä isompi firma kyseessä niin se, että jengi lähtee mukaan tietoturvaan ja yleiset linjaukset mahdollistaa ylläpidettävyyden. Jos tapahtuu joku virhe niin on helpompi selvittää, kuka on vastuussa. (H11)

On se jotenkin hirmu selkeetä, että noudatetaan käytänteitä ja miksi niitä noudatetaan. (H15)



KUVIO 9 Haastateltavien suhtautuminen tietoturvakäytänteisiin

Osa haastateltavista kuitenkin suhtautui tietoturvakäytänteisiin enemmän negatiivisesti.

No on ne vähän semmonen pakollinen paha. (H6)

Tietoturvakäytänteet ei haittaa kauheasti jokapäiväistä työskentelyä, mutta kyllä välillä ne ärsyttävät. (H9)

> Joskus voi olla semmosia, että ne hidastaa tai muuten suoraviivaisemman tehtävän muuttaa mutkikkaammaksi. (H12)
>
> Hyvin pitkälti nimenomaan turhautumista ja välillä epäilystä siitä, että kun on tekemässä jotain tietoturvaan liittyvää asiaa ja koittaa tehdä sen oikein, niin on semmonen fiilis, että ei oo ihan varma, onko nyt tekemässä oikein. (H13)

Haastatteluiden alkupuolella haastateltavilta myös kysyttiin, kuinka hyvin tietoturvasta ja tietoturvakäytänteistä kommunikoidaan heidän mielestään heidän organisaatiossaan. Useat haastateltavat kertoivat, että kommunikointi on ollut vähäistä ja he kokisivat yleisemmän kommunikoinnin hyödylliseksi.

> Aika huonosti, koska ei kauheesti tuu mitään informaatiota noista. (H3)
>
> No tuntuu siltä, ettei niistä oikeen ihan hirveesti ollut puhetta. (H2)

7.2 Stressaaviksi koetut tietoturvakäytänteet

Haastatteluissa tuli esille suuri määrä erilaisia tietoturvakäytänteitä, jotka haastateltavat kokivat stressaaviksi. Näitä olivat muun muassa salasanavaatimukset, arkaluontoisen tiedon käsittely ja kaksivaiheisen kirjautumisen käyttäminen. Esille tulleet tietoturvakäytänteet luokiteltiin ryhmiin, joita muodostui neljä kappaletta. Nämä ryhmät ovat salasanakäytänteet, tietoturvateknologiat, tiedon tietoturvakäytänteet ja laitekäytänteet.

7.2.1 Salasanakäytänteet

Salasanakäytänteistä tunnistettiin neljä yksittäistä tietoturvakäytännettä, jotka haastateltavat kokivat stressaaviksi. Ensinnäkin salasanakäytänteistä salasanojen luomiseen liittyvät salasanavaatimukset koettiin eniten stressaavimmaksi tekijäksi. Esimerkiksi H1 ja H10 kokivat kyllä ymmärtävänsä organisaatioidensa järjestelmien salasanavaatimukset, mutta ne ovat heidän mielestään turhan monimutkaiset. Monimutkaiset salasanavaatimukset vaikeuttavat uuden salasanan keksimistä.

> Salasanavaatimukset joihinkin palveluihin on vähän turhan vaativat. Hirveästi erikoismerkkejä, pieniä kirjaimia, isoja kirjaimia. En välttämättä koe näitä tarpeelliseksi. (H1)
>
> Kuukauden välein joudutaan salasanat vaihtamaan. Ei mulla loputtomiin ole kahdeksanmerkkisiä salasanoja. Sekin on semmoinen pakkojuttu. (H10)
>
> Meillä pitää olla joku kryptinen 20-merkkinen salasana. On se ärsyttävää välillä. Se on aika montaa kertaa mulla vaihtunut, kun on soppari vaihtunut. Ja sitten tulee uusi salasana. (H11)

H15 kertoi, että heidän organisaatiossaan salasanavaatimukset ovat niin monimutkaiset, että uuden salasanan määrittämiseen menee usein jopa enemmän aikaa, kuin järjestelmässä työtehtävän suorittamiseen menevää aikaa.

> Niissä [salasanoissa] on aivan järkyttävät vaatimukset. Kyllä ne [salasanavaatimukset] silleen ymmärtää, ettei salasana voi olla ”salasana”. Mutta etenkin jotkut ohjelmat mitä nykyisessä työssä käytän, niin niihin on tosi hankala keksiä se salasana ja sehän pitäisi vielä sitten jotenkin muistaa. (H15)

Toisena salasanakäytänteisiin liittyvänä tietoturvakäytänteenä oli salasanan vanheneminen liian nopeasti. H7, H8 ja H15 kokivat, että salasanan vaihtaminen usein vie heiltä liikaa arvokasta työaikaa.

> Vaikka esimerkiksi se, että asiakastunnuksiin on määrätty tietynlainen vanhenemisaika, esimerkiksi kaksi kuukautta. Eli et pääse kirjautumaan järjestelmään, jos et uusi sitä [salasanaa] ennen ja sieltä tulee varoitusviesti sitä ennen [vanhenemista]. Mutta sitten tulee projekti ja asiakas päättää, että ne [salasanat] vaihdetaankin kuukauden välein. (H7)

> Meillä on järjestelmä, jonka salasana vanhenee liian usein, vaikka sitä käytetään säännöllisesti. (H8)

> Meillä pitää nykyään aika usein uusia nuo salasanat. Kyllähän sitä välillä ajattelee, että eikö tässä nyt voisi kuukauden vielä tällä vanhalla mennä. (H15)

Kolmantena salasanakäytänteisiin liittyvänä stressaavana asiana oli se, ettei salasanaa voi tarvittaessa vaihtaa itse. H7, H8 ja H13 kertoivat, että he kokevat stressiä salasanan uusimisesta etenkin tilanteissa, joissa se tulee yllättäen ja vie liikaa aikaa. Tällöin he saattavat kiireiden lomassa joutua turvaamaan kollegaan, joka vaihtaa heille salasanan.

> Toki järjestelmä ilmoittaa, että salasana on vanhentunut, mutta se on turhauttavaa, kun on kiireinen päivä ja salasanat on vanhentunut, ja lisäksi jos on semmonen palvelu, mihin ei voi itse vaihtaa salasanaa, niin pitää pyytää vaikkapa työkaveria vaihtamaan. (H7)

> Kun et voi käyttää tietokonetta salasanan vanhentumisen takia ja koska et voi vaihtaa sitä [salasanaa] itse. Pitää ottaa Helpdeskiin yhteyttä ja se vie paljon aikaa. (H8)

Salasanakäytänteisiin liittyvä neljäs stressitekijä on suuri salasanojen määrä. Haastateltavat H7 ja H14 kokivat suuren salasanojen määrän stressaavaksi, jonka stressaavuutta myös lisää salasanahallintapalvelun puuttuminen.

> Asiakas haluaakin henkilökohtaiset tunnukset, eikä yhteiskäyttötunnuksia. Asiakkaiden salasanakäytänteiden määrä on todella suuri. Tännekin on tämä salasana ja tuonne toinen salasana. (H7)

> Kyllähän salasanat ja niihin liittyvät käytänteet välillä voi turhauttaakin, että meillä on käytännössä yli 100 paikkaa, jossa pitäs olla varmastikin omat salasanat mutta eihän se ole käytännössä mahdollista. (H14)

7.2.2 Tietoturvateknologiat

Toisena tunnistettuna stressaavana tietoturvakäytänneluokkana on tietoturvateknologiat. Tähän ryhmään kuuluvat kaikki tietoturvakäytänteet, jotka liittyvät erilaisiin teknologisiin ratkaisuihin tietoturvan varmistamiseksi. Haastatteluissa tuli esille kolme erilaista tietoturvateknologiaa, jotka ovat VPN-yhteyden käyttäminen, kaksivaiheinen tunnistautuminen ja salatun sähköpostin käyttö. VPN-yhteyden käytön stressaavaksi kokivat haastateltavat H1, H2, H6 ja H9.

> Vaikka on toimiston verkossa, niin tarvitsee vielä VPN-yhteyden, että pääsee yhteen paikkaan. Lähinnä se, että tarvitsee vielä toisen vaiheen, että ei riitä, että on toimiston verkossa. Vaikka luulisi riittävän, sillä [toimiston verkolla] kuitenkin pääsee jo moneen paikkaan, millä ei pääsisi verkon ulkopuolelta. Mutta sitten tarttee kuitenkin vielä ylimääräisen VPN-yhteyden. (H1)

> Sitten töissä, kun työkoneella laittaa VPN-yhteyden päälle, niin se joskus sotkee puhelinjärjestelmän. Kun lyöt VPN päälle niin alkaa pätkimään puhelinjärjestelmän yhteyttä. (H2)

> Kyllähän ne [tietoturvakäytänteet] on lisänneet työmäärää. Varsinkin lisää viivettä esimerkiksi tunnusten hakemisessa, että pitää tehdä selvityksiä, monivaiheisia hyväksymisiä ja pitää asentaa ohjelmia tai VPN-yhteyden käyttäminen. Kyllähän se vähän turhauttaa ja stressaa. (H6)

> Tuli vielä VPN:stä mieleen, että tietyissä järjestelmissä meillä tarvii sitä, että sun pitää olla yliopiston netissä, että pääset kirjautumaan sisään. Se on vähän ärsyttävää, kun ei suoraan lue missään tai ole mitään listausta, että miten minnekin pääsee. (H9)

Toisena tietoturvateknologioihin liittyvä stressaava tekijä oli kaksivaiheisen tunnistautuminen, jonka H1, H3, H9 sekä H13 kokivat stressaavaksi.

> RSA-avain, se mikä vaihtuu koko ajan nopeasti, se vähän tuntuu siltä, että onko se nyt tarpeellinen, kirjoitat vähän ja se menee väärin ja numero taas vaihtuu tai pitää odotella, että se vaihtuu. (H1)

> Kaksivaiheinen tunnistautuminen, se on todella hyvä, mutta se on myös raivostuttava. Aina joutuu kaivaa sen puhelimen ja varsinkin jos se on toteutettu niillä tekstiviesteillä. Sit sä näet sen koodin sieltä ja odotat ensin mahdollisesti 5 minuuttia että se tulee sieltä. (H3)

> Se kaksivaiheinen tunnistautuminen on ärsyttävä ja uusi lisä. Se oli ennen vapaaehtoinen, mut nyt se on pakollinen. (H9)

> Meillä on organisaation sisäinen Teams käytössä, mikä on muuten oikein hyvä, mutta sinne pitää kirjautua kerran kuukaudessa. Ja jotta sinne pääsee kirjautumaan, niin sinne vaatii puhelinnumeron, joka liitetään sinun organisaatiosi sähköpostiin, siis työpuhelimen numero. Ja kerran kuukaudessa se pyytää sun tunnusta, joka tulee kerran kuukaudessa puhelimeen. Ja se ei aina todellakaan toimi, voi mennä useitakin tunteja, että sä saat sen puhelimeen. Eli kaksivaiheinen tunnistautuminen stressaa. (H13)

Kolmas tietoturvateknologioissa stressaavana tekijänä oli salatun sähköpostin käyttäminen. Sen kokivat stressaavaksi haastateltavat H2 ja H13.

