Tietoturvakäyttäytymiseen vaikuttavat tekijät

Laura Mainio

2021 Laurea

Laurea-ammattikorkeakoulu

Tietoturvakäyttäytymiseen vaikuttavat tekijät

Laura Mainio
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Joulukuu, 2021

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Laura Mainio

Tietoturvakäyttäytymiseen vaikuttavat tekijät

Vuosi 2021 Sivumäärä 43

Opinnäytetyön tavoitteena oli selvittää, mitkä tekijät vaikuttavat tietoturvakäyttäytymiseen. Lähtökohta toimeksiannolle oli se, että tiedon luokitteluun ja käsittelyyn liittyvät ohjeet muuttuivat OP Ryhmässä, ja haaste oli se, miten saada henkilöstö toimimaan ohjeiden mukaan. Koulutus toteutettiin verkkokurssina. Verkkokurssin tavoitteena on lisätä tietoturvatietoisuutta, mutta tietoisuus ei aina siirry käytännön toimintaan.

Opinnäytetyön viitekehykseen kuului tietoturvakäyttäytyminen, tietoturvatietoisuus ja niihin liittyvät motivaatioteoriat. Lähestymistavaksi valikoitui toimintatutkimus, joka sopii hyvin tutkimukselliseen kehittämistyöhön. Tiedonkeruumenetelmät olivat haastattelu ja kirjallisuuskatsaus.

Tutkimusaineiston perusteella tietoturvakäyttäytymiseen vaikuttavat tekijät ovat asenteet, palkkiot ja rangaistukset, tarpeet, tietoisuus, muisti, keskittymiskyky, verkkokurssin ominaisuudet, ajankäytön haasteet, vaikutukset omaan työhön, viestintä ja arvot. Johtopäätös on se, ettei tietoisuuden lisääminen vaikuta suoraan käyttäytymiseen, mutta koulutuksella voidaan korostaa hyviä toimintamalleja. Lisäksi organisaatiossa varmistetaan, että ohjeiden noudattaminen on käytännössä mahdollista. Viestinnällä voidaan vaikuttaa siltä osin, ettei tietoturvallisuuteen liittyviä ohjeistuksia unohdeta. Palkitsemisella voi motivoida henkilöstöä toimimaan turvallisemmin.

Asiasanat: Käyttäytyminen, motivaatio, tietoturvatietoisuus, verkkokoulutus

Laurea University of Applied Sciences
Degree Programme in Safety, Security and Risk Management
Bachelor's Thesis

Laura Mainio

Abstract

Factors Influencing Information Security Behavior

Year 2021 Pages 43

The objective of the thesis was to map which factors influence information security behavior. The starting point for the assignment was that the instructions related to the classification of information were changed in OP Financial Group, and the challenge is how to have the employees act in accordance with the instructions. Security training was implemented as an online course. The purpose of the online course is to raise information security awareness, but awareness does not automatically translate into employees acting securely.

The frame of reference introduces the themes of information security behavior, information security awareness and related motivation theories. The research approach chosen was action research, which is well suited for research and development work. Data collection methods include an interview and a literature review.

Based on the research data, the factors influencing information security behavior are attitudes, rewards and sanctions, needs, awareness, memory, ability to concentrate, features of the online course, time management, implications for one's own work, communication and values. In conclusion, raising awareness with training does not directly affect behavior but it can emphasize working practices. In addition, the organization can ensure that it is practically possible to follow the instructions in the organization. Communication can make an impact on the information security-related instructions so that they are not forgotten. Rewarding can motivate employees to act more securely.

Keywords: Behavior, Information Security Awareness, Motivation, Online Learning

Sisällys

1 Johdanto

Organisaatiot hyödyntävät erilaista teknologiaa parantaakseen tietoturvallisuutta, mutta huomiota kiinnitetään entistä enemmän tietoturvapolitiikkaan, yrityskulttuuriin ja yksilöiden rooliin tietoturvallisuudessa. Yritysjohto on vastuussa siitä, miten tietoturvauhkia torjutaan, ja osaltaan vaikuttaa siihen, miten organisaatiossa suhtaudutaan tietoturvallisuuteen. Tietoturvallisuutta tulee ajatella laajemmasta näkökulmasta eikä vain tietotekniikan näkökulmasta (Keskuskauppakamari 2016). Tutkimukset tietoturvarikkomuksista osoittavat, että pelkästään henkilöstön huolimattomuus tai se, ettei tietoturvaohjeistuksia ole noudatettu, on johtanut organisaatioissa miljoonien dollarien menetyksiin (Herath & Rao 2009, 107). Jos organisaatio ei kykene ennaltaehkäisemään tietoturvarikkomuksia, joissa syynä on työntekijöiden huolimattomuus, kertoo se siitä, ettei organisaatiossa oteta tarpeeksi huomioon työntekijöiden arvoja ja uskomuksia eikä keinoja, joilla voidaan vaikuttaa sääntöjen ja ohjeiden noudattamiseen (Herath 2009, 107, Mishra & Dhillon, 2006 mukaan).
Tietoturvatietoisuus on olennainen asia, jos halutaan muuttaa toimintamalleja. Organisaation velvollisuus on huolehtia siitä, että henkilöstö on riittävällä tasolla perehdytetty yrityksen tietoturvaohjeisiin ja sääntöihin sekä varmistaa, että tietoa on saatavilla tarpeeksi. Tietoisuus ei kuitenkaan takaa sitä, että jokainen toimii sääntöjen tai ohjeistusten mukaan. Esimerkiksi jokainen tupakoitsija tietää tavan riskit terveydelle, mutta monet tupakoivat silti. Jokaista työntekijää ei ole isossa organisaatiossa mahdollista motivoida erikseen noudattamaan sääntöjä, mutta on olemassa keinoja, joilla käyttäytymiseen voidaan vaikuttaa.

Ihmisten käyttäytymistä ja motivaatiota työelämäkontekstissa on tutkittu paljon viime vuosina. Motivaatio vaikuttaa siihen, toimiiko henkilöstö tietoturvaohjeiden mukaisesti. Ihmistä on pidetty heikoimpana lenkkinä tietoturvallisuuden kannalta, koska ohjeet ja säännöt ovat turhia, jos henkilöstö ei ole motivoitunut noudattamaan niitä (Herath 2009). Toisaalta tämä ajattelumalli saattaa aiheuttaa luottamuspulaa, ja siten demotivoida henkilöstöä. Motivaatiota noudattaa tietoturvaohjeita ei voi syntyä, jos henkilöstö ei ole tietoinen erilaisista riskeistä tai ei ole tietoinen turvallisista toimintatavoista. Myös yrityskulttuuri on vaikuttava tekijä yksilöiden käyttäytymisessä, ja muutosta voi ohjata yrityskulttuurin kautta. Yrityskulttuuri ohjaa yksilöiden käyttäytymistä yhteisten arvojen mukaisesti ja sitouttamalla yksilöä organisaatioon (Hu, Dinev, Hart & Cooke 2012, 618). Opinnäytetyössä perehdytään aiempiin tutkimuksiin, jotka liittyvät henkilöstön käyttäytymiseen ja motivaatioon sekä siihen, miten organisaatiossa voidaan motivoida työntekijöitä.

2 Toimeksiannon lähtökohdat

Lähtökohta toimeksiannolle oli se, että OP:n tiedon luokitteluun ja käsittelyyn liittyvät ohjeet muutetiin kokonaan, ja haaste on se, miten saada henkilöstö toimimaan ohjeiden mukaan. OP:ssa oli jo aiemmin käytössä tiedon turvaluokat, mutta harva tiesi näistä luokista tai käytti niitä, koska tietoisuutta ei pidetty yllä. Tiedon turvaluokilla tarkoitetaan sitä, että tieto luokitellaan sen arkaluontoisuuden mukaan esimerkiksi luottamukselliseksi ja jokaista luokkaa kohden on erilliset ohjeet siitä, miten tietoa käsitellään. Luokittelulla varmistetaan se, että jokainen tietää miten tietoa kuuluu käsitellä sille annetun luokan perusteella. Tiedon käsittelyllä tarkoitetaan tiedon luomista, muokkaamista, tallentamista, jakamista, siirtämistä ja tuhoamista. Työntekijällä on vastuu tiedon turvallisesta käsittelystä käsittelyn jokaisessa vaiheessa.

Koulutuksella pyritään lisäämään tietoutta tarpeesta luokitella tiedot ja miten se tehdään, jotta henkilöstö voisi toimia turvallisemmin. Tiedon vääränlainen käsittely voi johtaa siihen, että tietoa joutuu vääriin käsiin. Kauppakamarin artikkelin mukaan voidaan puhua Compliance riskeistä. Compliance eli vaatimustenmukaisuus voidaan määritellä sääntöjen, lakien ja määräyksien noudattamiseksi. Ne voivat realisoitua asiakkaiden ja yhteistyökumppaneiden menetyksinä, sakkoina, vahingonkorvauksina, toimilupien menetyksinä ja yrityksen arvon laskuna. Myös maineriskeistä ollaan koko ajan tietoisempia, koska someaikana on entistä vaikeampaa korjata jo syntyneitä mainevahinkoja. Pelkästään lainsäädännön noudattaminen ei aina riitä, vaan pitää toimia eettisesti oikein suuren yleisön mielestä. (Kauppakamari 10.4.2017.)

Toimeksiantajan toivomusten mukaisesti koulutus toteutettiin verkkokurssina. Koulutuksella voidaan lisätä henkilöstön tietoturvatietoisuutta ja pienissä organisaatioissa perehdytys voidaan toteuttaa joustavasti eri metodeilla, kuten esimerkiksi luokkakoulutuksena tai digitaalisena koulutuksena. Isoissa organisaatioissa metodin valinnassa on rajoituksia varsinkin, jos kysymys on monialaisesta yrityksestä ja koulutus koskee koko henkilöstöä. Yleensä ratkaisu on verkkokurssi tai webinaari eli luento, joka kuvataan ja jonka voi katsoa myös jälkikäteen. Verkkokoulutuksen heikkous on se, että keskittymiskyky saattaa helpommin harhailla työasioihin, jos verkkokurssin suorittamiseen ei varaa erikseen aikaa. Verkkokurssi on usein edullisempi vaihtoehto kuin luokkaopetus, koska kouluttaja ei myy omaa aikaansa vaan kustannukset tulevat digitaalisesta tuotteesta (Digivallankumous 2019). Verkkokurssin voi myös suorittaa milloin vain ja paikasta riippumatta. Webinaareihin verrattuna verkkokurssissa voidaan myös testata osaamista tehtävillä.

2.1 Kohdeorganisaatio

OP Ryhmä on Suomen johtava finanssiryhmä ja alan suurin työnantaja Suomessa. OP Ryhmän muodostavat yli 150 itsenäistä osuuspankkia ja niiden omistama keskusyhteisö OP Osuuskunta tytär- ja lähiyhteisöineen. OP:ssa työskentelee yli 12 000 finanssialan ammattilaista, joista Baltiassa noin 400. OP Ryhmän liiketoiminta on jaettu kolmeen pääliiketoiminta-alueeseen, jotka ovat pankkitoiminta, vahinkovakuutus ja varallisuudenhoito. Terveys- ja hyvinvointipalvelut ovat osa vahinkovakuutusliiketoimintaa. (OP 8.3.2019.)

OP Ryhmän tavoitteena on muuttua asteittain pelkästä finanssitoimijasta digitaalisen ajan monialaiseksi palveluyritykseksi, jolla on vahva finanssiosaaminen. OP:n strategiassa korostuu asiakaskokemuksen kehittäminen palveluita ja toimintoja digitalisoimalla. (OP 8.3.2019.) Palveluiden digitalisoituminen on mullistanut koko rahoitusjärjestelmän, mutta on myös tuonut mukanaan uuden uhan; kyberrikollisuuden. Esimerkiksi OP Ryhmään kohdistui uudenvuoden yönä 2015 palvelunestohyökkäys, joka aiheutti häiriöitä OP-Pohjolan verkkosivuston ja maksukorttien toimintaan (Yle 2.1.2015). On tärkeää, että asiakkaat luottavat järjestelmän vakauteen ja siihen, että heidän tietojaan käsitellään asianmukaisesti.

Liiketoimintojen laajentaminen on aloitettu terveys- ja hyvinvointiliiketoiminnasta. Strategian taustalla on muutokset finanssialalla sekä muutokset asiakkaiden odotuksissa. OP:n tavoitteena on laajentaa toimintaa asiakkaille lisäarvoa tuottaville uusille alueille, esimerkiksi asumiseen, liikkumiseen ja sähköiseen kaupankäyntiin (OP 8.3.2019). Toiminnan laajentuminen sekä toukokuussa 2018 voimaan astunut EU tietosuoja-asetus vaikuttavat OP:n sisäisiin tietoturvavaatimuksiin.

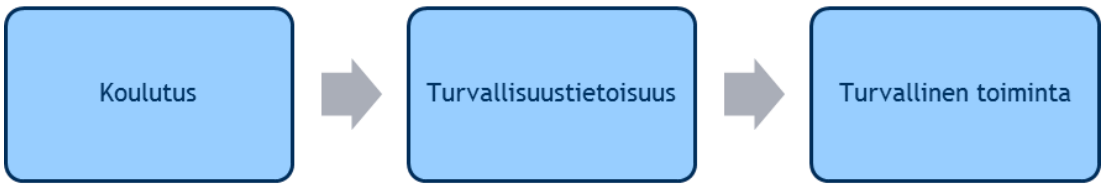
Kuvio 1: Ryhmärakenne v. 2019 (OP 8.3.2019)

Verkkokoulutuksen kohderyhmä on koko OP Ryhmän henkilöstö ja kumppanit kaikilta pääliiketoiminta-alueilta, ja tämä asettaa huomattavia haasteita verkkokoulutuksen sisällölle.

2.2 Opinnäytetyön rajaukset ja tavoite

Opinnäytetyössä ei keskitytä verkkokoulutuksen tai ohjeistuksen varsinaiseen sisältöön, vaan siihen mitkä tekijät vaikuttavat siihen, noudattaako henkilöstö tietoturvaohjeistuksia. Opinnäytetyön tutkimuksen tavoite on vastata myös siihen, miten tätä tietoa voidaan käytännössä hyödyntää. Tutkimuskysymykseksi muotoutui ”Mitkä tekijät vaikuttavat tietoturvakäyttäytymiseen?”

Koulutuksen tarkoitus on lisätä henkilöstön tietoisuutta ja ymmärrystä organisaation turvallisuuteen liittyvistä säännöistä, ohjeista ja riskeistä. Oppiminen ja opitun asian siirtäminen käytännön toimintaan on kuitenkin yksilön vastuulla eli koulutuksen, tietoisuuden ja käyttäytymisen väliin jää paljon muuttuvia tekijöitä.



Kuvio 2: Koulutuksen vaikutus toimintaan

3 Tietoperusta

Luvussa käsitellään opinnäytetyön tietoperustaa ja avataan siihen liittyviä käsitteitä. Luvussa esitellään erilaisia asenteita, jotka vaikuttavat henkilöstön valmiuteen noudattaa turvallisuutta koskevia ohjeita ja toimintatapoja sekä motivaatioteorioita, jotka kuvaavat motivaation luonnetta, syntymistä ja ylläpitoa työympäristössä. Motivaatioon liittyviä teorioita on paljon, joten tutkimuslähteinä hyödynnetään niitä, jotka liittyvät motivaatiotekijöihin työympäristön ja tietoturvallisuuden näkökulmasta.

Motivaatioteoriat voidaan jakaa sisältö- ja prosessiteorioihin. Sisältö eli tarveteoriat selittävät käyttäytymisen sisäisiä syitä, jotka saavat aikaan ja ylläpitävät käyttäytymistä tai jotka vaikuttavat käyttäytymisen loppumiseen. Sisältöteoriat keskittyvät ihmisten tarpeisiin, kuten Maslowin tarvehierarkia, joka esitellään luvussa 3.2. Prosessiteoriat kuvaavat yksilöllisiä eroja reagoinnissa ulkoisiin ja sisäisiin tekijöihin. Prosessiteoriat kuvaavat myös, miten toiminta syntyy, ylläpidetään ja miten sen saa loppumaan (Kinnunen 2015,15). Esimerkki prosessiteoriasta on odotusarvoteoria, joka esitellään luvussa 3.5.

3.1 Käsitteet

Motivaatio

Motivaatiolla tarkoitetaan niitä sisäisiä ja ulkoisia syitä, joiden takia toimimme niin kuin toimimme. Motiivi on tarve, joka halutaan tyydyttää, ja nämä tarpeet voivat olla tietoisia tai tiedostamattomia (Kinnunen 2015,14). Motivaatio voi olla sisä- tai ulkosyntyistä eli käyttäytyykö ihminen tietyllä tavalla, koska toiminnan tavoite on henkilökohtaisella tasolla tärkeä vai perustuuko toiminta ulkoisiin seurauksiin kuten rangaistuksiin, palkintoihin tai pakollisuuteen.

Tietoturvakäyttäytyminen

Tietoturvakäyttäytymisellä tarkoitetaan sitä, miten henkilöstö käsittelee tietoa työpaikalla, työmatkoilla ja kotona. Tietoturvallinen käyttäytyminen edellyttää sitä, että henkilöstö osaa käsitellä tietoa asianmukaisesti, ja osaa soveltaa tietoturvaohjeita omaan työhönsä sekä on tietoinen tietoturvallisuuteen liittyvistä riskeistä. Tietoturvakäyttäytymiseen liittyy myös muiden työntekijöiden ohjeistaminen tarvittaessa sekä mahdollisista puutteista tai rikkomuksista ilmoittaminen asianmukaiselle taholle. Motivaatio vaikuttaa tietoturvakäyttäytymiseen.

Tietoturvatietoisuus

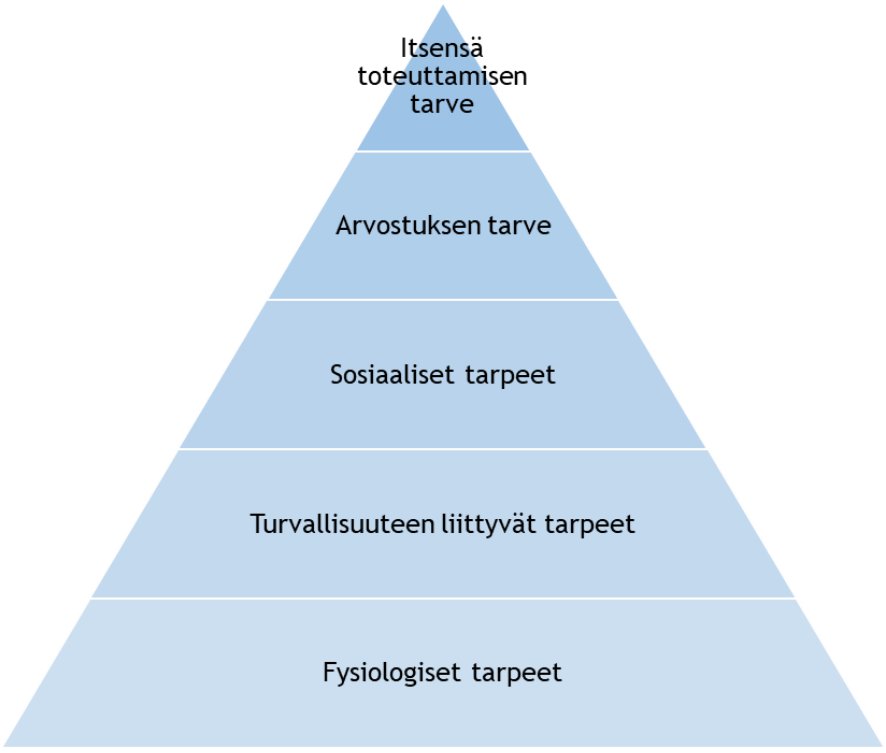
Vahti-ohjeiden mukaan tietoturvatietoisuus on organisaation henkilöstön tai muun kohdejoukon tiedot ja asenteet, jotka koskevat turvallisuuden tavoitteita ja keinoja (VAHTI 8/2008). Tietoturvatietoisuuteen sisältyy myös idea siitä, että henkilöstö on sitoutunut noudattamaan organisaation tietoturvamääräyksiä (Bulgurc, Cavusoglu & Benbasat 2010, 532). Tietoturvatietoisuus voidaan jakaa yleiseen tietoturvatietoisuuteen ja tietoisuuteen tietoturvapolitiikasta. Tietoturvatietoisuudella tarkoitetaan esimerkiksi sitä, että yksilö on tietoinen siitä, että salasanat ovat välttämättömiä, mutta ei välttämättä tietoinen siitä, millaiset kriteerit organisaatio on asettanut salasanojen pituudelle tai käytettäville merkeille, mikä taas liittyy tietoisuuteen tietoturvapolitiikasta. (Bulgurc ym. 2010, 533.)

Verkkokoulutus

Verkkokoulutuksella voidaan tarkoittaa jollekin verkkoalustalle tehtävää verkkokurssia tai muuta verkossa olevaa koulutusmateriaalia kuten kuvia ja videoita. Verkkokurssit sisältävät yleensä tehtäviä, joilla testataan osaamista.

3.2 Maslowin tarvehierarkia

Yksi tunnetuimmista motivaatioteorioista on Maslowin tarvehierarkia. Teorian mukaan ihmisellä on viidenlaisia tarpeita ja yksilöt tavoittelevat aina korkeampaa tarvetasoa. Alemman tason tarve täytyy olla täytetty ennen kuin voidaan siirtyä seuraavalle tasolle. Joskus yksilö saattaa jättää alemman tason tarpeet tyydyttämättä pyrkiessään johonkin tärkeään päämäärään. Tasot ovat:



Kuvio 3: Maslowin tarvehierarkia (tiedot: Roper ym. 2006, 86)

Fysiologiset tarpeet ovat perustarpeita, joihin kuuluu esimerkiksi ruoka, juoma ja seksuaalisuus. Turvallisuuden tarpeisiin liittyy esimerkiksi luotto auktoriteetteihin tai kun turvaudutaan totuttuun. Sosiaalisiin tarpeisiin liittyy itsensä hyväksytyksi tunteminen ja kuuluminen ryhmään. Arvostuksen tarpeeseen sisältyy tekijöitä, joissa yksilö pyrkii erottumaan joukosta.