> Sit mikä työssä niin kun ärsyttää niin on se, että pitää lähettää koneella sähköposteja asiakkaalle, niitä ei voi lähettää tavallisen sähköpostin kautta vaan aina pitää niin kuin salata erikseen. (H2)

> Se [tietoturvakäytänteiden stressaavuus] on liittynyt asiakkaiden tietojen lähettämiseen toiselle yritykselle. Oikea käytänne oisi se, että pitäs käyttää tuota turvapostia. Meillä ei ole turvapostia käytössä, heillä [toisella organisaatiolla] on se. (H13)

7.2.3 Tiedon tietoturvakäytänteet

Kolmas stressaavaksi ilmennyt tietoturvakäytänneluokka oli tiedon tietoturvakäytänteet. Lähes puolet haastateltavista koki organisaation arkaluonteisen tiedon, kuten asiakastiedon, käsittelyn ja kommunikoinnin stressaavaksi. Tämän tietoturvakäytänneryhmän stressaavaksi kokivat H2, H5, H12, H13, H14 ja H15.

> Sitten myös, että töitä ei voi tehdä missä vaan, vaan pitää ottaa huomioon tietoturvajutut, että kuka kuulee tai on samassa tilassa. Pienessä kämpässä varsinkin se on vähä ongelmana, että jos joku on kylässä niin et voi tehdä mitään hommia, jotta ei paljasta tietoja. (H2)

> No ehkä tavallaan se, että niin kun minkälaista tietoa voi jakaa sidosryhmien välillä. Tai sitten niin kun esimerkiksi, jos joku kaveri kysyy mitä teit tänään töissä, niin siinä tulee semmonen turhautuminen. Vois selittää suoraan, että mitä on tehny, mutta sitten taas ei välttämättä tiedä voiko niin sanoa, sitten tulee vaan sanottua hyvin suppeasti. (H5)

> No just asiakastietojen käsittely [stressaa]. Itse asiassa eilen todettiin, että [tietoja] on tullut väärään paikkaan ja ne pitäis jonnekkin siirtää. Sitten pitäs keksiä, että minne ne siirretään. Ne on periaatteessa ollut voinut olla uhattuna. Jos joku tarpeeks tietää niin pääsisi käsiksi. (H12)

> Me pyritään kertomaan vaan etunimi ja sukunimen 1. kirjain, mutta sitten siellä saattaa olla, että meillä onkin monta samalla etunimellä ja sukunimen 1. kirjaimella olevia henkilöitä, ja myöskin jos keskustellaan meidän työntekijöiden kanssa näistä, niin välillä on silleen vähän, että mitenkä paljon me uskalletaan sanoa siitä sukunimestä eteenpäin, että voidaan erotella ne niin, että jos joku ulkopuolinen näkisi ne viestit niin hän ei voisi tunnistaa tätä henkilöä. (H13)

> [Stressaavuus liittyy] Ehkä pääosin asiakkaisiin liittyvään dataan ja sen käsittelyyn. Sekä se, että ei vahingossa luovuta mitään tietoja mitä ei tulisi luovuttaa, mutta toisaalta myös se, ettei hävitä tai tuhoa tietoja, joita ei välttämättä ole varmuuskopioitu. (H14)

> Miten henkilötietoja sisältävistä asioista kommunikoidaan, niin ei ole käyty hirveän selkeästi läpi. Ja kun tehdään täysin etänä, se koskee varmaan kaikkea mikä muutenkin koskee niitä. Ehkä semmoinen epätietoisuus jää siitä, perusjutut on selkeitä. (H15)

7.2.4 Laite- ja USB-käytänteet

Viimeinen tunnistettu stressaava tietoturvakäytänneluokka on laite- ja USB-käytänteet. Laitekäytänteisiin kuuluvat tietokoneen lukitseminen, käyttöoikeuksien hakemisen ja USB-käytänteet. Ensimmäisen tietoturvakäytänteen, eli tietokoneen lukitsemisen stressaavaksi kokivat haastateltavat H2 ja H9.

> Koneen lukitseminen voi välillä tuntua vähän siltä [stressaavalta], että jos nopeesti jossain käy. Toki siinä taustalla pitää ymmärtää miksi niin pitää tehdä. (H2)

> Mun kone lukittautuu tosi nopeesti. Sitä vois varmaan ehkä mennä vaihtamaan asetuksista, mut ei välttämättä kyllä. Se menee niin nopeesti pimeeks, että jos mä käyn vaikka vessassa välissä tai jossain on jotain muuta mitä tekee, niin se on sitten kirjautunut ulos, että pitää salasana laittaa uudestaan. (H9)

Myös laitteiden ja järjestelmien käyttöoikeuksien hakeminen koettiin stressaavaksi. H6 ja H12 kokivat käyttöoikeuksien hakemisen turhan monimutkaiseksi ja aikaa vieväksi prosessiksi.

> Kyllähän ne [tietoturvakäytänteet] on lisänneet työmäärää. Varsinkin lisää viivettä esimerkiksi tunnusten hakemisessa, että pitää tehdä selvityksiä, monivaiheisia hyväksymisiä ja pitää asentaa ohjelmia. (H6)

> Joskus aiemmin on ollut, että lomakkeita pitää täyttää ennen, kun pääsee sitä varsinaista [työtä] tekemään. Kyllä siihen turhaa aikaa vähän kuluu. (H12)

Viimeisenä laitekäytänteisiin liittyvänä tietoturvakäytänteenä oli USB-käytänteet. H11 koki ne stressaavaksi.

> Laitteiden kanssa [on ollut stressiä], kun niissä ei oo semmosta selkeitä linjauksia. Saako käyttää omia hiiriä tai näppäimistöjä. Laitteiden tietoturva, se on ehkä se mistä mulle on tullu stressiä. (H11)

> Mä oon välillä ladannu jotain mun kännykkään työkoneen USB:sta, ja mä oon ehkä tietoisestikin toiminut tietoturvakäytänteiden vastaisesti. Se on ollu mulle semmonen mistä on aiheutunut stressiä. USB-käytänteet ja laitteiden käyttö on ollu eniten stressiä aiheuttavia. (H11)

7.3 Tietoturvakäytänteiden stressaavuuden syyt

Tässä alaluvussa käydään läpi haastateltavien esittämiä syitä heitä stressaaville tietoturvakäytänteille. Alaluvun rakenne on samanlainen kuin edeltävässä alaluvussa, eli vastaukset käydään läpi samojen tietoturvakäytänneluokkien avulla.

7.3.1 Salasanakäytänteet

Salasanakäytänteiden stressaavuuden syitä oli useita ja ne vaihtelivat. Salasanavaatimuksien osalta haastateltavat H1, H11 ja H15 kertoivat salasanan muistamisen olevan hankalaa monimutkaisten salasanavaatimuksien takia. H1 ja H15 myös kertoivat salasanan keksimisen kuormittavaksi, sillä monimutkaisten salasanavaatimusten vuoksi siihen pitää käyttää runsaasti aikaa.

> No varmaan se ylimääränen aika mikä menee, luot hirveän vaikean salasanan, sen unohtaa helpommin. (H1)

> En mä muista sitä [salasanaa] ulkoo ikinä niin oon pitäny sitä kännykässä. Kyllä se hidastaa. (H11)

> Niihin on tosi hankala keksiä se salasana ja sehän pitäs vielä sitten jotenkin muistaa. Tavallaan se pituus ja millaisia merkkejä pitää sisältää, missä järjestyksessä. (H15)

Salasanojen vanheneminen puolestaan koettiin stressaavaksi sen takia, että salasana pitää vaihtaa usein. H7 myös lisäsi, että hän kokee stressiä jo ennakkoon, jos tietää, ettei voi olla vaihtamassa salasanaa ennen sen vanhenemista.

> Ja sit ku me tehdään semmosta työtä, ettet voi olla sellaisessa vuorossa, että voisit vaihtaa sen salanan. Siitä tulee semmonen stressi, että et voikaan vaihtaa ajoissa. Se turhauttaa siis, että kun salasana pitäisi vaihtaa parin kuukauden välein, niin sitten se pitääkin vaihtaa kuukauden välein. (H7)

> No tietysti, jos hirveen tiuhaan on tämmösiä salasanojen uusimisia, esimerkiksi johonkin sisäiseen verkkoon. Meillä pitää nykyään aika usein uusia nuo salasanat. Kyllähän sitä välillä ajattelee, että eikö tässä nyt voisi kuukauden vielä tällä vanhalla mennä. (H15)

Haastateltavat kokivat työtehtävien tekemisen hidastumisen ja ylimääräisen ajan käyttämisen olevan stressaavuuden syynä tilanteissa, joissa he eivät itse pysty vaihtamaan vanhentunutta salasanaa.

> Ja lisäksi jos on semmoinen palvelu, mihin ei voi itse vaihtaa salasanaa niin pitää pyytää vaikkapa työkaveria vaihtamaan. Se hidastaa työtehtävien tekemistä hirveästi. (H7)

> Se on stressaavaa etenkin kiireiseinä päivänä, kun et voi käyttää tietokonetta vanhentuneen salasanan takia, ja sitä ei voi edes vaihtaa itse. Sun pitää soittaa Helpdeskiin, se vie paljon aikaa ja sieltä ei aina edes vastata. (H8)

Suuren salasanamäärän stressaavuuden taustalla puolestaan on niiden muistamiseen liittyvät ongelmat, varsinkin, jos organisaatiossa ei ole käytössä salasanojen hallintapalvelua.