Itsensä toteuttamisen tarpeessa ihminen kokee, että hänellä on kyky ja mahdollisuus saavuttaa päämääränsä. Maslowin tarvehierarkia on saanut kritiikkiä muun muassa hierarkian universaalisuudesta, koska aineistoa kerättiin vapaasti erilaisissa tilanteissa ja keskustellen valikoitujen ihmisten kanssa. (Otavan opisto 2015.) Kuitenkin henkilöstön motivoinnissa tarvehierarkia on käytännöllinen tapa tutkia esimerkiksi sitä, millaisilla palkkioilla voidaan vaikuttaa parhaiten käyttäytymiseen.

3.3 Henkilöstön asenteet

Jos halutaan vaikuttaa henkilöstön käyttäytymiseen, erilaiset asenteet turvallisuutta kohtaan täytyy ottaa huomioon. On helpompaa motivoida työntekijää, jolla on jo valmiiksi positiivinen asenne kuin työntekijää, joka lähtökohtaisesti suhtautuu negatiivisesti tietoturvallisuutta koskeviin ohjeistuksiin ja toimintatapoihin. Kaikenlaisia asenteita on tärkeä ymmärtää, jotta organisaatiossa osataan käyttää erilaisia lähestymistapoja motivoinnissa. (Roper ym. 2006, 74-75.) Asenteet voidaan jakaa kuuteen kategoriaan:

Taulukko 1: Henkilöstön asenteet (tiedot: Roper ym. 2006, 75-76)

Vastustus (Subversion)	• Rikotaan tahallisesti organisaation turvallisuusmääräyksiä ja ohjeita • Kategoriaan kuuluu esim. salaisen tiedon jako kilpailijoille työpaikan toivossa • Suurin haaste ovat työntekijät, jotka pitävät itseään liian tärkeinä noudattamaan määräyksiä tai työntekijät, jotka pitävät turvallisuusvaatimuksia turhina
Välttely (Avoidance)	• Vältellään turvallisuushenkilöstöä eikä osallistuta turvallisuuteen liittyviin asioihin • Jos joku rikkoo turvallisuusvaatimuksia, siihen ei puututa
Välinpitämättömyys (Apathy)	• Ei välitetä turvallisuudesta, uhkakuviin ei ehkä uskota tai uskotaan ettei turvallisuuteen vaikuttavista toimenpiteistä ole apua • Noudatetaan sääntöjä, jos tulee sanktioita, mutta muussa tapauksessa vaatimuksista ei välitetä
Myöntyväisyys (Compliance)	• Sääntöjä noudatetaan ja toimitaan vaatimusten mukaan, mutta jos jotain asiaa ei erikseen mainita säännöissä, ajatellaan ettei se ole oma ongelma eikä tilanteissa osata toimia ilman sääntöjä
Osanotto (Participation)	• Ajatellaan, että organisaation turvallisuusmääräykset ovat järkeviä ja niitä noudatetaan • Valmius tehdä yhteistyötä ja toimia eri tilanteissa turvallisesti sekä ehdottaa parannuksia, jos sellainen tulee mieleen
Vastuunotto (Ownership)	• Otetaan vastuu organisaation turvallisuudesta, koska kysymys on yhteisistä säännöistä ja vaatimuksista • Turvallisuusasiantuntijat neuvovat ja auttavat eivätkä ole pelkästään auktoriteetti • Johdon tasolla ideaali tilanne, koska silloin käytetään tarpeeksi resursseja turvallisuuteen

3.4 Positiivinen ja negatiivinen motivaatio

Positiivisessa motivaatiossa ihminen luottaa siihen, että tavoitteen saavuttamisesta tai oikeanlaisesta toiminnasta seuraa palkinto tai muu positiivinen seuraus. Negatiivisessa motivaatiossa taas luotetaan siihen, että vääränlaisesta toiminnasta seuraa rangaistus. (Roper ym. 2006, 80.)

Usein organisaatioissa motivointi perustuu rangaistuksiin kuten varoituksiin ja irtisanomiseen, jos turvallisuusvaatimuksia rikotaan, mutta harvemmin palkitsemiseen. Sääntöjen noudattaminen on toki perusolettamus jokaisessa organisaatiossa, mutta jos halutaan motivoida henkilöstöä olemaan oma-aloitteisempia ja ottamaan henkilökohtaista vastuuta organisaation tietoturvallisuudesta, organisaatio voisi harkita myös positiivisen motivaation keinojen käyttämistä. Carl Roperin, Joseph Graun, and Lynn Fischerin kirjassa otetaan myös kantaa siihen, että negatiivinen motivaatio on epäluotettavin motivaatiomuoto, koska ei ole varmuutta siitä, motivoivatko negatiiviset seuraukset noudattamaan sääntöjä vai rikkomaan niitä jäämättä kiinni. Tutkimusten mukaan positiivinen motivaatio on luotettavampaa, koska ihmiset huijaavat epätodennäköisemmin, kun tiedossa on palkinto, kun taas rangaistuksen pelossa huijataan todennäköisemmin. (Roper ym. 2006, 80.)

Tietoturvallisuuden kannalta tärkeää on se, että asetetut tavoitteet saavutetaan toimimalla turvallisesti. Virheiden peittely ei auta saavuttamaan tavoitetta, vaan vie vain kauemmas tavoitteesta. Negatiivisella motivaatiolla on kuitenkin myös oma paikkansa varsinkin, jos on kysymys vakavista tietoturvarikkomuksista, jotta henkilöstö osaa myös välttää epätoivottuja toimintamalleja.

3.5 Odotusarvoteoria

Victor Vroomin 1960-luvulla kehittämä motivaatioteoria on yksi käytetyimmistä teorioista yritysmaailmassa. Odotusarvoteorian mukaan ihminen motivoituu, jos tehtävästä suoriutuminen tuottaa hänelle toivotun palkkion tai hyödyn. Saatavan palkkion ei pidä olla liian helposti eikä vaikeasti saavutettavissa (odotusarvo). (Roper ym. 2006, 81.) Palkkiolla ei välttämättä tarkoiteta aineellista hyötyä vaan palkkio voi olla myös jokin abstrakti asia kuten kunnioitus tai ihailu. Teoria kiteytyy VIE -kaavaan, jossa

E, expectancy

Odotukset eli tuottaako vaivannäkö paremman suoriutumisen. Jos annettu tehtävä koetaan liian vaikeaksi, sen eteen ei haluta työskennellä. Henkilöstö pitää siis saada uskomaan, että tietoturvaohjeiden noudattaminen ei ole niin vaikeaa ja aikaa vievää kuin ajatellaan. Ensinnäkin pitäisi pyrkiä välttämään sitä, että jokin asia esitetään vaikeana. (Roper ym. 2006,85.)

Esimerkiksi oikean turvaluokan valitseminen dokumenttiin pitäisi esittää helppona ja yksinkertaisena asiana kun seuraa ohjetta. Joskus näkee ohjeita, jotka vaikuttavat ensin monimutkaisilta, mutta usein asian voi tiivistää muutamaan kysymykseen tai kohtaan, joiden avulla kuka tahansa selviää tehtävästä vaivatta. Työntekijä voi myös joutua tilanteeseen, jossa hän ei tiedä, mikä on oikea tapa toimia. Turvallisuusvastaavien yhteystiedot pitäisi olla helposti saatavilla, ja korostaa sitä, että apua voi saada aina tarvittaessa (Roper ym. 2006, 85).

I, instrumentality

Miten yksilö arvioi suorituksen edistävän palkkioiden saamista. Yksilöiden pitää uskoa siihen, että käyttäytymisestä seuraa palkinto tai rangaistus. Uhkaukset ja lupaukset pitää siis toteuttaa, ja henkilöstön pitää myös tietää, että ne toteutetaan. Positiivisen motivaation kohdalla tämä tarkoittaa käytännössä sitä, että palkitsemisesta on jollain tavalla tiedotettu esimerkiksi sisäisissä uutisissa. Kun joku palkitaan hyvästä suoriutumisesta, se voidaan tehdä esimerkiksi tiimipalaverin aikana. Negatiivisen motivaation kohdalla ei voi välttämättä voi toimia samoin, koska tietoturvasääntöjen rikkomisesta seuraava rangaistus esim. irtisanominen tai varoitus voi kuulua salassa pidettävän tiedon piiriin. Negatiivisten seurausten julkitulo voi myös vaikuttaa henkilöstön asenteisiin siten, että turvallisuutta pidetään asiana, joka aiheuttaa vain ongelmia työntekijöille. (Roper ym. 2006, 84.)

V, valence

Miten haluttavana yksilö pitää käyttäytymisensä päämäärää henkilökohtaisesti (Riihelä 2012,15). Valenssi muistuttaa, että yksilöt antavat erisuuruisen arvon eri palkinnoille eri tilanteissa (Roper ym. 2006, 81). Ei ole tietenkään mahdollista tietää jokaisen ajatuksia siitä, mikä on sopiva palkinto, mutta joitain yleistyksiä on mahdollista tehdä esimerkiksi Maslowin tarvehierarkian perusteella. Rahaa pidetään usein hyvänä palkintona, mutta rahan antaminen palkinnoksi ei ole aina mahdollista eikä se ole myöskään ainoa palkinto. Aiemmin puhuttiin siitä, että palkkion ei tarvitse olla aineellinen. Kehuminen ei maksa mitään, ja kehuminen voi olla tehokas väline, kun sitä käyttää oikein. Kehumisen vaikutusta voi tehostaa kehumalla yksilöä muiden läsnä ollessa, koska julkinen kehuminen nostaa yksilön arvoa yhteisön silmissä, ja näin ollen yksilöt yleensä arvostavat sitä (Roper ym. 2006, 83). Kehuminen kannattaa tehdä myös kehuttavan yksilön esimiehen läsnä ollessa, ja kirjallisessa kehumisessa kirje tai sähköposti kannattaa lähettää myös esimiehelle. Tällöin myös esimies voi motivoitua tukemaan positiivista käyttäytymistä. (Roper ym. 2006.)

3.6 Suojelumotivaatioteoria (PMT)

Suojelumotivaatioteoria (Protection Motivation Theory, PMT) selittää, miten yksilöt suhtautuvat uhkiin tai vaaroihin ja millaisia toimintatapoja yksilö valitsee. Suojelumotivaatioteoriassa

on kolme tekijää, jotka selittävät miten uhkiin suhtaudutaan, joita kutsutaan uhkien arviointitekijöiksi. Tekijät ovat palkintoja tai etuja (sisäinen tai ulkoinen motivaatio, joka vaikuttaa siihen, jatkaako tai lisääkö ei-haluttua käyttäytymistä), uhkan suuruus ja haavoittuvuus (missä määrin yksilön katsotaan olevan alttiina uhalle). Suojelumotivaatiossa on myös kolme tekijää, jotka selittävät yksilön kykyä selviytyä uhasta, jota kutsutaan selviytymisarvioiksi. Näitä ovat reaktion tehokkuus (usko selviytymistoimien koettuihin hyötyihin poistamalla uhka), kustannukset (yksilölle suojaavan käyttäytymisen toteuttamisessa) ja minäpystyvyys (missä määrin yksilö kokee, että suojakäyttäytyminen on mahdollista toteuttaa). (Pahnila, Sippola, Vance 2012, 190-191.)

Teorian yleiseen luonteeseen liittyen, suojelumotivaatioteoriaa on viime aikoina sovellettu tietoturvallisuuteen. Teoriassa uhkia koskevat tiedot aiheuttavat yksilöissä kognitiivisen välitysprosessin, jossa arvioidaan positiivisia tai kielteisiä vastauksia. Työntekijöiden tietoturvakäytäntöjen noudattamatta jättäminen edustaa epäadaptiivista vastausta, kun taas niiden noudattaminen on adaptiivinen vastaus. (Pahnila ym. 2012, 191.)

Tutkimuksessa Motivating IS security compliance: Insights from Habit and Protection Motivation Theory todetaan, että aiemmissa tutkimuksissa ei ole tutkittu aiemman ja automaattisen käyttäytymisen vaikutusta työntekijöiden päätökseen noudattaa tietoturvakäytäntöjä. Aiemman käyttäytymisen oletetaan vaikuttavan voimakkaasti päätöksentekoon. Tämän aukon korjaamiseksi yhdistettiin tavat (rutiininomainen muoto aiemmasta käyttäytymisestä) suojelumotivaatioteoriaan (PMT) -periaatteeseen selittääkseen tietoturvakäytäntöjen noudattamisen. Suomessa toteutettu empiirinen testi osoitti, että tavanomainen tietoturvan noudattaminen vahvisti voimakkaasti PMT:n teoreettisia kognitiivisia prosesseja sekä työntekijöiden aikomusta noudattaa niitä tulevaisuudessa. Tutkijat havaitsivat myös, että melkein kaikki PMT:n komponentit vaikuttivat merkittävästi työntekijöiden aikomukseen noudattaa tietoturvakäytäntöjä. Yhdessä nämä tulokset korostivat työntekijöiden aiemman ja automaattisen käyttäytymisen merkitystä tässä asiassa. (Pahnila ym. 2012, 190.)

Tutkimuksessa käytettiin kuvitteellisia skenaarioita, jossa tutkittaville kuvailtiin tietoturvarikkomukseen liittyvä toiminta tai päätös. Tutkittavia henkilöitä pyydettiin sitten vastaamaan kyselyyn. Tutkimuksessa valittiin viisi yleistä tietoturvarikkomusta, jotka olivat yleisiä tutkimuskohteena olevassa organisaatiossa. Niiden pohjalta luotiin viisi skenaariota, jotka olivat: salasanojen jakaminen, työaseman lukitsematta jättäminen, luottamuksellisen tiedon lukeminen tulostimella, antamalla lasten käyttää työasemaa kotona ja asentaa ohjelmia ja arkaluontoisen tiedon kopiointi USB-tikulle ilman salausta. (Pahnila ym. 2012, 192.) Tarkoituksena oli selvittää todennäköisyys sille, kuinka todennäköisesti tutkittava henkilö toimii samalla tavalla kuin skenaarioissa.

Esimerkki

Rikkomus: Luottamuksellisten dokumenttien lukeminen

Jack käy toimiston tulostimella yksin ja näkee toisen työntekijän tulostaman dokumentin. Dokumentti on luottamuksellinen. Organisaation tietoturvasäännöt kieltävät luottamuksellisen aineiston lukemisen muilta kuin asianmukaisilta henkilöiltä, mutta Jack on utelias ja lukee nopeasti dokumentin. (Pahnila ym. 2012,195.)

Tutkimuksen johtopäätöksissä todettiin, että ammatinharjoittajien on varmistettava, että työntekijät tunnistavat tietoturvauhat ja riskit, joita nämä uhat aiheuttavat heidän organisaatiolleen. Lisäksi on tärkeää kertoa työntekijöille, että heidän organisaatioonsa kohdistuu todennäköisesti tietoturvauhkia, jos he eivät ota tietotietotekniikan tekniikoita ja käytäntöjä vakavasti ja noudattavat käytäntöjä. Toiseksi työntekijöiden tulisi tietää, että tietotietoturvapolitiikan noudattaminen on osa heidän työvastuutaan. Kolmanneksi organisaatioiden on varmistettava, että tietoturvakäytäntöjä ja -menettelyjä ei ole vaikea käyttää. Viimeiseksi on tärkeää varmistaa, että työntekijät noudattavat tietoturvallisuuspolitiikkaa. (Pahnila ym. 2012.)

4 Tutkimusmenetelmät

Tässä luvussa esitellään tiedonkeruu- ja aineiston analysointimenetelmät sekä menetelmien rajoitteita. Tutkimus on luonteeltaan toimintatutkimus. Toimintatutkimuksessa lähtökohtana on toiminnan tai käytänteiden muuttaminen (Ojasalo, Moilanen & Ritalahti 2009, 60), joten toimintatutkimus lähestymistapana on sovellettavissa tähän opinnäytetyöhön. Toimintatutkimus katsotaan yleensä laadulliseksi lähestymistavaksi, mutta myös määrällisiä menetelmiä voidaan käyttää (Ojasalo, Moilanen & Ritalahti 2010, 61). Opinnäytetyössä hyödynnetään kuitenkin pelkästään laadullisia eli kvalitatiivisia menetelmiä, koska tarkoitus on ymmärtää tutkittavan ilmiön laatua ja ominaisuuksia kokonaisvaltaisesti.

4.1 Tiedonkeruumenetelmät

Opinnäytetyötä varten käytetyt tiedonkeruumenetelmät ovat laadullisia, ja valitut menetelmät ovat haastattelu ja kirjallisuuskatsaus. Laadullisessa tutkimuksessa käytetään harkinnanvaraista otantaa ja tutkittavia yksilöitä ei yleensä ole kovin suurta määrää. Tärkeintä on aineiston laatu, ei määrä. Haastattelun tuloksia vertaillaan myös aiempiin tutkimuksiin, jotka liittyvät motivaatioon ja henkilöstön asenteisiin tietoturvanäkökulmasta.

Kirjallisuuskatsauksella kartoitetaan sitä, millaista tietoa joltakin rajatulta alueelta on olemassa. Yleensä haetaan vastausta johonkin kysymykseen, kuten tutkimusongelmaan. Kirjallisuuskatsauksen avulla saadaan tietoa siitä, miten paljon tutkimustietoa on olemassa, millaisesta näkökulmasta aihetta on tutkittu ja millaisin menetelmin. (JAMK 24.4.2019.) Opinnäyte-

työssä esitellään motivaatioteorioita ja aiempia tutkimuksia, joiden kautta pyritään selittämään ihmisten käyttäytymistä tietoturvakontekstissa. Opinnäytetyössä myös vertaillaan haastattelun ja aiempien tutkimusten tuloksia.

Valitsin opinnäytetyön tiedonkeruumenetelmäksi haastattelun, koska haastattelussa ollaan suorassa vuorovaikutuksessa tutkittavan kanssa, joka mahdollistaa tiedonhankinnan suuntauksen itse tilanteessa (Hirsjärvi & Hurme 2008, 34). Tutkijan tehtävä on välittää kuvaa haastateltavan ajatuksista, käsityksistä, kokemuksista ja tunteista (Hirsjärvi & Hurme 2008, 41). Opinnäytetyön menetelmä on teemahaastattelu, joka ei etene tarkkojen, yksityiskohtaisten, valmiiksi muotoiltujen kysymysten kautta vaan väljemmin kohdentuen tiettyihin ennalta suunniteltuihin teemoihin. Teemahaastattelu on astetta strukturoidumpi kuin avoin haastattelu, koska siinä aihepiiriin tutustumisen pohjalta valmistellut aihepiirit ja teemat ovat kaikille haastateltaville samoja. (KvaliMotv 8.3.2019.)

4.2 Menetelmien rajoitteet

Ryhmähaastatteluiden ongelmat tai haasteet ovat paljolti luonteeltaan sosiaalisia eli ryhmän ilmapiiri vaikuttaa siihen, ketkä puhuvat, mitä puhutaan ja milloin puheenvuoroja otetaan eikä ryhmässä välttämättä uskalleta kertoa kaikkea verrattuna kahdenkeskiseen haastatteluun. Haastattelijalta vaaditaan taitoa olla läsnä tilanteessa ja rohkaista ryhmässä mahdollisesti syrjään jääviä henkilöitä puhumaan. Haastatteluajankohdan sopiminen voi olla hankalaa, koska pitää sovittaa yhteen useiden ihmisten aikataulut. Tekniset ongelmat voivat myös vaikeuttaa haastattelua, jos esimerkiksi mikrofoni ei toimi. Mikrofoneja, joiden toimivuus on testattu, on oltava riittävästi, jotta keskustelu saataisiin tallennettua mahdollisimman hyvin. Ryhmähaastattelun nauhoittaminen saattaa tuottaa ongelmia, sillä ihmiset puhuvat usein toistensa päälle, jolloin äänestä on vaikeaa saada selvää. On myös tärkeää, että haastatteluiden litteroiminen eli tekstimuotoon muuttaminen suoritetaan mahdollisimman pian keskustelutilanteen jälkeen, jotta asiat ja puheenvuorot ovat vielä tuoreessa muistissa. (KvaliMotv, Hirsjärvi & Hurme 2001 mukaan, 61-63; Eskola & Suoranta 2000, 97-98 mukaan.)

Haastattelu on laadullinen menetelmä, ja esimerkiksi yhteiskuntatieteiden tutkimusmetodien professori Pertti Tötön mukaan laadullinen tutkimus ei pysty vastaamaan kysymykseen miksi. Syy-seuraus-suhteen todentamiseen tarvitaan aina tietoa ilmiöiden korrelaatiosta, ja sitä taas ei voi todeta ilman määrällistä tutkimusta. Jos määrälliset metodit unohdetaan, Tötön mukaan samalla hylätään varsinaisia syitä koskevat kysymykset. Ilman määrällisiä menetelmiä laadullinen tutkimus ei todista mitään tutkittujen erikoistapausten ulkopuolelta, vain esittää valistuneita yleistäviä oletuksia, hypoteeseja. (Ylioppilaslehti 1.12.2000.)

Yleensä tutkimuksissa hyödynnetään triangulaatiota eli käytetään sekä määrällisiä että laadullisia menetelmiä, jotta tulokset ovat luotettavammat. Opinnäytetyössä hyödynnettiin myös

aiempia tutkimuksia, joissa on käytetty määrällisiä menetelmiä. Kirjallisuuskatsauksessa haasteina on tähän opinnäytetyöhön sopivien tutkimusten tai muun kirjallisuuden löytäminen.

4.3 Aineiston analysointimenetelmät

Laadulliselle analyysille on tyypillistä, että aineistoa analysoidaan samanaikaisesti aineiston keruun ja tulkinnan kanssa, ja eroaa tässä suhteessa määrällisestä analyysistä. Tässä tutkimuksessa aineisto puretaan ja koodataan, jonka jälkeen edetään analyysiin. Laadullisessa analyysissa analyysi voi alkaa haastattelutilanteesta eli tutkija voi haastatellessaan tehdä havaintoja ilmiöstä. (Hirsjärvi & Hurme 2008, 136.) Esimerkiksi haastateltavien ilmeistä ja eleistä voi tehdä haastattelutilanteessa päätelmiä, mikä ei enää onnistu haastattelun jälkeen. Aineistoa analysoidaan myös lähellä aineistoa ja sen kontekstia eli laadullinen tutkimus säilyttää aineiston sanallisessa muodossa ja osittain alkuperäisessä sanallisessa muodossa. (Hirsjärvi & Hurme 2008, 136.) Litteroinnissa kannattaa siis säilyttää alkuperäinen ilmaisutapa.