> Mutta sitten asiakas haluaakin henkilökohtaiset tunnukset, eikä yhteiskäyttötunnuksia. Se asiakkaiden salasanakäytänteiden määrä on todella suuri. Tännekin on tämä salasana ja tuonne toinen. (H7)

> Salasanahallinta on siis aiheuttanut stressiä ja turhautumista. Se stressi ilmenee siihen liittyvänä hallintana ja se niin kun nimenomaan turhautumista siitä, ettei ole sulavaa se työskentely. Ei ole käytössä salasanhallinta palveluakaan. (H14)

7.3.2 Tietoturvateknologiat

Tietoturvateknologioista VPN-yhteyden käyttö koettiin stressaavaksi erinäisistä syistä. H1 koki VPN-yhteyden käytön aikaa vieväksi ja työlääksi, H2:n organisaatiossa VPN-yhteys aiheuttaa häiriöitä muihin järjestelmiin, ja H9 koki VPN-käytön ohjeistuksen epäselväksi.

> Lähinnä se, että tarvitsee vielä toisen vaiheen, että ei riitä että on toimiston verkossa. Vaikka luulisi riittävän, sillä kuitenkin pääsee jo moneen paikkaan, millä ei pääsisi verkon ulkopuolelta. (H1)

> Kun lyöt VPN päälle niin alkaa pätkimään puhelinjärjestelmän yhteyttä. Siitä tulee pientä stressiä, kun pitää yrittää luottaa siihen, että työkalut toimisivat mutta sitten aina ei toimikaan. (H2)

> Se on vähän ärsyttävää, kun ei suoraan lue missään tai ole mitään listausta, että miten minnekin pääsee. Sen oon huomannu, että tieto on tosi piilossa, että sun pitää kaivamalla kaivaa oikeesti ne. (H9)

Kaksivaiheisessa tunnistautumisessa puolestaan stressaavuuden pääasiallisena syynä oli se, että sen käyttö vei aikaa ja kaksivaiheista tunnistautumista piti käyttää yhtäkkiä. Osa haastateltavista koki stressiä jo pelkästään kaksivaiheisen tunnistautumisen ajattelemisesta.

> Se on ehkä se vaiva mikä sun pitää nähdä. Sä kaivat sen puhelimen sieltä esiin, ja jos on muita kiireitä ja sit sä joudut kaivaa sen puhelimen sieltä esiin. Sillä välin, kun sun pitäs kuunnella sitä asiakasta ja selvittää tilannetta. Silloin se tuntuu turhalta ja raivostuttavalta, varsinkin sovellukset time outtaa [aikakatkaisee] yhteyden tosi nopeesti, monesti just ne mitkä vaatii sitä kaksivaiheista tunnistautumista. (H3)

> Omasta mielestä on turhaa, jos se yhtäkkiä heittää sut ulos [kirjautuu ulos] niin miksi. Kyllä mä ymmärtäisin, jos uudella laitteella koittaisi, mut jos se tekee tommosia random heittämisiä välillä niin ärsyttää. En tiiä kuinka paljon enemmän stressaisi sitten kiireisinä päivinä, jos pitäisi alkaa aina vahvistelemaan kirjautumista, jos pitää johonkin vaikka heti vastata tai palaveri on alkamassa. (H9)

> Se vei jo minun valmiiksi vähistä työtunneista aikaa yllättävän paljon aikaa pois. Varsinkin just se, että työt viivästyvät, välillä on semmosia, että pitää hyvin nopealla aikataululla saada asioita tehtyä Teamsin puolella, se just aiheuttaa ylimääräisestä stressiä. Ja jo pelkästään sen ajatteleminen, eli kun tiedostaa, että kuukausi on kohta lopullaan ja kohta se Teams tulee taas kyselemään sitä [kaksivaiheista tunnistautumista], se aiheuttaa entisestään stressiä. Jos ei ole merkannut sitä kalenteriin ylös niin se tulee aina vähän yllätyksenä lisäksi. (H13)

7.3.3 Tiedon tietoturvakäytänteet

Tietoon ja sen käsittelyyn liittyvissä tietoturvakäytänteissä eniten stressaavana asiana koettiin olevan tietoturvakäytänteiden epäselvyys tiedon käsittelyyn liittyen. Osa haastateltavista ei ollut tietoinen, mikä on oikea toimintapa jossain tilanteessa, ja osa koki tietoturvakäytänteiden olevan vaikeaselkoisia. Osa haastateltavista myös koki tietoturvakäytänteiden vähyyden tai puuttumisen oleva stressaava tekijä.

> Jos on itse sisäistänyt, että näin voi sanoa, sitten jos ilmenee, että ei voikkaan niin sitten siitä tulee stressiä, että mitä kaikkea on mennyt sanomaan. (H5)

> Ne on periaatteessa ollut voinut olla uhattuna. Jos joku tarpeeks tietää niin pääsisi käsiksi. Mutta aina se, että jos kysytään että tarvitsemme nimen sinulta niin sitten asiakas antaa henkilötunnukset ja katuosoitteet ja hyvä ettei pankkitilitietoja anna. (H12)

> Totta kai meille se on tiedossa, ettei sais lähettää, mutta kun ne ei ala lähettämään meille sitä turvapostia, vaan ne sanoo, että lähettäkää vaan suoraan normaalisti, niin sitten on vähän ollut että mitenkähän tarkkaa tää sitten oikeesti on. (H13)

> Kun niitä [tietoturvakäytänteitä] ajattelee tarpeeksi pitkälle, niin sen mitä niin kun on tekemässä oikein, sen voi helposti kääntää semmoseks, että ei nyt kuulosta oikeelle. Että tän vois tehdä myös paremmin. Ja että vois olla paljonkin tarkempaa nämä käytänteet. (H13)

> Siinä on vähän jargonia [IT-alan ammattisanastoa]. Siellä tulee semmosia tilanteita paljon vastaan, missä on hyvin yksittäisiä tilanteita ja tapauksia, mihin pitää sitten pyrkiä jokaisessa eri tilanteessa ja tapauksessa katsomaan parhaansa mukaan, mitenkä asiat pitää hoitaa. (H13)

> Jos vielä tarkennan, niin niiden [tietoturvakäytänteiden] puuttumisesta. Pieni firma, niin välttämättä ei ole kaikkiin tilanteisiin ei ole olemassa kauhean tarkkaa ohjeistusta tai käytännettä, voi aina välillä vaatia soveltamista. Se voi johtaa sitten stressaantumiseen kyllä. (H14)

> Ehkä semmonen epätietoisuus jää siitä. Ehkä on semmosia tiettyjä asioita, mitä vois vielä joku tarkentaa. Just kun sähköisesti kommunikoidaan asioista, kun etänä tehdään töitä, niin millaisia tietoja sinne sitten voi työkaverille laittaa. Mitä saa laittaa ja mitä pitäs sensuroida. (H15)

7.3.4 Laite- ja USB-käytänteet

Tietokoneen lukitsemisen haastateltavat kokivat stressaavana ylimääräisenä työvaiheen takia ja siksi, että se vie liikaa aikaa heidän muilta työtehtäviltään.

> Se on ehkä just se että, ihan lyhytaikaisesti meet johonkin pois, yksinkertainen ja nopee juttuhan se on. (H4)

> Se tietenkin vie aikaa enemmän, mikä ärsyttää. Se on eri asia, jos mä oisin työpaikalla ja menisin alakertaan syömään, niin sillon mä ottasin koneen mukaan ja kirjautuisin ulos. Mutta jos mä oon etätöissä kotona, mä oon yksin kotona, ei kukaan siinä välissä pääse menemään koneelle. (H9)

Laitekäytänteissä ja USB-käytänteissä H11 stressasi epäselvyys, mikä on sallittua ja mikä ei.

> Mä en tiiä saako niin tehdä ja mä en ehkä itekkään tiedä niinkun miten suuri riski on, että onko tää nyt sallittua. Mä veikkaan, että se on linjattu, ettei saa käyttää omia laitteita mut en sit tiiä varmaksi. (H11)

Tunnusten hakemisen stressaavuuden taustalla oli ainoastaan lisääntynyt työmäärä.

> Kyllähän ne on lisänneet työmäärää. Kyllähän ne lisäävät työtä, tai ei siis lisää työtä mutta lisää viivettä. Kyllähän se vähän turhauttaa, esimerkiksi juuri ne tunnushaut. (H6)

> Kyllä siihen sinänsä turhaa aikaa vähän kuluu. (H12)

7.4 Turvallisuusstressin muuttuminen

Tutkimuskysymyksillä tavoiteltujen tuloksien lisäksi haastatteluista nousi esille myös mielenkiintoisia tietoturvakäyttäytymisen ja koetun turvallisuusstressin muuttumiseen liittyviä seikkoja. Haastatteluissa kysyttiin haastateltavilta, kuinka heidän työskentelytapansa ja työskentelytottumukset on muuttuneet tietoturvakäytänteiden myötä. Useat haastateltavat kertoivat, että he ovat nykyään tietoturvakäytänteitä noudattaessaan entistä varovaisempia ja ajattelevaisempia tietoturvakäyttäytymisestään.

> Pieni varovaisuus siihen [tietoturvakäyttäytymiseen] tulee. Että ei kirjoita heti kaikkea mitä mieleen tulee, vaan mietti että mitä kaikkea minä voin tästä jakaa. (H5)

> Jos on ajatellut, että jonkun asian vois tehdä tosi nopeesti, mutta sit tulee tarkentavia käytäntöjä tietoturvakäytännöistä. Että et voi hakee tiettyä tietoo ihan sokkona vaan, tai pitää tietyt asiat mennä tiettyjen hyväksyntäprosessien läpi. Että et voi tehdä kaikkea suoraan vaikka tietäisit sen olevan ok. (H6)

> Jotkut asiat tekee harkitummin. Jos miettii jotain salasanoja tai minne ne kirjaa ylös. (H11)
>
> Ei sähköpostiin laita kaikkia tietoja, varsinkaan salaamattomia tai tämmöisiä. Niitä [tietoturvakäytänteitä] vähän ajattelee nykyään enemmän. (H12)
>
> On ne joo muuttunut. Niillä [tietoturvakäytänteillä] on ollu semmonen vaikutus, että on tarkempi ja huolellisempi. Että tavallaan monta asiaa joutuu tarkistamaan tai miettimään. (H14)

Osa haastateltavista puolestaan kertoi, ettei tietoturvakäytänteet ole juurikaan muuttanut heidän työskentelytapojansa tai työskentelytottumuksia. Tällaiset haastateltavat eivät kertoneet kokevansa kovin suurta turvallisuusstressiä. Haastateltavilla oli ollut jo kokemusta tietoturvakäytänteiden noudattamisesta entuudestaan tai he kykenivät ymmärtämään tietoturvakäytänteiden merkityksen kattavasti.

> No en kyllä sanoisi, koska ei ole tullut mitään uutta tietoturvatietoa mikä olisi muuttanut radikaalisti. Samalla maalaisjärjellä mennään edelleen. **(H2)**
>
> Oman koulutuksen ja tutkimuksen kautta on tullut selväksi, että jos tietoturvasta ei pidä huolta niin se on paljon pahempi kuin se, että käytät muutaman minuutin aikaa, että huolehdit siitä. (H3)
>
> No en sanos, että on muuttunut, kun aika samat ovat, kuin aikaisemmissa työpaikoissa ollut. Ehkä ne ovat semmosia perusjuttuja kuitenkin mitä on aiemmin ollu, niin ei oikeen muuttanut toimintatapoja. (H15)

8 JOHTOPÄÄTÖKSET

Tässä luvussa käydään läpi tutkimuksen tuloksien perusteella esitettävät johtopäätökset. Luku on jaettu kolmeen alalukuun, joista ensimmäisissä vastataan tutkielman kahteen tutkimuskysymykseen tuloksien pohjalta. Tuloksia ja johtopäätöksiä myös samalla yhdistetään kirjallisuuskatsauksessa tarkastellun turvallisuusstressin ja tietoturvakäyttäytymisen aikaisempaan kirjallisuuteen. Toinen alaluku kattaa tutkielman kontribuutioiden läpikäynnin tutkimukselle ja käytännölle. Alaluvussa siis esitetään asioita ja tapoja, joilla tämän tutkielman tuloksia voidaan hyödyntää esimerkiksi organisaatioiden ja työntekijöiden näkökulmasta. Viimeisessä alaluvussa käydään läpi tutkielman tunnistetut rajoitteet sekä niistä avautuvat jatkotutkimusaiheet.

8.1 Tutkimuskysymyksiin vastaaminen

Tutkielmalle määriteltiin kaksi tutkimuskysymystä, jotka olivat ”Millaiset tietoturvakäytänteet suomalaiset IT-alan työntekijät kokevat stressaaviksi?” ja ”Miksi ensimmäisen tutkimuskysymyksen tietoturvakäytänteet ovat stressaavia?” Tutkielmassa siis haluttiin saada selville ensiksikin stressaaviksi koettuja tietoturvakäytänteitä sekä syitä niiden stressaavuudelle. Haastatteluissa tuli esille useita erilaisia tietoturvakäytänteitä ja stressitekijöitä, jotka haastateltavat kokivat stressaaviksi. Esille tulleet stressaavat tietoturvakäytänteet on koottu alla olevaan taulukkoon tietoturvakäytänneluokan perusteella (taulukko 13). Esille tulleet tietoturvakäytänteet ja niiden stressitekijät luokiteltiin tietoturvakäytänneluokkiin, joita muodostui neljä kappaletta. Nämä luokat ovat salasanakäytänteet, tietoturvateknologiat, tiedon tietoturvakäytänteet ja laitekäytänteet. Tietoturvakäytänteiden stressaavuuden syyt koottiin myös yhteen ja yhdistettiin tutkimuskirjallisuudessa määriteltyihin turvallisuusstressin stressitekijöihin, jotka löytyvät taulukosta alempaa (taulukko 14). D’Arcy ym. (2014) mukaan turvallisuusstressin stressitekijöinä on ylikuormitus, monimutkaisuus ja epävarmuus. Ylikuormitus liittyy työtehtäviin käytettävissä olevan työajan vähentymiseen

tietoturvakäytänteiden noudattamisen vuoksi, monimutkaisuus on tietoturvakäytänteiden hankalaa ymmärrettävyyttä, ja epävarmuus liittyy tietoturvakäytänteiden lisääntymiseen, muuttumiseen tai muuhun epävarmuuteen (D'Arcy ym., 2014). Haastatteluissa esille tulleiden stressaavien tietoturvakäytänteiden stressaavuuden syissä hyödynnettiin tätä alkuperäistä määritelmää selittämään, miksi tietyt tietoturvakäytänteet koetaan stressaaviksi.

TAULUKKO 13 Stressaaviksi koetut tietoturvakäytänteet

Luokka	**Tietoturvakäytänne**	**Vastanneet haastateltavat**
Salasanakäytänteet	Salasanavaatimukset	H1, H10, H11, H15
	Salasanan vanheneminen	H7, H8, H13, H15
	Salasanaa ei voi vaihtaa itse	H7, H8
	Samaa salasanaa ei saa käyttää useissa paikoissa	H7, H14
Tietoturvateknologiat	VPN	H1, H2, H6, H9
	Kaksivaiheinen kirjautuminen	H1, H3, H9, H13
	Salattu sähköposti	H2, H13
Tiedon tietoturvakäytänteet	Arkaluonteisen tiedon käsittely	H2, H5, H12, H13, H14, H15
Laite- ja USB-käytänteet	Tietokoneen lukitseminen	H4, H9
	Käyttöoikeudet	H6, H12
	USB-käytänteet	H11

Salasanakäytänteet vaikuttavat olevan tuloksien perusteella yksi stressaavimmaksi koettu tietoturvakäytänneluokka, sillä kahdeksan haastateltavaa viidestätoista kertoi kokeneensa turvallisuusstressiä salasanakäytänteiden takia. Salasanakäytänteiden luokasta tunnistettiin neljä eri stressiä aiheuttavaa tietoturvakäytännettä, jotka ovat salasanavaatimukset, salasanan vanheneminen, salasanaa ei voi vaihtaa itse ja salasanojen suuri määrä. Salasanakäytänteiden ensimmäisellä tietoturvakäytänteellä, eli salasanavaatimuksilla tarkoitetaan laitteille ja järjestelmille asetettavia salasanoja, joiden laatimisessa työntekijöiden tulee noudattaa organisaation tietoturvakäytänteiden asettamia vaatimuksia. Salasanan tulee yleensä olla vähintään tietyn monta merkkiä pitkä, sen pitää sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä, eikä samaa salasanaa ei voi käyttää uudestaan. Haastateltavat kokivat, että salasanavaatimusten stressitekijöinä on monimutkaisen salasanan keksiminen sekä sen muistaminen. Esimerkiksi haastateltavan H10 organisaatiossa salasanan tuli olla tasan 8-merkkinen, eikä se voi sisältää enempää tai vähempää merkkejä. H10 myös kertoi, että hän kokee ongelmalliseksi sellaisen salasanan keksimisen, joka on vielä muistettavissa ja jonka luomiseen hän joutuu käyttämään entistä enemmän aikaa joka kerralla. Vastaavasti H11 kertoi, että heidän organisaatiossaan järjestelmät vaativat yli 20-merkkisen salasanan. Salasanan luominen on haasteellista ja aikaa vievää näiden vaatimusten takia. Molemmat stressitekijät vastaavat turvallisuusstressin ylikuormitusta, sillä monimutkaisen salasanan keksiminen ja sen muistaminen vie ylimääräistä aikaa. Uuden salasanan keksiminen voi myös pysäyttää työnteon, kunnes uusi salasana on asetettu. Uuden salasanan keksiminen liittyy myös turvallisuusstressin monimutkaisuuteen, sillä osa haastateltavista koki uuden salasanan

salasanavaatimuksien olevan epäselviä tai vaatimuksia ei esitetä selkeästi uuden salasanan luomisen yhteydessä.

TAULUKKO 14 Stressaavien tietoturvakäytänteiden stressitekijät

Tietoturvakäytänne	**Stressitekijä**	**Turvallisuusstressin stressitekijä (D'Arcy ym., 2014)**
Salasanavaatimukset	Salasanan keksiminen	Ylikuormitus ja monimutkaisuus
	Salasanan muistaminen	Ylikuormitus
Salasanan vanheneminen	Salasanaa ei ehdi vaihtamaan ajoissa	Ylikuormitus
	Salasanan pitää vaihtaa usein	Ylikuormitus
Salasanaa ei voi vaihtaa itse	Salasanan vaihtaminen vie paljon aikaa	Ylikuormitus
Samaa salasanaa ei saa käyttää useissa paikoissa	Salasanahallintapalvelun puuttuminen	Ylikuormitus
	Suuren salasanamäärän muistaminen	Ylikuormitus
VPN	Työnteon hidastuminen	Ylikuormitus
	Tekniset ongelmat	Ylikuormitus
	Epäselvät ohjeistukset	Monimutkaisuus
Kaksivaiheinen tunnistautuminen	Käyttö vie liikaa aikaa	Ylikuormitus
	Tekniset ongelmat	Ylikuormitus
Salattu sähköposti	Käyttö vie liikaa aikaa	Ylikuormitus
		Monimutkaisuus
Arkaluonteisen tiedon käsittely	Epäselvyys	Monimutkaisuus
	Puutteelliset tietoturvakäytänteet	Monimutkaisuus
Tietokoneen lukitseminen	Toistuva sisäänkirjautuminen	Ylikuormitus
Käyttöoikeudet	Pitkäkestoinen hakuprosessi	Ylikuormitus
Laitteiden käyttö	Epäselvyys	Monimutkaisuus
USB-käytänteet	Epäselvyys	Monimutkaisuus

Haastateltavat kokivat salasanakäytänteistä myös salasanan vanhenemisen stressaavaksi tietoturvakäytänteeksi. Sen stressitekijöiksi paljastui, ettei salasanaa voi aina vaihtaa ajoissa, ja sen vaihtamiseen kuluu aikaa. Salasanojen vanhenemisen stressitekijöiksi kerrottiin, ettei salasanaa pääse aina vaihtamaan ajoissa, sekä salasanan vaihtamaan usein joutuminen. Esimerkiksi H7 koki salasanan vanhenemisesta stressiä sen takia, että hän ei voi olla välttämättä aina paikalla vaihtamassa sitä, jolloin salasana menee lukkoon. H15 puolestaan koki turhautumista siitä, että salasanat tulee vaihtaa liian usein. Molemmat stressitekijät vastaavat ylikuormitusta, sillä ne aiheuttavat joko esteen työnteolle tai työntekijät joutuvat käyttämään salasanan vaihtamiseen ylimääräistä työaikaa usein. Luokan kolmas stressaava tietoturvakäytänne oli se, eli ettei salasanaa voi vaihtaa itse. Tämä koettiin erityisen stressaavana tilanteissa, kun salasana pitää vaihtaa äkillisesti tai kiireessä. Esimerkiksi H8 kertoi, että heidän organisaatiossaan salasanan voi vaihtaa vain soittamalla ulkoistettuun HelpDeskiin, josta ei aina edes

vastata. H8 koki tämän erityisen stressaavana silloin, kun hänellä oli töissä muutenkin kiireistä, jolloin työnteko käytännössä pysähtyi niin pitkäksi aikaa, kun hän sai salasanan vaihdettua. Tietoturvakäytänteen stressitekijänä olikin työnteon hidastuminen, sillä koska työntekijät eivät pysty vaihtamaan salasanaa itse, heidän työnsä pysähtyvät salasanan vaihtamiseen saakka. Tämä stressitekijä vastaa edellisten tavoin turvallisuusstressin ylikuormitusta. Salasanakäytänteiden viimeinen stressaavaksi havaittu tietoturvakäytänne on salasanojen suuri määrä, jolla käytännössä tarkoitetaan, ettei samaa salasanaa saa käyttää organisaation eri järjestelmissä. Muun muassa H14 kertoi, että hän joutuu hallitsemaan jopa 100 salasanaa eri järjestelmiin, jonka hän kokee haastavana ja hyvin stressiä. Koettua turvallisuusstressiä lisää se, ettei H14:n organisaatio tarjoa salasananhallintapalveluita. Tietoturvakäytänne aiheuttaa työnteon hidastumista monimutkaisen salasanahallinnan takia, joten se vastaa myös ylikuormitusta stressitekijänä.