Tutkija käyttää analysoinnissa induktiivista tai abduktiivista päättelyä. Induktiivinen päättely on aineistolähtöistä ja abduktiivisessa päättelyssä tutkijalla on valmiiksi jokin teoria, joka pyritään todentamaan aineiston avulla (Hirsjärvi & Hurme 2008, 136). Ei ole mahdollista käyttää pelkästään induktiivista päättelyä aineiston analysoinnissa, koska induktiivinen päättely perustuu havaintojen kuvaamiseen ilman ennakkokäsityksiä tutkittavasta ilmiöstä (KvaliMotv, Tuomi & Sarajärvi 2002, 98 mukaan). Abduktiivinen päättely on taas teoriasidonnainen lähestymistapa (KvaliMotv, Tuomi & Sarajärvi 2002, 99 mukaan), jolloin teoriasta haetaan selityksiä tulkintojen tueksi (KvaliMotv, Eskola 2001a mukaan). Joka tapauksessa analyysitekniikat ovat moninaisia laadullisessa tutkimuksessa ja standardoituja tekniikoita on vähän.

Haastatteluaineiston analysointiin olen ottanut mallia Hirsjärven ja Hurmeen Tutkimushaastattelu-kirjasta. Haastatteluaineiston purkamisessa, analysoinnissa ja tulkinnassa on useita vaiheita. Kaaviossa on kuvattu yksinkertaistettuna jokainen vaihe.

Kuvio 4: Haastatteluaineiston analyysi ja tulkinta (mukaillen Hirsjärvi & Hurme 2008, 135-152)

Aineiston luokittelu ei ole analyysin lopullinen tavoite, vaan välivaihe analyysin rakentamisessa. Aineiston yhdistelyllä pyritään löytämään samankaltaisuuksia ja eroavaisuuksia sekä säännönmukaisuutta (Hirsjärvi & Hurme 2008, 149). Kirjallisuuskatsauksessa aineiston analyysin lähtökohta on se, että vastataan selkeään kysymykseen, ja opinnäytetyössä käytetään analyysimenetelmänä kuvailevaa kirjallisuuskatsausta. Kuvaileva kirjallisuuskatsaus voidaan tiivistää niin, että se on perinteinen kirjallisuuskatsaus. Se on yleisin kirjallisuuskatsauksen perustyyppi, jossa ei ole tiukkoja tarkkoja sääntöjä ja siinä pyritään kuvaamaan ilmiön ominaisuuksia laajasti (Salminen 2011, 6). Kirjallisuuskatsauksen analyysi on luonteeltaan myös laadullinen analyysi.

5 Opinnäytetyön prosessi

Opinnäytetyön prosessi jakautui useaan työvaiheeseen. Opinnäytetyön toteutusprosessiin on liittynyt jonkin verran haasteita. Suurin haaste oli itse tutkimuskysymyksen muotoilu ja menetelmien valinta. Tätä ennen oli epävarmaa, voiko aiheesta tehdä opinnäytetyötä, koska lupaa verkkokoulutukselle ei vielä ollut saatu. Tämä vaikutti myös opinnäytetyöprosessin aikatauluun. Pohdin ensin, että aihe liittyisi pelkästään siihen, miten tietoturvaosaamista voidaan kehittää tai miten tietoisuutta voidaan lisätä, mutta näitä asioita on käsitelty hyvin paljon eri tutkimuksissa eikä tietoisuuden lisääminen vaikuta suoraan käyttäytymiseen. Organisaation

olisi hyvä huomioida erilaiset ihmisen käyttäytymiseen vaikuttavat tekijät ja miten ne vaikuttavat toisiinsa. Lopputulema oli se, että päädyin tutkimaan tietoisuuden, motivaation ja käyttäytymisen välistä suhdetta tietoturvanäkökulmasta. Pisin vaihe oli opinnäytetyön kirjoittaminen. Vaikeinta oli päättää, mitkä tutkimukset ja motivaatioteoriat ovat olennaisia opinnäytetyön kannalta. Tavoitteena on kuitenkin esittää ja julkaista valmis työ syksyllä 2021.

Lähtökohta oli verkkokurssin suunnittelu, joka alkoi tammikuussa 2018 ja päättyi huhtikuussa 2018. OP Ryhmässä pakollisen verkkokurssin suunnitteluun ja toteutukseen liittyy useita eri vaiheita, jotta voidaan varmistaa, että sisältö on olennaista OP Ryhmän kannalta ja se sopii tyyliltään OP Ryhmän brändiin. Verkkokurssin suunnitteluun liittyi myös viestinnän suunnittelu.

Vahti-ohjeiden mukaan organisaation omia koulutus- ja ohjeaineistoja laadittaessa on suositeltavaa noudattaa seuraavia kriteerejä ja laadullisia ominaisuuksia, jotka ovat mielestäni hyvä lähtökohta tietoturvakoulutusten suunnittelussa verkkokurssin kohderyhmää ajatellen. Ensinnäkin ohjeiden ja koulutusten tietosisällön on oltava linjassa sekä lainsäädännön että VAHTI-ohjeiden kanssa ja ohje- ja koulutusaineiston on oltava helppolukuista. Ohje on ymmärrettävä kaikille työntekijöille työtehtävästä riippumatta ja kirjoitustyylin on oltava lukijalle läheinen. Tätä tavoitellaan muun muassa sinuttelulla ja opastamisella. Ohjeen on herätettävä käyttäjät ajattelemaan tietoturva-asioita omassa työssään. (Vahti-ohjeet 2009.)

Tiedon luokittelu ja käsittely ei ole erillisenä koulutuksena pakollinen, mutta on osana joka toinen vuosi pakollisena olevaa tietoturvakoulutusta. Verkkokurssin pakollisuus tulee perustua alan lainsäädännön tai standardien vaatimuksiin tai asiakkaiden vaatimuksiin. Perusteluina on käytetty muun muassa liikesalaisuuslakia. 15.8.2018 voimaan astunut Liikesalaisuuslaki kattaa elinkeinotoimintaan liittyvien liikesalaisuuksien sekä teknisten ohjeiden suojan (Turun kauppakamari 10.8.2018). Turun kauppakamarin (10.8.2018) sivustolla määritetään liikesalaisuus seuraavanlaisesti:

”Liikesalaisuudella tarkoitetaan tietoa, joka ei ole kokonaisuutena tai osiensa täsmällisenä kokoonpanona ja yhdistelmänä tällaisia tietoja tavanomaisesti käsitteleville henkilöille yleisesti tunnettua tai helposti selville saatavissa, ja jolla edellä mainittujen ominaisuuksien vuoksi on taloudellista arvoa elinkeinotoiminnassa, ja jonka laillinen haltija on ryhtynyt kohtuullisiin toimenpiteisiin sen suojaamiseksi. -- Liikesalaisuus taas voi koostua asiakas- tai hinnoittelutiedoista, liiketoimintamalleista tai strategioista. Usein liikesalaisuus sisältää sekä teknisiä että kaupallisia tietoja yhdessä. Liikesalaisuuden haltijalta edellytetään toimenpiteitä liikesalaisuuden suojaamiseksi.”

Henkilöstön tulisi osata tunnistaa, mitkä tiedot voidaan lukea liikesalaisuudeksi. Koulutuksen tavoite on se, että työntekijä osaa myös itsenäisesti arvioida tiedon sensitiivisyyttä ja määritellä sille luokan.

Verkkokurssin sisältö suunniteltiin seuraavaksi. Lisäksi ulkoasun eli verkkokurssissa käytettävien kuvien, tekstin ja muotojen täytyy sopia brändiin. Tässä vaiheessa suunnittelua pidettiin workshop, johon osallistui kaksi henkilöä arvioimaan suunnitelmaa. Verkkokurssista laadittiin alustava versio PowerPoint –tiedostona turvallisuusjohtajalle, ja versio läpikäytiin tunnin mittaisessa palaverissa. Tässä vaiheessa toteutukselle myönnettiin rahoitus. Tärkeää verkkokurssin toteutuksessa oli viestinnän rooli. Viestinnän tarkoitus oli varmistaa, että mahdollisimman moni tietää kurssin olemassaolosta, ja tutustuu ohjeisiin. Erilaisia viestintätapoja mietittiin pitkään, ja lopulta päädyttiin uutiseen ja videoon, joka sisälsi näytellyn kohtauksen. Tavoite oli myös se, että henkilöstö kiinnostuisi tietoturvallisuudesta. Lopuksi valmis suunnitelma esiteltiin yhteistyökumppanille, joka sitten toteutti varsinaisen kurssin. Verkkokurssi ja ohjeet julkaistiin kesäkuussa 2018. Tämän lisäksi julkaistiin myös videon sisältävä uutinen intraan.

Varsinaisessa opinnäytetyöprosessissa ensimmäinen vaihe oli suunnitelman laatiminen ja esittäminen seminaarissa. Tämän jälkeen alkoi haastattelun toteutuksen suunnittelu ja lähetettiin kutsut potentiaalisille haastateltaville. Haastattelu toteutettiin marraskuussa 2018. Haastattelu otetiin nauhalle, joka litteroitiin eli kirjoitin dokumenttiin sen, mitä osallistujat keskustelivat. Ryhmähaastattelussa keskusteltiin verkkokurssin sisällöstä, tietoturvaohjeistuksesta sekä henkilöstön toimintatavoista. Haastatteluaineiston perusteella tehdään päätelmiä, mitkä asiat verkkokurssissa ja muuten vaikuttavat siihen, noudattaako henkilöstö tietoturvaohjeistuksia. Verkkokurssi voidaan arvioida kolmella eri tasolla:

Taso	Tarkoitus	Esimerkkimetodi
Johtotason arviointi	Tarkistetaan, että koulutusmateriaalissa käsitellään aihetta tarkoituksenmukaisesti eikä materiaalissa ole asiavirheitä. Varmistetaan, että henkilöstö suorittaa kurssin	Viestintä, suoritusten määrän seuranta, turvallisuusjohtaja tarkistaa materiaalin
Henkilöstötason arviointi	Koulutusmateriaalissa esitetyt asiat on ymmärretty, ja koulutus arvioidaan positiivisesti	Palautteet, haastattelut, kyselyt
Vaikuttavuustason arviointi	Vaikuttiko koulutus käyttäytymiseen eli toimiiko henkilöstö turvallisemmin	Auditointi, tietoturvarikkomusten vähentyminen, seuranta

Taulukko 2: Koulutuksen arvioinnin tasot (mukaillen Roper, ym. 2006, 222)

Johtotason arviointi on tehty ennen verkkokurssin julkaisua. Opinnäytetyössä keskitytään tason 2 eli henkilöstötason arviointiin, koska vaikuttavuustason arviointia varten ei ole ollut tarpeeksi pitkää seuranta-aikaa.

Kaikille verkkokurssin suorittaneille lähetettiin sähköposti, jossa heitä pyydettiin osallistumaan ryhmähaastatteluun. Tavoite haastateltavien määrälle oli 4-7, ja ilmoittautuneita oli 4. Ryhmähaastattelu järjestettiin OP Vallilan pääkonttorilla 9.11.2018 ja kesti noin tunnin. Haastateltavat olivat tietoisia siitä, että haastattelu nauhoitetaan, ja jokainen antoi suostumuksensa tähän. Osallistuminen oli myös vapaaehtoista eikä nimiä mainita opinnäytetyössä. Anonymiteetin säilyminen on tutkimuksessa tärkeää, jotta osallistujat vastaisivat kysymyksiin mahdollisimman todenmukaisesti ja uskaltaisivat ilmaista mielipiteitään.

Seuraavissa luvuissa käsitellään haastatteluaineiston ja muiden aineistojen analysointia ja tuloksia.