Toinen tuloksien perusteella muodostettu tietoturvakäytänneluokka on tietoturvateknologiat, joka sisältää VPN-yhteyden käytön, kaksivaiheisen tunnistautumisen ja salatun sähköpostin käytön tietoturvakäytänteet. Kuusi haastateltavaa viidestätoista koki tietoturvateknologioiden käytön stressaavaksi. VPN-yhteyttä käytetään usein organisaatioissa suojatun yhteyden muodostamiseksi organisaation sisäverkkoon, järjestelmiin ja laitteisiin, ja VPN-yhteydellä voidaan myös mahdollistaa työnteko etänä, kun työntekijän tietokone ei ole yhdistettynä organisaation verkkoon. Haastateltavat kokivat VPN-yhteyden käytön stressaavaksi useista syistä. Se hidastaa työntekoa, aiheuttaa teknisiä ongelmia sekä sitä koskevat ohjeistukset koetaan epäselviksi. Esimerkiksi H2 kertoi VPN-yhteyden käytön aiheuttavan häiriöitä muihin järjestelmiin, joka aiheuttaa epäluottamusta sen toimintaa kohtaan. Häiriöt myös lisäävät työmäärää, sillä järjestelmiä joudutaan käynnistämään uudestaan. H9 puolestaan kertoi, ettei heidän organisaatiossaan ole selviä ohjeistuksia siitä, mihin järjestelmiin VPN-yhteyttä tarvitaan ja mihin ei. VPN-yhteyden käytöstä aiheutuva työnteon hidastuminen ja tekniset ongelmat viittaavat turvallisuusstressin ylikuormitukseen, kun taas H9 kertomat epäselvät ohjeistukset vastaavat turvallisuusstressin monimutkaisuuden stressitekijää. Kaksivaiheisen tunnistautumisen osalta koettu stressaavuus liittyi vain ylikuormitukseen, eli lisääntyneeseen työmäärään tai työnteon hidastumiseen. Useat haastateltavat kokivat kaksivaiheisen tunnistautumisen aikaa vievänä, varsinkin jos he joutuvat tekemään kaksivaiheisen tunnistautumisen moneen kertaan kiireiseinä työpäivänä. H13 koki mielestään todella korkeaa turvallisuusstressiä kaksivaiheisen tunnistautumisen aiheuttamasta ylikuormituksesta ja hän stressasi asiaa jopa ennen itse kaksivaiheisen tunnistautumisen käyttöä, sillä se pysäyttää hänen työntekonsa pitkäksi aikaa epäonnistuessaan. Viimeiseinä tietoturvateknologioihin liittyvä esille tullut stressaava tietoturvakäytänne oli salatun sähköpostin käyttäminen. Se aiheutti haastateltaville turvallisuusstressiä sekä ylikuormituksen että monimutkaisuuden muodossa. Salatun sähköpostin käyttö koettiin aikaa vieväksi ja H13:n mielestä siihen liittyvät ohjeistukset epäselviksi.

Arkaluonteisen tiedon käsittelyn koki stressaavaksi kuusi haastateltavaa viidestätoista. Arkaluonteisen tiedon käsittelyllä tarkoitetaan organisaation

sisäisen tai salaisen tiedon, kuten asiakasdatan käsittelyä, tallennusta ja sen kommunikointia. Tiedon käsittely koettiin stressaavaksi tietoturvakäytänteiden puutteellisuuden tai niiden epäselvyyden takia, joka aiheutti haastateltavissa epävarmuuden tunnetta tai tiedon vuotamisen pelkoa. Esimerkiksi H14 kertoi, ettei heidän organisaatiossaan ole koulutettu kovinkaan selkeästi tai tarkasti tiedon käsittelyyn liittyviä tietoturvakäytänteitä, jonka vuoksi hän joutuu usein toimimaan ilman ohjeistuksia, jonka hän kokee stressaavana. H13 mukaan stressaavuus puolestaan johtui tietoturvakäytänteiden epäselvyydestä niiden sisältämän vaikeaselkoisen IT-alan ammattisanaston vuoksi. Tiedon käsittelyn tietoturvakäytänteiden stressaavuuden stressitekijänä on siis ainoastaan monimutkaisuus.

Viimeiseinä tietoturvakäytänneluokkana on laite- ja USB-käytänteet, jotka kokivat stressaavaksi viisi haastateltavaa. Luokan ensimmäisen tietoturvakäytänteen tietokoneen lukitsemisen stressitekijänä oli ainoastaan ylikuormitus, sillä laitteet lukittautuivat joko liian nopeasti tai organisaation tietoturvakäytänteet velvoittavat lukitsemaan tietokoneen aina sen äänreltä poistuessa, joidenka takia tapahtuva toistuva lukitseminen ja sisäänkirjautuminen koettiin aikaa vieväksi. Myös käyttöoikeuksien hakemisen stressitekijänä oli ylikuormitus, sillä hakuprosessi koettiin liian pitkäkestoiseksi. USB-käytänteiden stressitekijänä puolestaan oli monimutkaisuus, sillä niitä koskevat tietoturvakäytänteet koettiin epäselviksi. H11 kertoi olevansa epätietoinen siitä, missä määrin organisaation tietokonetta voi käyttää omiin tarkoituksiin ja voiko hän esimerkiksi siirtää tiedostoja puhelimeensa tietokoneen USB-portin kautta.

Tutkielman tuloksien perusteella suomalaiset IT-alan työntekijät kokevat turvallisuusstressiä salasanojen, tietoturvateknologioiden, tiedon tietoturvan ja laitekäytänteiden tietoturvakäytänteistä. Turvallisuusstressin muodostumisen puolestaan aiheuttaa ylikuormitukseen ja monimutkaisuuteen liittyvät stressitekijät. Tietoturvakäytänteistä ja niiden noudattamisesta aiheutuva turvallisuusstressi vaikuttaa tuloksien perusteella liittyvän pääosin ylikuormitukseen, sillä ylikuormitus oli turvallisuusstressin stressitekijänä suurimmassa osassa haastateltavien stressaavaksi kokemien tietoturvakäytänteiden stressaavuuden syynä. Ylikuormituksella tarkoitetaan ylimääräisen työajan käyttämiseen tietoturvakäytänteiden noudattamiseen, tai työnteon hidastumiseen tai estymiseen (D'Arcy ym., 2014). Havainto on linjassa aikaisempaan turvallisuusstressitutkimukseen, sillä ylikuormituksen on useasti todettu olevan yksi eniten turvallisuusstressiä aiheuttava stressitekijä (Lee ym., 2016; Pham ym., 2019). Lee ym. (2016) havaitsivat ylikuormituksen olevan turvallisuusstressin pääasiallinen aiheuttaja teknisiä työtehtäviä tekevien työntekijöiden keskuudessa, joiden organisaatiossa tietoturvakäytänteiden noudattamista valvontaan tarkasti. Tässä tutkielmassa haastateltavat olivat Leen ym. (2016) tutkimuksen lailla teknisiä työtehtäviä tekeviä IT-alan työntekijöitä, joten ylikuormituksen toteamista pääasialliseksi turvallisuusstressin stressitekijäksi voidaan pitää ainakin jokseenkin luotettavana tuloksena. Myös Phamin ym. (2019) tutkimuksessa todettiin ylikuormituksen olevan turvallisuusstressin pääasiallinen aiheuttaja, joka johtuu vaikeasta pääsystä tietoturvakäytänteisiin. Työntekijät joutuvat käyttämään ylimääräistä aikaa tietoturvakäytänteiden tarkasteluun pääsemiseen, jotta he voisivat toimia niiden

velvoittamalla tavalla (Pham ym., 2019). Lisäksi myös Nasirpouri Shadbadin ja Biroksen (2022) tutkimuksen mukaan turvallisuusstressi voi aiheuttaa työntekijässä uupumusta tai väsymystä, mikäli tietoturvakäytänteiden noudattaminen koetaan liian työlääksi tai aikaa vieväksi. Uupumus ja väsymys yhdistyvät suoraan D'Arcyn ym. (2014) turvallisuusstressin ylikuormituksen stressitekijään. Haastateltavat kokivat siis esille tulleiden tietoturvakäytänteiden olevan liian aikaa vieviä tai heidän työaikaansa vähentäviä, joka aiheuttaa heille erityisesti kiireiden keskellä turvallisuusstressiä turhaantumisen tai työläyden vuoksi.

Ylikuormituksen lisäksi myös monimutkaisuuden havaittiin olevan turvallisuusstressiä aiheuttava stressitekijä. Monimutkaisuuden stressitekijällä tarkoitetaan tietoturvakäytänteiden hankalaa ymmärrettyyttä, vaikeaselkoisuutta tai käytänteiden prosessien monimutkaisuutta (D'Arcy ym., 2014). Noin joka kolmannen tietoturvakäytänteen stressitekijänä oli monimutkaisuus. Monimutkaisuudesta aiheutuvaa turvallisuusstressiä havaittiin eniten tiedon tietoturvakäytänteiden noudattamisessa, mutta myös salasanavaatimuksissa ja USB- ja laitekäytännöissä. Haastateltavat siis kokevat arkaluonteiseen tietoon liittyvät tietoturvakäytänteet, salasanojen vaatimukset sekä organisaation tarjoamien laitteiden tietoturvakäytänteet vaikeaselkoisiksi, joka aiheuttaa haasteita tietoturvallisen toimintatavan omaksumisessa.

Turvallisuusstressin kolmatta stressitekijää, eli epävarmuutta, eivät haastateltavat kokeneet tuloksien pohjalta stressaavaksi. Turvallisuusstressin epävarmuudella tarkoitetaan usein tapahtuvaa uusien tietoturvakäytänteiden käyttöönottoa tai nykyisten muutoksia, jolloin työntekijät joutuvat usein omaksumaan uusia tietoturvakäytänteitä (D'Arcy ym., 2014). Se voi tarkoittaa, etteivät haastateltavat koe uusien tietoturvakäytänteiden omaksumista tai niiden usein tapahtuvaa muuttumista stressaavaksi. Suurin osa haastateltavista kertoi haastattelun taustatietokysymyksissä ymmärtävänsä organisaationsa tietoturvakäytänteet ja niiden merkityksen hyvin, jonka vuoksi uusien tietoturvakäytänteiden noudattamaan alkaminen ei ole haastateltaville haasteellista. Epävarmuuden stressitekijän puuttuminen tuloksista voi myös johtua haastateltavien suhteellisen lyhyestä työkokemuksista nykyisissä tehtävissään. Noin puolet haastateltavista on työskennellyt nykyisissä tehtävissään alle vuoden, joten tietoturvakäytänteet eivät siis välttämättä ole muuttuneet tai lisääntyneet heidän työsuhteensa aikana, jolloin niiden muuttumisesta aiheutuvaa epävarmuuttakaan ei pysty syntymään.

Tuloksista voidaan myös tehdä havaintoja haastateltavien tietoturvakäyttäytymisen muuttumisesta. Usea haastateltava kertoi muuttuneensa aikaisempaa varovaisemmaksi tai tarkkaavaisemmaksi tietoturvakäytänteisiin tutustumisen jälkeen ja niiden noudattamisen aikana nykyisissä työtehtävissään. Tuloksista voidaan havaita kaksi muutosta Karjalaisen ym. (2020) tietoturvakäyttäytymisen tasomallia hyödyntäen. Näistä ensimmäinen on tietoturvakäyttäytymiseen liittyvän ajattelun siirtyminen ensimmäiseltä eli intuitiiviselta tasolta deklaratiiviselle tasolle. Esimerkiksi H12 ja H14 kertoivat nykyään tarkistavansa tietoturvakäytänteiden mukaisen toimintatavan ennen jonkin asian suorittamista. Karjalaisen ym. (2020) mukaan intuitiivisen tason ajattelulla tarkoitetaan, että

työntekijät ovat yleensä tiedottomasti osaamattomia tietoturva-asioissa, ja tekevät tietoturvakäyttäytymiseen liittyvät päätökset intuitiivisesti. Deklaratiivinen tietoturvakäyttäytymisen ajattelun taso puolestaan tarkoittaa, että työntekijät ovat kykeneväisiä muuttamaan tietoturvakäyttäytymistään opetettujen asioiden pohjalta, mutta pystyvät myös rikkomaan niitä tietoisesti. Tämä voi ilmetä vaikkapa niin, että työntekijät noudattavat salasanakäytänteiden salasanavaatimuksia luomalla vaatimusten mukaiset salasanat, mutta tasosta riippumaton syrjäyttävä ajattelu saa työntekijät oikomaan käytänteiden noudattamisesta ja käyttämään samaa salasanaa tietoturvakäytänteiden vastaisesti useassa eri järjestelmässä. (Karjalainen ym., 2020.) Haastateltavat, joiden havaittiin olevan deklaratiivisella tasolla, pitivät tietoturvakäytänteitä turhauttavina ja saattoivat tehdä vastaavanlaisia oikomisia tietoturvakäyttäytymisessään.

Toisena havaittuna muutoksena on ajattelun tason siirtyminen deklaratiiviselta tasolta kolmannelle tasolle, eli toiminta-ajattelun tasolle. Esimerkiksi H3 pystyi arvioimaan tietoturvakäyttäytymisestään aiheutuvia riskejä ja siten toimimaan tietoturvakäytänteiden mukaisesti. Toiminta-ajattelun tasolla on tyypillistä, että työntekijä ymmärtää tietoturvakäytänteiden merkityksen hänelle relevantissa organisaatiokontekstissa (Karjalainen ym., 2020), jonka vuoksi tasomallin kolmannella tasolla olevat haastateltavat kertoivat kokevansa vain lievää turvallisuusstressiä tietoturvakäytänteistä. Koetun turvallisuusstressin määrään vaikuttaa myös olennaisesti minäpystyvyys IT-asioissa, jonka esimerkiksi Hooper ja Blunt (2020) havaitsivat olevan yksi merkittävimmistä tietoturvakäytänteiden noudattamisen ennustajista. Koska jokainen haastateltava kertoi kokevansa ainakin jonkin asteista turvallisuusstressiä, ei tutkielman perustella voida sanoa, että joku haastateltava olisi rutiiniajattelun tasolla. Karjalaisen ym. (2020) mukaan rutiinitasolla olevan henkilön tietoturvakäytänteiden noudattaminen ei vaadi henkilöltä enää suurta kognitiivista työmäärää, eli tietoturvakäytänteitä pystytään noudattamaan rutiininomaisesti.

8.2 Kontribuutiot tutkimukselle ja käytännölle

Tutkielmasta voidaan havaita useita kontribuutioita sekä alan tutkimukselle että käytännölle. Turvallisuusstressin tutkimus on, kuten myös aikaisemmin mainittu, vielä suhteellisen aluillaan, eikä aikaisempaa tutkimuskirjallisuutta ole runsaasti. Vaikka turvallisuusstressin olemassaolo on jo osoitettu useissa eri tutkimuksissa, tämäkin tutkielma vahvisti turvallisuusstressin olemassaolon. Suomalaiset IT-alan työntekijät kokevat turvallisuusstressiä henkilöstä riippuen eri vahvuisena. Tutkielma myös kohdistettiin nimenomaan IT-alan työntekijöihin, sillä aikaisemmassa turvallisuusstressi- tai tietoturvakäyttäytymistutkimuksessa tutkimuskohteena on ollut lähes aina jokin muu ammattiala, kuin IT-ala. Aikaisemmassa turvallisuusstressitutkimuksessa ei myöskään ole tutkittu, millaiset tietoturvakäytänteet työntekijät ylipäätään kokevat stressaaviksi. Tämä tutkimus pyrki täyttämään näitä tutkimusaukkoja selvittämällä, millaiset tietoturvakäytänteet aiheuttavat IT-alan työntekijöille turvallisuusstressiä. Tutkielman

tuloksien mukaan IT-alan työntekijät kokevat salasanakäytänteet, tietoturvateknologiat, tiedon tietoturvakäytänteet ja laitekäytänteet stressaavaksi. Näiden tietoturvakäytänteiden stressaavuuden syynä on ylikuormitus ja monimutkaisuus, eli tietoturvakäytänteet lisäävät työntekijöiden työmäärää, vähentävät työtehtäviin käytettävissä olevaa aikaa, tai ne koetaan vaikeaselkoisina ja monimutkaisina. Tutkielmassa ei havaittu, että turvallisuusstressiä aiheutuisi epävarmuuden stressitekijän takia, eli tietoturvakäytänteiden muuttumisesta aiheutuvan epävarmuuden takia.

Tutkielmalla on teoreettisten kontribuutioiden lisäksi useita käytännön hyötyjä sekä organisaatioille että työntekijöille. Ensiksikin organisaatiot pystyvät hyödyntämään tutkielman tuloksia tietoturvakäytänteiden kehittämisessä, sillä tutkielman tulokset paljastavat IT-alan työntekijöitä stressaavat tietoturvakäytänteet. Stressaavien tietoturvakäytänteiden kehittäminen vähemmän stressaavaksi on tärkeää, sillä etenkin ylikuormituksesta aiheutuva turvallisuusstressi voi johtaa työntekijät helposti rikkomaan tietoturvakäytänteitä, joka voi olla organisaatioille hyvinkin vahingollista. Kuten D'arcy ym. (2014) myös totesivat tutkimuksessaan, ylikuormituksen nouseminen henkilökohtaisen resilienssin yläpuolelle voi aiheuttaa tietoturvakäytänteiden rikkomista tai noudattamatta jättämistä, vaikka henkilö tietäisikin tekevänsä väärin. Toisin sanoen, vaikka työntekijöiden tietoturvaosaaminen olisi riittävällä tasolla, voi tietoturvakäytänteistä aiheutuva ylikuormitus silti johtaa tietoturvakäytänteiden rikkomiseen. Tietoturvakäytänteistä aiheutuva ylikuormitus tai niiden monimutkaisuus voi lisäksi aiheuttaa työntekijöissä turhautuneisuuden tunteita, jotka voivat johtaa myös herkästi tietoturvakäytänteiden todelliseen rikkomiseen. (D'Arcy & Teh, 2019).

Turvallisuusstressillä voi siis olla haittavaikutuksia, joihin lukeutuvat muun muassa turhautuminen, tietoturvakäytänteiden rikkominen tai noudattamatta jättäminen, väsymys ja työtehokkuuden laskeminen. Tietoturvakäytänteitä pitäisi myös suunnitella työntekijälähtöisesti esimerkiksi osallistamalla työntekijät niiden suunnitteluun, jolloin niiden käytännön toteutus olisi työntekijäystävällisempi. Tietoturvakäytänteiden merkityksen ymmärtämisellä sekä vahvalla koetulla minäpystyvyydellä on tietoturvakäyttäytymistä parantavia vaikutuksia (Hooper & Blunt, 2020; Karjalainen ym., 2020), jotka alleviivaavat tietoturvakoulutuksien tärkeyttä organisaatioissa, sillä parempi tietoturvaosaaminen ja minäpystyvyys voi myös vähentää koettua turvallisuusstressiä tietoturvakäytänteistä.