6 Aineiston analysointi

Äänitetty haastattelu litteroitiin eli muutettiin tekstimuotoon. Litterointi voidaan tehdä kokohaastatteludialogista tai valikoiden (Hirsjärvi & Hurme 2008, 138), ja tässä tapauksessa kysymys on puolistrukturoidusta haastattelusta, joten litterointi tehtiin kysyttyjen kysymysten perusteella. Litteroinnissa ei myöskään eroteltu puhujia toisistaan, jotta heitä ei tunnisteta. Litteroinnin jälkeen haastatteluaineisto analysoitiin, ja lähestymistapana on laadullinen sisältöanalyysi.

Aloitin haastatteluaineiston analyysin värikoodaamalla tekstistä kohtia, jotka mielestäni liittyivät toisiinsa. Tässä vaiheessa erottui neljä luokkaa:

Verkkokurssin sisältö ja ominaisuudet

Käyttäytyminen

Tietoisuus/osaaminen

Viestintä

Värikoodauksen jälkeen kokosin haastateltavien vastaukset Excel-taulukkoon, ja jokaisen vastauksen viereiseen sarakkeeseen kirjoitin pelkistetyn ilmauksen tai tulkinnan siitä, mitä on sanottu. Kun kaikki vastaukset oli tulkittu, jokainen ilmaus luokiteltiin. Tässä vaiheessa luokkia erottui enemmän kuin haastatteluaineistoa luettaessa. Luokkia löytyi yhteensä 10. Aiemman neljän luokan lisäksi löytyi ajankäytön haasteet, muisti, keskittymiskyky, arvot, asenteet ja vaikutukset omaan työhön.

Taulukko 3: Esimerkki 1

Ilmaisu	Pelkistetty ilmaisu / tutkijan tulkinta
konttoreissa mukavampi ottaa asiakas. Jos suorittaa puolentoista tunnin kurssia niin tämä ei ole mahdollista	Vaikea ottaa asiakkaita jos suorittaa puolentoista tunnin kurssia

Taulukko 4: Esimerkki 2

Ilmaisu	Pelkistetty ilmaisu / tutkijan tulkinta	Luokka
konttoreissa mukavampi ottaa asiakas. Jos suorittaa puolentoista tunnin kurssia niin tämä ei ole mahdollista	Vaikea ottaa asiakkaita jos suorittaa puolentoista tunnin kurssia	Ajankäytön haasteet

Aineiston analysoinnin ja tulkinnan jälkeen hahmottelin opinnäytetyön varsinaisia tuloksia. Tämän opinnäytetyön kannalta tämä tarkoittaa sitä, että vertailtiin haastatteluaineistoa muihin opinnäytetyössä käytettyihin aineistoihin. Tätä ennen keräsin opinnäytetyön tietoperusta-osiossa esitellyistä motivaatioteorioista ja tutkimuksista olennaisimmat ja toistuvat tekijät. Oletus on se, että löytyy samoja tekijöitä sekä eroja. Vertailun apuna oli taulukko, johon kokosin analyysin perusteella löytyneet tekijät, ja tiedon löytyykö tekijät kirjallisuuskatsauksen aineistosta vai haastatteluaineistosta. Eri tekijät voivat myös liittyä toisiinsa, ja pyrin avaamaan näitä yhteyksiä tuloksissa.

7 Tulokset

Tämän luvun tarkoituksena on esitellä opinnäytetyön tuloksia. Kirjallisuuskatsauksen ja ryhmähaastattelun tulosten pitäisi vastata kysymykseen ”Mitkä tekijät vaikuttavat tietoturvakäyttäytymiseen?”

Tutkimuksen tarkoituksena on myös vertailla eri tiedonkeruumenetelmien tuloksia keskenään. Opinnäytetyössä käytetyt motivaatioteoriat selittävät motivaation syntyä ja käyttäytymistä, joten oletetaan, että haastateltavat toimivat suunnilleen näiden mallien mukaisesti. Haastateltavat eivät välttämättä tunne psykologiassa käytettyjä käsitteitä tai teorioita ja otan tämän huomioon aineiston analysoinnissa. Jouduin myös tekemään omia tulkintoja, koska suullinen asioiden ilmaisu ei ole aina selkeää.

7.1 Ryhmähaastattelun tulokset

Tietoisuuteen ja osaamiseen liittyy **ajankäytön haasteet ja keskittymiskyky**, koska opiskeluun pitää varata aikaa ja materiaaliin pitää keskittyä, jotta oppiminen on mahdollista. Ajankäyttö ja keskittymiskyky liittyvät myös verkkokurssin sisältöön ja ominaisuuksiin siltä osin, että lyhyen verkkokurssin suorittamiseen on helpompi varata aikaa ja mielenkiinto aiheeseen säilyy, jolloin asenne tietoturvaohjeistuksia kohtaan on parempi.

Vastauksissa, jotka liittyivät **verkkokurssin sisältöön ja ominaisuuksiin** korostui selkeys, nopeus ja se, että verkkokurssissa toistettiin riittävästi olennaisia asioita. Haastateltavat pitivät siitä, että asia oli esitetty lyhyesti ja ytimekkäästi, ja verkkokurssin visuaalinen ulkoasu miellytti haastateltavia. Aineistosta käy ilmi, että pitkäkestoisten verkkokurssien suorittaminen voi olla haasteellista, koska keskittymiskyky ei välttämättä riitä tai verkkokurssia ei ehditä suorittamaan töiden takia. Esimerkiksi asiakaspalvelutehtävissä työskentelevät joutuvat erikseen varaamaan ajan kurssin suorittamiselle. Aineistosta erottui myös se, että haastateltavilla oli paremmat ennakkoasenteet, kun kurssi on kestoltaan lyhyt ja mielenkiinto aiheeseen säilyi.

Haastateltavilta kysyttiin mielipiteitä myös verkkokurssin tehtävistä, ja yksi oli sitä mieltä, että tehtävät eivät olleet liian helppoja, mutta eivät myöskään liian vaikeita. Suurin osa kuitenkin vastasi, ettei muista millaisia tehtäviä kurssissa oli. Aineiston perusteella haastateltavat eivät aina **muistaneet** noudattaa tietoturvaohjeistuksia, ja **unohtaminen** vaikutti olevan merkittävin käyttäytymiseen vaikuttava tekijä. Haastateltavat pitivät tärkeänä sitä, että verkkokurssi suoritetaan säännöllisin väliajoin, jotta ohjeistuksia muistetaan noudattaa.

Haastateltavat suhtautuivat tietoturvallisuuteen yleisesti ottaen positiivisesti, mutta tiedon luokittelu -ohjeistusta myös jossain määrin **kyseenalaistettiin** vetoamalla siihen, ettei tule koskaan jakamaan salaista tietoa ja tieto löytyy vain omalta koneelta. Sääntöjä pidettiin turhina, jos koettiin, ettei asia **vaikuta omaan työhön**. Pääosin asiaa pidettiin **tärkeänä** ja tiedostettiin, miten tietoa pitää käsitellä ja osattiin soveltaa ohjeita omaan työhön. Uskottiin myös siihen, että muu henkilöstö pitää aihetta tärkeänä. Haastateltavat kuitenkin myönsivät, ettei tietoisuus aina siirry käytännön toimintaan, jos toimintamalli ei ole vielä osa omaa rutiinia. Haastattelussa tuli myös ilmi, ettei henkilöstö aina myöskään puuttunut tilanteisiin, joissa toimittiin väärin tai ohjeiden vastaisesti ja tämä kertoo henkilöstön **asenteista**.

Haastattelussa keskusteltiin myös **viestinnästä** ja sen tärkeydestä. Osa oli huomannut intran uutisen verkkokurssista, mutta monet luottavat esimiehiin tiedon jakamisessa ja saivat tiedon verkkokurssista ja uusista ohjeista sähköpostitse. Sähköpostiin verrattuna etu oli kuitenkin se, että asia voidaan saada vaikuttamaan kiinnostavalta.

7.2 Kirjallisuuskatsauksen tulokset

Opinnäytetyöhön poimituissa motivaatioteorioissa nousi esille henkilöstön **asenteet**, **palkkiot** ja **rangaistukset**, **tarpeet** sekä **tietoisuus.**

Tietoturvakäyttäytymiseen liittyy erilaisia **asenteita**, jota kuvailtiin luvussa 3. Tärkeää on se, miten johto suhtautuu tietoturvallisuuteen eli johdon pitäisi näyttää esimerkkiä hyvistä toimintatavoista. Tietoturva-asiantuntijoiden tulisi auttaa ja neuvoa, ei pelkästään toimia auktoriteettina.

Maslowin tarvehierarkia esittää, että ihmisten **tarpeilla** on tietty järjestys; jos alemman tason tarve on täyttämättä, ihminen ei yleensä pyri tyydyttämään ylemmän tason tarpeita. Alimmalla tasolla ovat fysiologiset tarpeet eli esim. nälkä ja jano. Voisiko lounaan syömättä jättäminen vaikuttaa motivaatioon? Ehkä, mutta teorian mukaan ihminen voi myös ohittaa alemman tarpeen, koska teorian mukaan ihminen tavoittelee aina korkeampaa tarvetasoa. Hierarkiassa seuraavana on turvallisuus ja sosiaaliset tarpeet ja niiden jälkeen arvostus sekä itsensä toteuttaminen. Turvallisuudella tässä yhteydessä tarkoitetaan esim. auktoriteetteihin luottamista ja totuttuun turvautumista. Vaikka tarpeiden järjestys ja niiden luokittelu on kiistanalaista, koska tarpeet ovat yksilöllisiä, vaikuttavat ne tietoturvakäyttäytymiseen.

Turvallisuuden tarve voi vaikuttaa siten, että henkilöstö on tottunut toimimaan tietyllä tavalla ja vanhoista tottumuksista on vaikea luopua. Toisaalta henkilöstö voi luottaa esimieheen ja turvallisuuden tarve tyydytetään esimiehen ohjeita noudattamalla. **Sosiaalisiin tarpeisiin** kuuluu työyhteisö ja yhteenkuuluvuuden tunne. Jos kaikki noudattavat samoja sääntöjä, yksilön on helpompi mennä joukon mukana. **Arvostuksen tarpeeseen** kuuluu se, että yksilö pyrkii erottumaan joukosta. Henkilöstön jäseniä voidaan palkita esimerkillisestä toiminnasta. **Itsensä toteuttamisen tarpeessa** yksilö näkee, että hänellä on kyky ja mahdollisuus saavuttaa päämääränsä. Päämäärät voivat liittyä myös tietoturvakäyttäytymiseen.

Odotusarvoteorian mukaan **palkkio** ei välttämättä tarkoita aineellista hyötyä, vaan palkkiolla voidaan tarkoittaa myös ihailua tai kehua. Monet pyrkivät noudattamaan ohjeita rangaistuksen pelossa, mutta motivaatio et välttämättä riitä tietoturvaongelmien ilmoittamiseen. Odotusarvoteoria ottaa huomioon, miten yksilöt arvioivat vaivannäköä suhteessa palkkioon sekä toteutuuko luvatut palkkiot ja rangaistukset. Organisaation tulee olla valmis toteuttamaan annetut lupaukset ja tehdä tietoturvallisesta toiminnasta helpompaa.

Suojelumotivaatiossa nostetaan esille **”palkinnot”** tietoturvapolitiikan noudattamatta jättämisestä. Ajan säästö on yksi näistä, joten organisaatiossa kannattaa tutkia, paljon aikaa tietoturvapolitiikan mukaiset käytännöt vievät ja onko prosesseissa kehityskohteita. Suojelumotivaatioteoriaan liittyvässä tutkimuksessa yksi skenaario oli salasanojen jakaminen. Miksi sala-

sanoja jaetaan? Yksi mahdollinen selitys on se, että valtuuksien saamisessa kestää kauan. Pahimmassa tapauksessa työt seisovat puuttuvien salasanojen takia, ja henkilöstö arvioi salasanan jakamisen kollegan kanssa pienemmäksi uhaksi kuin tietoturvapolitiikan noudattamatta jättämisen.

Suojelumotivaatioon liittyvän tutkimuksen Motivating IS security compliance: Insights from Habit and Protection Motivation Theory johtopäätöksissä todettiin, että työntekijöiden pitäisi pystyä tunnistaa tietoturvauhat ja -riskit. Tämän lisäksi todettiin, että on tärkeä kertoa henkilöstölle organisaatioon todennäköisesti kohdistuvista tietoturvauhkista tilanteissa, jolloin henkilöstö ei käytä tietoturvan teknisiä menetelmiä, ota tietoturvakäytäntöjä vakavasti tai noudata niitä. Toisin sanoen henkilöstön **tietoturvatietoisuus** vaikuttaa tietoturvakäyttäytymiseen. Henkilöstön pitää olla tietoinen riskeistä ja turvallisista toimintatavoista, jotta he osaavat käyttäytyä tietoturvallisesti ja organisaatioiden on varmistettava, että tietoturvakäytäntöjä ja -menettelyjä ei ole vaikea käyttää.

7.3 Tulosten vertailu

Kirjallisuuskatsauksen ja haastattelun aineistojen väliltä löytyi yhtäläisyyksiä. Vertailussa otan huomioon sen, että vaikka tekijää x ei mainita aiemmissa tutkimuksissa tai toisinpäin, eri tekijät voivat vaikuttaa toisiinsa. Seuraavassa taulukossa on eritelty haastatteluaineistosta ja muusta aineistosta löytyneitä tekijöitä.

Taulukko 5: Tulosten vertailu

Tekijät	**Kirjallisuuskatsaus**	**Haastattelu**
Asenteet	Kyllä	Kyllä
Palkkiot ja rangaistukset	Kyllä	
Tarpeet	Kyllä	
Tietoisuus	Kyllä	Kyllä
Muisti		Kyllä
Keskittymiskyky		Kyllä
Verkkokurssin ominaisuudet		Kyllä
Ajankäytön haasteet		Kyllä

Vaikutukset omaan työhön		Kyllä
Viestintä		Kyllä
Arvot		Kyllä

Asenteet tulivat esille sekä kirjallisuuskatsauksen analysoinnissa että haastatteluaineiston analysoinnissa. Haastateltavien suhtautuminen tietoturvallisuuteen oli melko epäjohdonmukaista, välillä tietoturvallisuus oli tärkeää ja välillä ei. Haastattelussa nousi esille jossain määrin välttelevä tai apaattinen asenne tietoturvallisuutta kohtaan, esimerkiksi tilanteet, joissa henkilöstö ei aina puuttunut tilanteisiin, jossa toimittiin väärin tai ohjeiden vastaisesti. Kuitenkin haastateltavat vakuuttivat välittävänsä tietoturvallisuudesta, mikä osoittaa sen, että asiasta välittäminen ei automaattisesti tarkoita, että käytännössä toimitaan ohjeistuksen mukaisesti. Tähän todennäköisesti vaikuttaa se, ettei riskejä täysin tiedosteta ja aiempi tiedon puute, mitkä ovat korjattavissa olevia asioita.

Palkitseminen ei tullut esille haastattelussa, mutta haastateltavat myönsivät, että on helpompaa jättää joskus noudattamatta tietoturvaohjeistuksia, koska silloin säästää aikaa. Ajan säästämisen voisi kuitenkin tulkita palkinnoksi. Suojelumotivaatioteoriaan liittyvässä tutkimuksessa ihmiset näkevät ajan säästämisen hyötynä noudattamatta jättämisestä. **Rangaistukset** mainitaan osana motivaation ja käyttäytymisen perustaa. Yleensä ihmiset välttelevät toimintaa, joista seuraa rangaistus.

Tarpeet muodostavat pohjan motivaatiolle (esim. Maslowin tarvehierarkia -teoria**).** Haastatteluaineistossa kuitenkin erottui jossain määrin turvallisuuden tarve, esim. haastateltavat myönsivät, ettei tietoisuus tietoturvaohjeistuksista aina siirry käytännön toimintaan, jos toimintamalli ei ole osa omaa rutiinia. Rutiinit voivat lisätä turvallisuuden tunnetta, koska työntekijä pystyy ennakoimaan tulevaa paremmin ja uudet ohjeistukset voivat herättää epävarmuutta työntekijöissä.

Tietoisuus oli keskeinen aihe haastattelussa, koska verkkokurssin tarkoitus oli lisätä tietoturvatietoisuutta. Suojelumotivaatioteoriaan liittyvässä tutkimuksessa otettiin myös kantaa tietoisuuteen. Haastattelussa keskusteltiin myös **verkkokurssin ominaisuuksista**, **keskittymiskyvystä** ja **muistista.** Nämä tekijät vaikuttavat tietoturvatietoisuuteen. Verkkokurssin tulee olla sisällöltään ymmärrettävä koko henkilöstön näkökulmasta, esimerkiksi konttorin toimihenkilö ymmärtää tietoturvallisuuden eri näkökulmasta kuin tietoturva-asiantuntija. Jos verkkokurssi on liian pitkä, vaikeaselkoinen tai tehtävät ovat liian helppoja tai vaikeita, kurssin sisältöön ei jaksa keskittyä kunnolla. Kun asiat esitetään selkeästi, niiden muistaminen on helpompaa.

Lisäksi **viestintä, vaikutukset omaan työhön, ajankäytön haasteet ja arvot** vaikuttivat haastatteluaineiston perusteella tietoturvakäyttäytymiseen. Näistä ei suoraan mainittu muussa aineistossa. Arvojen osalta haastattelussa toistui se, että tietoturvallisuutta pidetään tärkeänä, mutta ei tullut selväksi, onko kyseessä haastateltavan oma arvomaailma vai organisaation.

8 Johtopäätökset

Tässä luvussa otetaan kantaa siihen, saavutettiinko tutkimuksen tavoitteet, pohditaan kehitysehdotuksia ja tulosten pohjalta potentiaalisia tutkimuksen kohteita/aiheita sekä arvioidaan opinnäytetyön tutkimuksen luotettavuutta.

8.1 Pohdinta

Opinnäytetyön tutkimuskysymys oli ”Mitkä tekijät vaikuttavat tietoturvakäyttäytymiseen?”. Opinnäytetyön aineistojen analysoinnin perusteella löytyi erilaisia tekijöitä, joista on kerrottu edellisessä luvussa. Opinnäytetyön tavoite on tältä osin saavutettu. Tulosten perusteella ei voi suoraan todeta, että koulutuksella voidaan vaikuttaa käyttäytymiseen, vaan tietoturvakäyttäytymiseen vaikuttavat myös muut tekijät. Koulutuksella voidaan kuitenkin korostaa hyviä toimintamalleja, jonka lisäksi organisaatiossa varmistetaan, että ohjeiden noudattaminen on käytännössä mahdollista eikä haittaa työntekoa.

Haastattelun perusteella verkkokurssi oli toteutettu onnistuneesti. Asia oli pyritty esittämään mahdollisimman yksinkertaisesti, ja verkkokurssista tehtiin tarkoituksella sen verran lyhyt, että sen suorittaminen on kaikille mahdollista työtehtävistä riippumatta. Tehtävissä oli myös pyritty ottamaan huomioon erilaiset työtehtävät yleisellä tasolla.

Motivaation kannalta on helpompaa välttää epätoivottua toimintaa kuin toimia tai muuttaa omia toimintamalleja. Tämän takia esimerkiksi epäkohtiin puuttuminen tai turvaluokan lisääminen dokumenttiin voi olla vaikeaa. Henkilöstön asenteet vaikuttavat paljon siihen, siirtyykö uusi toimintamalli käytännön tekemiseen. Haastattelun perusteella asenteissa tietoturvasääntöjä kohtaan henkilöstö kuuluu enimmäkseen siihen kategoriaan, jossa sääntöjä enimmäkseen noudatetaan, mutta tilanteisiin ei aina haluta tai osata puuttua. Luvussa 3 esiteltiin motivaatioteorioita, joissa käsiteltiin palkitsemista motivaatiotekijänä. Tämä ei tullut esille haastattelussa, mutta palkkion voi ymmärtää myös abstraktimmin esim. ajan säästö. Jos henkilöstö kokee, että uudet toimintamallit vievät aikaa muulta työltä, on helpompaa pysyä vanhassa toimintamallissa.

Tutkimuksen toteutusvaiheessa ja sen jälkeen heräsi monenlaisia ajatuksia. Ensinnäkin tietoturvatietoisuuden rooli siinä, siirtyykö opittu asia käytännön tekemiseen, on vähän pienempi kuin mitä aiemmin luulin. Huomaan tämän asian myös omassa toiminnassani. Tiedostan, miksi

ohjeistuksia on tärkeää noudattaa, mutta jos ohjeistukset 1) ovat epäkäytännöllisiä 2) vaikeuttavat joustavaa päätöksentekoa 3) estävät tavoitteen saavuttamisen, niihin on helppo suhtautua negatiivisesti tai vähättelevästi. Ajatustasolla tietoturvallisuutta pidetään tärkeänä, mutta kuitenkin irrallisena omasta arjesta. Haastateltavat pitivät verkkokurssista ja pitivät asiaa tärkeänä, mutta ymmärrys siitä, miten uusi tieto sovelletaan omaan työhön, vaihteli.

8.2 Kehittämisehdotukset ja jatkotutkimukset

Tutkimuksessa tuli ilmi useita tekijöitä, jotka vaikuttavat tietoturvakäyttäytymiseen ja nämä tekijät kannattaa ottaa huomioon tulevaisuudessa, kun suunnitellaan verkkokursseja tai pohditaan, miten henkilöstö saadaan noudattamaan ohjeistuksia.

Ensiksi organisaation tulisi varmistaa, että henkilöstö tunnistaa tietoturvauhat ja riskit, ja että tietoturvakäytäntöjä ja -menettelyjä ei ole vaikeaa soveltaa omassa työssä. Toiseksi haastateltavien näkökulmasta unohtaminen oli merkittävä syy siihen, miksi ohjeistuksia ei aina noudateta ja tähän voidaan vaikuttaa sillä, että kurssi suoritetaan säännöllisin väliajoin. Voidaan myös järjestää tietoturvateemaviikkoja, joiden tarkoitus on muistuttaa olemassa olevista ohjeista, jotka koskevat tiedon käsittelyä. Unohtamisen lisäksi keskittyminen koettiin vaikeaksi, jos verkkokurssi on liian pitkä tai vaikeaselkoinen. Ajallisesti lyhyitä kursseja pidettiin parempina, koska niihin ei tarvitse varata erikseen aikaa eikä keskeytysten todennäköisyys on pienempi. Kolmanneksi olisi myös hyvä pohtia, miten tietoturvallisuudesta viestitään, missä kanavissa ja kenelle kohdennetaan, jotta viesti sisäistetään ja tavoittaa mahdollisimman monta henkilöä. Uutisten ja sähköpostien lisäksi esimerkiksi tiimipalavereissa olisi hyvä läpikäydä ohjeistukset muiden ajankohtaisten asioiden lisäksi.