Tutkimuksen tulokset avaavat hyötyjä myös organisaatioiden työntekijöille. Tuloksien avulla työntekijät voivat ensiksikin tunnistaa, kokevatko he tällä hetkellä turvallisuusstressiä ja jos kokevat, niin millaisista tietoturvakäytänteistä. Stressaavien tietoturvakäytänteiden tunnistaminen voi olla ensimmäinen askel turvallisuusstressin vähentämisessä. Turvallisuusstressin kokemisen ymmärtämisellä voi myös olla vaikutuksia tietoturvakäytänteiden noudattamiseen.

8.3 Tutkimuksen rajoitteet ja jatkotutkimusaiheet

Tutkimuksella on muutamia rajoitteita, jotka myös avaavat mielenkiintoisia jatkotutkimusaiheita. Yhtenä rajoitteena voidaan pitää haastateltavien suhteellisen pientä lukumäärää, jonka vuoksi tutkimuksen tulokset eivät ole välttämättä yleistettävissä. Haastateltavien valinta rajattiin suomalaisiin IT-alan työntekijöihin, joten tutkielman tulokset eivät myöskään välttämättä ole yleistettävissä muihin ammattialoihin. Toisaalta tutkimus haluttiin kohdistaa nimenomaan IT-alan työntekijöihin sen vuoksi, ettei tietoturvakäyttäytymistä tai turvallisuusstressiä ole aikaisemmin muutamia poikkeuksia lukuun ottamatta tutkittu IT-alan näkökulmasta. Ensimmäisenä jatkotutkimusaiheena olisikin siis sekä kasvattaa tutkittavien haastateltavien lukumäärää että laajentaa tutkimuksen kohteena käytettyä ammattiryhmää IT-alan ulkopuolelle, sillä varsinkin turvallisuusstressi kaipaisi lisää tutkimustietoa eri konteksteista ja tilanteista.

Toinen tutkielman rajoite ja jatkotutkimusaihe liittyy aineistonkeräämiseen. Tutkielman aineistonkeruumenetelmänä toimi haastattelut, joissa tutkittavat kertoivat omia kokemuksiaan ja mielipiteitään tietoturvakäytänteiden stressaavuudesta. Haastatteluissa ei pyritty kertomaan turvallisuusstressin syntytapaa ja teoriaa kovin kattavasti, sillä se olisi voinut rajata tai ankkuroida haastateltavien vastauksia. Tutkielmassa haluttiin nimenomaan esitellä tietoturvakäytänteiden stressaavuus haastateltaville ilmiönä ja antaa sitten haastateltavien itse määritellä, millaiset tietoturvakäytänteet he kokevat itse stressaavia. Tämän vuoksi on mahdollista, että haastateltavat ovat kokeneet stressaavuuden eri tavalla, jolloin osa haastateltavista tuo ilmi kaikki vähänkin negatiivisia tunteita aiheuttavat asiat tietoturvakäytänteistä, kun taas osa kertoo vain hyvin vahvasti mielestään stressaavista tietoturvakäytänteistä. Haastatteluissa pyrittiin tuomaan haastateltaville ilmi, että tietoturvakäytänteiden stressaavuus tunnereaktiona voi tarkoittaa negatiivisia tunteita, kuten esimerkiksi turhaantumista tai väsymystä. Tästä rajoitteesta avautuu tutkielman toinen jatkotutkimusaihe, joka on turvallisuusstressin kokemisen mittaaminen eri tavalla, kuin yksilöhaastatteluilla. Olisi mielenkiintoista saada tietää, millaisia tuloksia esimerkiksi ryhmähaastattelut tuottaisivat, joissa haastateltavat pystyisivät keskustelemaan myös keskenään tietoturvakäytänteiden stressaavuudesta ja niiden syistä.

Viimeiseinä jatkotutkimusaiheena on turvallisuusstressin muuttumisen tarkastelu pidemmällä aikavälillä. Vaikkakin tietoturvakäyttäytymisen muuttumista ajan kanssa on tutkittu esimerkiksi Karjalaisen ym. (2019) ja Karjalaisen ym. (2020) toimesta, turvallisuusstressin muuttumista on tutkittu hyvin niukasti. Tulevaisuuden tutkimukset voisivat perehtyä turvallisuusstressin muuttumiseen esimerkiksi tietoturvakoulutuksien vaikutuksesta juuri Karjalaisen ym. (2020) tietoturvakäyttäytymisen tasomalliin pohjaten.

9 YHTEENVETO

Huolellisesti suunnitellut, käyttöönotetut ja valvotut tietoturvakäytänteet ovat organisaatioiden yksi tärkeimmistä tietoturvaa edistävistä tekijöistä. Ne ohjaavat yrityksen henkilöstön tietoturvakäyttäytymistä, pienentävät tietoturvariskien mahdollisuuksia ja muodostavat organisaatioiden sisäisen tietoturvakulttuurin perustan (Paananen ym., 2020). Tietoturvakäytänteet sekä niiden noudattaminen voidaan kuitenkin kokea stressaavaksi, joka voi aiheuttaa niiden rikkomista tai noudattamatta jättämistä. Tätä tietoturvakäytänteistä ja niiden noudattamisesta aiheutuvaa kuormitusta kutsutaan turvallisuusstressiksi. Tutkielmassa haluttiin saada selville, millaiset tietoturvakäytänteet organisaatioiden työntekijät kokevat stressaaviksi, eli millaiset tietoturvakäytänteet aiheuttavat turvallisuusstressiä. Tämän lisäksi haluttiin selvittää, miksi ensimmäisen tutkimuskysymyksen tietoturvakäytänteet ovat stressaavia. Tutkielman tutkimuskysymyksiksi siis muodostui *"Millaiset tietoturvakäytänteet työntekijät kokevat stressaaviksi?"* ja *"Miksi ensimmäisen tutkimuskysymyksen tietoturvakäytänteet ovat stressaavia?"*.

Tutkielma alkoi kirjallisuuskatsauksella, jossa tutustuttiin tutkielman tutkimusaiheen kannalta kolmeen olennaiseen aihealueeseen, eli tietoturvaan ja tietoturvakäytänteisiin, tietoturvakäyttäytymiseen ja sen muuttumiseen, sekä turvallisuusstressin aiempaan tutkimukseen. Ensimmäisessä teorialuvussa tarkasteltiin ensin tietoturvan määritelmää, jonka jälkeen tutustuttiin tietoturvakäytänteisiin. Tietoturvakäytänteet voivat olla korkean tason, matalan tason tai metatason tietoturvakäytänteitä, joista etenkin metatason käytänteet ovat yleistymässä. Metatason käytänteet ovat tietoturvakäytänteiden kehittämiseen liittyviä tietoturvakäytänteitä. Luvussa tutustuttiin myös erilaisiin tietoturvakäytänteiden kehitysmetodeihin, kuten jatkuvan kehittämisen PFIRES-malliin. Kolmannessa pääluvussa tarkasteltiin organisaatiokontekstin tietoturvakäyttäytymistä, tutustuttiin siihen vaikuttaviin tekijöihin sekä selvitettiin tietoturvakäytänteiden muuttumiseen liittyviä asioita. Tietoturvakäyttäytymiseen vaikuttavia tekijöitä kuvaa hyvin esimerkiksi Moodyn ym. (2018) esittelemä tietoturvakäyttäytymisen yhtenäismalli, joka kuvaa työntekijöiden tiettyyn tietoturvakäyttäytymiseen johtavia tekijöitä. Luvussa myös tutustuttiin tietoturvakäyttäytymisen muuttumiseen liittyviin tutkimuksiin, joista dynaamisuutta kuvaa loistavasti Karjalaisen ym. (2019)

dialektinen prosessimalli ja Karjalaisen ym. (2020) tasomalli. Viimeisessä teorialuvussa tarkasteltiin ensin, miten D'Arcy ym. (2014) aloittivat turvallisuusstressin tutkimuksen johtamalla ilmiön teknostressin käsitteen pohjalta. Luvussa myös tarkasteltiin turvallisuusstressin tutkimuksessa hyödynnettyihin teorioihin sekä tutkimusaiheen aiempaan tutkimukseen.

Tutkielman empiirinen osuus toteutettiin laadullisena tutkimuksena. Aineistonkeruumenetelmänä käytettiin teemahaastatteluja, joista osa pidettiin etänä ja osa kasvokkain. Haastatteluita toteutettiin yhteensä 15 kappaletta eri organisaatioiden IT-alan työntekijöiden kanssa. Kerätyn aineiston litteroinnin jälkeen aineiston analysointimenetelmäksi puolestaan valikoitui teemoittelu, jossa esille tulleita kokonaisuuksia luokiteltiin teemoiksi.

Tutkimuksen tuloksien mukaan työntekijät kokevat salasanakäytänteet, tietoturvateknologioiden käytön, arkaluonteisen tiedon käsittelyn sekä laitekäytänteet stressaaviksi tietoturvakäytänteiksi. Tietoturvakäytänteiden stressaavuuden syynä on ylivoimaisesti turvallisuusstressin stressitekijä ylikuormitus, jonka on myös aikaisemmissa tutkimuksissa havaittu olevan turvallisuusstressin aiheutumisen pääsyy. Ylikuormitus ilmenee tietoturvakäytänteiden noudattamiseen menevänä ylimääräisenä ajankäyttönä, joka on pois työntekijöiden muihin työtehtäviin käytettävissä olevasta ajasta. Tietoturvakäytänteiden noudattamisen aiheuttama lisääntynyt työmäärä ja työtehtäviin käytettävissä olevan ajan vähentyminen aiheuttaa työntekijöille stressiä etenkin kiireisinä työpäivinä. Turvallisuusstressi voi myös tuloksien mukaan ilmetä monimutkaisuutena salasanavaatimuksien, epäselvien tiedon tietoturvakäytänteiden ja laitekäytänteiden takia. Työntekijät eivät ole aina ajan tasalla organisaation salasanavaatimuksista, jolloin niitä joudutaan kertamaan uuden salasanan luomisen yhteydessä. Monimutkaisuutta esiintyy lisäksi arkaluonteisen tiedon käsittelyssä, jolloin tietoturvakäytänteet esimerkiksi tiedon kommunikoinnin ja tallentamisen osalta koetaan vaikeaselkoisiksi. Myös USB- ja laitekäytänteet koetaan osittain monimutkaisiksi, mikä aiheuttaa turvallisuusstressiä.

Tutkimuksen tuloksia voidaan hyödyntää organisaatioissa tietoturvakäytänteiden kehitykseen, turvallisuusstressin parempaan huomioimiseen ja sen vähentämiseen organisaatiossa. Tuloksista on hyötyä myös työntekijöille turvallisuusstressin tunnistamisen ja henkilökohtaisten vähentämismetodien löytämisessä. Tutkielman suhteellisen alhainen haastateltavien lukumäärä ja aineistonkeruumenetelmän rajoitteet voivat rajoittaa tutkielman tuloksien yleistettävyyttä, jonka vuoksi jatkotutkimusten tulisi ottaa nämä huomioon.

LÄHTEET

Bandura, A., Barbaranelli, C., Caprara, G. V. & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. *Journal of Personality and Social Psychology, 71(2),* 364–374. https://doi.org/10.1037/0022-3514.71.2.364

Baskerville, R. & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15(5/6),* 337 – 346. https://doi.org/10.1108/09576050210447019

Bibble, B. J. (1986). Recent Development in Role Theory. *Annual Review of Sociology, 12*, 67–92.

Brod, C. (1984). *Technostress: The human cost of the computer revolution*. Addison-Wesley.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34(3),* 523-A7. https://doi.org/10.2307/25750690

Cabrera, J. S., Reyes, A. R. L. & Lasco, C. A. (2020). Multicriteria Decision Analysis on Information Security Policy: A Prioritization Approach. *Advances in Technology Innovation, 6(1),* 31–38.

Calder, A., Watkins, S. G. & Watkins, S. (2019). *Information Security Risk Management for ISO 27001/ISO 27002, third edition*. IT Governance Ltd.

Chen, L., Zhen, J., Dong, K. & Xie, Z. (2020). Effects of Sanction on the Mentality of Information Security Policy Compliance. *Revista Argentina de Clínica Psicológica, 29(1)*, 39–49. http://dx.doi.org.ezproxy.jyu.fi/10.24205/03276716.2020.6

Cheng, L., Li, Y., Li, W., Holm, E. & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*, 447–459. https://doi.org/10.1016/j.cose.2013.09.009

D'Arcy, J. & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22(5)*, 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

D'Arcy, J., Herath, T. & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31(2),* 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., Herath, T., Yim, M.-S., Nam, K. & Rao, H. R. (2018). Employee Moral Disengagement in Response to Stressful Information Security

Requirements: A Methodological Replication of a Coping-Based Model. *AIS Transactions on Replication Research, 4(8),* 1–18. http://dx.doi.org/10.17705/1atrr.00028

D'Arcy, J. & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management, 56(7),* 103–151. https://doi.org/10.1016/j.im.2019.02.006

Doherty, N. F. & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People, 31(2),* 348–367. https://doi.org/10.1108/ITP-08-2016-0194

Han, J., Kim, Y. J. & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 66,* 52–65. https://doi.org/10.1016/j.cose.2016.12.016

Hirsjärvi, S. & Hurme, H. (2008). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö.* Gaudeamus.

Ho-Jin, P. & Cho, J.-S. (2016). The influence of information security technostress on the job satisfaction of employees. *Journal of Business and Retail Management Research, 11(1)*, 66–75.

Hooper, V. & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology, 39(8),* 862–874. https://doi.org/10.1080/0144929X.2019.1623322

Hu, Q., Dinev, T., Hart, P. & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences, 43(4)*, 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Hwang, I. & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81*, 282–293. https://doi.org/10.1016/j.chb.2017.12.022

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Information security controls* (ISO/IEC Standard No. 27002). Haettu osoitteesta https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

International Organization for Standardization. (2013). *Information technology – Security techniques – Information security management systems – Requirements* (ISO/IEC Standard No. 27001). Haettu osoitteesta https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Johnston, A. C. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34(3),* 549–566. https://doi.org/10.2307/25750691

Kajtazi, M., Cavusoglu, H., Benbasat, I. & Haftor, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information & Computer Security, 26(2),* 171–193. https://doi.org/10.1108/ICS-09-2017-0066

Karjalainen, M., Sarker, S. & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research, 30(2),* 687–704. https://doi.org/10.1287/isre.2018.0827

Karjalainen, M., Siponen, M. & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security, 93*, 101782–18. https://doi.org/10.1016/j.cose.2020.101782

Kim, S. H., Yang, K. H. & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal, 2014*, 1–12. https://doi.org/10.1155/2014/463870

Klockars, C. (1974). *The Professional Fence*. New York: Free Press.

Koohang, A., Nowak, A., Paliszkiewicz, J. & Nord, J. H. (2020). Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. *Journal of Computer Information Systems, 60(1),* 1–8. https://doi.org/10.1080/08874417.2019.1668738

Lazarus, R. S. (1991). Progress on a cognitive-motivational-relational theory of emotion. *American Psychologist, 46(8),* 819–834. https://doi.org/10.1037/0003-066X.46.8.819

Lazarus, R. S. & Folkman, S. (1984). *Stress, appraisal, and coping.* (11. uud. painos) New York, Springer.

Lee, C., Lee, C. C. & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59,* 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Li, Y., Zhang, N. & Siponen, M. (2019). Keeping secure to the end: A long-term perspective to understand employees' consequence-delayed information security violation. *Behaviour & Information Technology, 38(5),* 435–453. https://doi.org/10.1080/0144929X.2018.1539519

Merhi, M. I. & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior, 92,* 37–46. https://doi.org/10.1016/j.chb.2018.10.031

Minor, W. (1981). Techniques of Neutralization: A Reconceptualization and Empirical Examination. *Journal of Research in Crime and Delinquency, 18(2),* 295–318.

Moody, G. D., Siponen, M. & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42(1),* 285-A22.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18(2),* 126–139. https://doi.org/10.1057/ejis.2009.10

Nasirpouri Shadbad, F. & Biros, D. (2021). Understanding Employee Information Security Policy Compliance from Role Theory Perspective. *Journal of Computer Information Systems, 61(6),* 571–580. https://doi.org/10.1080/08874417.2020.1845584

Nasirpouri Shadbad, F. & Biros, D. (2022). Technostress and its influence on employee information security policy compliance. *Information Technology & People, 35(1),* 119–141. https://doi.org/10.1108/ITP-09-2020-0610

Paananen, H., Lapke, M. & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security, 88*, 101608. https://doi.org/10.1016/j.cose.2019.101608

Pham, H. C., Brennan, L. & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications, 46,* 96–107. https://doi.org/10.1016/j.jisa.2019.03.012

Puusa, A., Juuti, P. & Aaltio, I. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät.* Helsinki: Gaudeamus.

Raggad, B. G. (2010). *Information Security Management: Concepts and Practice*. Boca Raton: Taylor & Francis Group.

Rajab, M. & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security, 80,* 211–223. https://doi.org/10.1016/j.cose.2018.09.016

Rao, F. A., Dominic, P. D. D., Ali, S. E. A., Rehman, M. & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences, 11(8),* 1–38. http://dx.doi.org.ezproxy.jyu.fi/10.3390/app11083383

Rees, J., Bandyopadhyay, S. & Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM, 46(7),* 101–106. https://doi.org/10.1145/792704.792706

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Sharma, S. & Warkentin, M. (2019). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security, 87,* 101397. https://doi.org/10.1016/j.cose.2018.09.005

Siponen, M., Adam Mahmood, M. & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51(2),* 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M. & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34(3),* 487-A12. https://doi.org/10.2307/25750688

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48(7),* 296–302. https://doi.org/10.1016/j.im.2011.07.002

Sykes, G. M. & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review, 22(6),* 664–670. https://doi.org/10.2307/2089195

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S. & Ragu-Nathan, T. S. (2007). The Impact of Technostress on Role Stress and Productivity. *Journal of Management Information Systems, 24(1),* 301–328. https://doi.org/10.2753/MIS0742-1222240109

Tsohou, A., Siponen, M. & Newman, M. (2020). How does information technology-based service degradation influence consumers' use of services? An information technology-based service degradation decision theory. *Journal of Information Technology, 35(1),* 2–24. https://doi.org/10.1177/0268396219856019

Ward, P. & Smith, C. L. (2002). The Development of Access Control Policies for Information Technology Systems. *Computers & Security, 21(4),* 356–371. https://doi.org/10.1016/S0167-4048(02)00414-5

Weiss, H. & Cropanzano, R. (1996). Affective events theory: A theoretical discussion of the structure, causes and consequences of affective experiences at work. *Research in Organizational Behavior, 18,* 1–74.

Willison, R., Warkentin, M. & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, 28(2),* 266–293. https://doi.org/10.1111/isj.12129

LIITE 1 HAASTATTELURUNKO

Tutkimuskysymykset

1. *Millaiset tietoturvakäytänteet koetaan stressaaviksi?*
2. *Miksi ensimmäisen tutkimuskysymyksen tietoturvakäytänteet koetaan stressaaviksi?*

Yleiset taustakysymykset

- Ikä?
- Sukupuoli?
- Koulutustaso?
- Työkokemus vuosissa nykyisissä tehtävissä?

Taustakysymykset tietoturvakäytänteistä

- Oletko tutustunut organisaatiosi tietoturvakäytänteisiin?
- Oletko osallistunut organisaatiosi järjestämään tietoturvakoulutukseen?
- Kuinka hyvin arvioisit ymmärtäväsi organisaatiosi tietoturvakäytänteet? (Erittäin huono 1–2–3–4–5 Erittäin hyvä)

Turvallisuusstressi

- Millaisia ajatuksia ja tunteita tietoturvakäytänteet herättävät sinussa?
- Millaisissa tilanteissa olet kokenut stressiä tietoturvakäytänteistä tai niiden noudattamisesta?
- Millaiset tietoturvakäytänteet koet turhauttaviksi?
- Millaiset tietoturvakäytänteet ovat mielestäsi stressaavia?
- Miksi mainitsemasi tietoturvakäytänne on mielestäsi stressaava?
- Miten hyvin mielestäsi tietoturvakäytänteistä kommunikoidaan organisaatiossasi?

Turvallisuusstressin kirjallisuuteen pohjautuvia apukysymyksiä (D'Arcy ym., 2014)

- Miten tietoturvakäytänteet vaikuttavat työmääräsi?
- Millaisia vaikutuksia tietoturvakäytänteillä on työskentelytapoihisi ja -tottumuksiisi?
- Koetko tietoturvakäytänteet helpoiksi ymmärtää?
- Ovatko tietoturvakäytänteet mielestäsi monimutkaisia?
- Kuinka paljon aikaa tietoturvakäytänteiden opettelu vie aikaa sinulta?
- Ottaako organisaatiosi käyttöön uusia tietoturvakäytänteitä usein?
- Muuttuvatko tietoturvakäytänteet organisaatiossasi usein?