Haastattelussa kukaan ei ottanut puheeksi palkitsemista, ja se voi myös kertoa siitä, että tietoturvallisuutta pidetään välttämättömänä pahana. Palkitseminen ja kiittäminen henkilökohtaisesti proaktiivisesta toiminnasta voisi motivoida henkilöstöä toimimaan turvallisemmin ja puuttumaan epäkohtiin.

Vaikuttavuustason arviointia ei opinnäytetyössä käsitelty aiemmassa luvussa mainitun seuranta-ajan puuttumisen takia. Vaikka tietoturvarikkomukset olisivat vähentyneet, suoraa yhteyttä sen ja koulutuksen välille on vaikeaa vetää, koska asiaan vaikuttaa monet muutkin tekijät. Jatkotutkimus voi kuitenkin liittyä siihen, toimiiko henkilöstö käytännössä uuden toimintamallin mukaisesti.

8.3 Luotettavuuden arviointi

Laadullisen tutkimuksen luotettavuuden arviointiin ei ole yksiselitteistä ohjeistusta. Tutkimuksen tarkoitus ja tutkittava kohde pitäisi kuvata riittävän tarkasti, jotta lukija ymmärtää,

mitä tarkastellaan ja miksi (Tuomi & Sarajärvi 2018, 162-163). Opinnäytetyössä pyrin selittämään tarkasti tutkimuksen lähtökohdan, mitä toteutuksen aikana tapahtui ja miten tulkitsen aineistoja. Esimerkiksi tulokset osiossa on tärkeää avata tulkintoja tutkijan ja haastattelijan näkökulmasta.

Luotettavuutta voidaan arvioida reliabiliteetin ja validiteetin kannalta, mutta näitä mittareita käytetään yleensä määrällisten tutkimusten arvioinnissa. Reliabiliteetti tarkoittaa mittaustuloksen toistettavuutta ja validiteetti on hyvä silloin, kun tutkimuksen kohderyhmä ja kysymykset ovat oikeat. Validiteetin arviointi liittyy siihen, kuinka hyvin tutkimusote ja käytetyt menetelmät vastaavat sitä ilmiötä, jota tutkitaan. (Hiltunen, 18.2.2009.) En kuitenkaan arvioi opinnäytetyön reliabiliteettia, koska käytin vain laadullisia menetelmiä. Esimerkiksi haastattelu oli luonteeltaan puolistrukturoitu ja kysymykset olivat avoimia, joten tulokset vaihtelevat, jos tutkimuksen toistaa. Validiteetin osalta käytetyt menetelmät soveltuivat ilmiön tutkimiseen ja sain vastauksia tutkimuskysymykseen.

Opinnäytetyön tutkimussuuntaukseksi valikoitui laadullinen tutkimus ja tarkemmin toimintatutkimus. Tutkimusongelma ohjasi menetelmien valintaa ja valitsin tiedonkeruumenetelmiksi haastattelun ja kirjallisuuskatsauksen. Menetelmiä käyttämällä pyrin löytämään vastauksia tutkimuskysymyksiin ja niitä myös löytyi. Hirsjärven ja Hurmeen mukaan haastatteluaineistoihin perustuvissa laadullisissa analyyseissa tutkijan pyrkimyksenä on päätyä onnistuneisiin tulkintoihin, ja tulkintaa voidaan tehdä useista näkökulmista. Onnistuneen tulkinnan tärkein kriteeri on se, että myös lukija voi löytää tekstistä ne asiat, jotka tutkijakin löysi riippumatta näkökulmasta. (Hirsjärvi & Hurme 2008, 151.) Tein analyysin aineistolähtöisesti, joten lukijan pitäisi löytää haastatteluaineistosta (liitteet) ja kirjallisuuskatsauksessa käytetystä aineistosta (motivaatioteoriat) samat tekijät, jotka on kuvattu tuloksissa.

Motivaatioteorioita ja niihin liittyviä tutkimuksia on todella paljon, joten valikoin tutkimukseen sellaisia tutkimuslähteitä, jotka sopivat olivat aiheeltaan samankaltaisia kuin opinnäytetyöni aihe, esimerkiksi Niina Kinnusen Tietoturvaohjeistusten noudattamisen motivaatio, ja sen muuttuminen (2015), kirja Security Education, Awareness, and Training: From Theory to Practice (Carl Roper, Joseph Grau, and Lynn Fischer 2006) sekä Tejaswini Herathin ja H. Raghav Raon tutkimus Protection motivation and deterrence: A framework for security policy compliance in organisations. Tutkimuslähteitä olisi voinut käyttää enemmänkin laajemman kokonaiskuvan saamiseksi. Toisaalta haastattelu oli opinnäytetyössä pääosassa tiedonkeruumenetelmissä, koska olennaista oli henkilöstön näkökulma asiaan.

Lähteet

Painetut

Hirsjärvi S. & Hurme H. 2008. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Gaudeamus Helsinki University Press.

Ojasalo K., Moilanen T. & Ritalahti J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. WSOYpro Oy. 1-2. painos.

Roper C., Grau J. & Fischer L. 2006. Security Education, Awareness and Training: From Theory to Practice. Elsevier Inc. Oxford, UK.

Tuomi J. & Sarajärvi A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Kustanneosakeyhtiö Tammi.

Sähköiset

Bulgurc, B., Cavusoglu H. & Benbasat I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. University of British Columbia. Viitattu 22.11.2021. https://www.researchgate.net/publication/220260207_Information_Security_Policy_Compliance_An_Empirical_Study_of_Rationality-Based_Beliefs_and_Information_Security_Awareness

Herath T. & Rao, H. 2009. Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems. Viitattu 22.11.2021. https://www.researchgate.net/publication/220393154_Protection_motivation_and_deterrence_A_framework_for_security_policy_compliance_in_organisations

Hiissa P. Verkkokurssien 20 huimaa hyötyä! Digivallankumous. Viitattu 23.4.2019. https://www.digivallankumous.fi/verkkokurssit/

Hiltunen, L. Validiteetti ja reliabiliteetti. 18.2.2009. Jyväskylän yliopisto. Viitattu 22.11.2021. http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ja_reliabiliteetti.pdf

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 Institute. Viitattu 22.11.2021. https://www.researchgate.net/publication/263103781_Managing_Employee_Compliance_with_Information_Security_Policies_The_Critical_Role_of_Top_Management_and_Organizational_Culture

© International Chamber of Commerce (ICC). Keskuskauppakamari. 2016. ICC Cyber security guide for business. Tietoturvaopas yrityksille. Viitattu 22.11.2021. https://kauppakamari.fi/hankkeet/julkaisut/tietoturvaopas-yrityksille/

JAMK. Opinnäytetyön ohjaajan käsikirja. Kirjallisuuskatsaukset. Viitattu 24.4.2019. https://oppimateriaalit.jamk.fi/yamk-kasikirja/kirjallisuuskatsaukset/

Jyväskylän yliopisto. Laadullinen analyysi. Koppa. Viitattu 10.4.2019. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysi-menetelmat/laadullinen-analyysi

Kinnunen N. 2015. Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen. Vaasan Yliopisto. Viitattu 10.3.2019. https://osuva.uwasa.fi/bitstream/handle/10024/7444/isbn_978-952-476-637-1.pdf?sequence=1

KvaliMotv. Aineisto- ja teorialähtöisyys. Viitattu 7.12.2021. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L2_3_2_3.html

KvaliMotv. Ryhmähaastattelu. Viitattu 7.3.2020. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_4.html

KvaliMotv. Teemahaastattelu. Viitattu 8.3.2019. https://www.fsd.uta.fi/menetelmaopetus/kvali/L6_3_2.html

Nieminen, I-M. 2.1.2015. OP-Pohjolaan kohdistui palvelunestohyökkäys – verkkopalvelut toimivat jälleen. Yle. Viitattu 8.3.2019. https://yle.fi/uutiset/3-7715863

OP. Strategia. Viitattu 8.3.2019. https://www.op.fi/op-ryhma/tietoa-ryhmasta/op-lyhyesti/strategia

OP. Ryhmärakenne. Viitattu 8.3.2019. https://www.op.fi/op-ryhma/tietoa-ryhmasta/hallinnointi/ryhmarakenne

Otavan opisto. Oppimateriaalit. Maslowin tarvehierarkia. Viitattu 19.4.2019. http://opinnot.internetix.fi/fi/materiaalit/ps/ps4/03_motivaation_emootioiden/04_3.4_maslowin_tarvehierarkia?C:D=gjtb.e7S7

Pahnila S., Siponen M. & Vance A. 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Elsevier. Viitattu 22.11.2021. https://www.researchgate.net/publication/257222773_Motivating_IS_security_compliance_Insights_from_Habit_and_Protection_Motivation_Theory

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Opetusjulkaisuja 62. Julkisjohtaminen 4. Vaasan yliopisto. Vaasa. Viitattu 7.11.2021. http://urn.fi/URN:ISBN:978-952-476-349-3

Silen M. 10.4.2017. Mitä on Compliance? Helsingin seudun kauppakamari. Viitattu 7.5.2019.

https://www.kauppakamarilehti.fi/index.php/neuvontapalvelut/mita-on-compliance/

Sommers, S. 1.12.2000. Ei se laatu vaan se määrä. Ylioppilaslehti. Viitattu 7.3.2020. https://ylioppilaslehti.fi/2000/12/ei-se-laatu-vaan-se-maara/

Turun kauppakamari. 10.8.2018. Uusi liikesalaisuuslaki pähkinänkuoressa. (Viitattu 8.3.2019) https://turunkauppakamari.fi/2018/08/10/uusi-liikesalaisuuslaki-pahkinankuoressa/

Valtiovarainministeriö. 08.10.2009. VAHTI 8/2008 Valtionhallinnon tietoturvasanasto. Viitattu 19.4.2019. https://www.vahtiohje.fi/web/guest/maaritelmat-t

Valtiovarainministeriö. 08.10.2009. Koulutusmateriaali. Koulutus- ja ohjeaineistolle asetettavat vaatimukset. Viitattu 19.4.2019. https://www.vahtiohje.fi/web/guest/koulutusmateriaali

Kuviot

Taulukot

Liitteet

Liite 1: Haastattelukysymykset

Kysymykset haastatteluun

- Mitä hyvää kurssissa oli?
- Mitä huonoa?
- Oliko kurssi sopivan pituinen?
- Ovatko tehtävät hyviä? Mikä niissä on hyvää tai huonoa?
- Onko tehtäviä liian vähän/paljon?

- Mitä kurssin olisi pitänyt sisältää mielestäsi?
- Kurssissa selitettiin tiedon luokittelun tärkeys. Muuttaisitko toimintatapojasi kurssissa annetuiden syiden perusteella ja jos et, miksi?
- Vaikuttiko kurssi siihen, miten ja mitä ajattelet tietoturvallisuudesta?
- Monet pitävät tiedon luokittelua turhana. Muuttuivatko ennakkokäsityksesi tiedon luokittelusta?

Liite 2: Haastattelu OP Vallilassa

Haastattelu

1. Ajankohta ja paikka
   9.11.2018 klo 15:30-16:30, OP Vallila
2. Eettisyys

   Osallistuminen edellyttää suostumusta seuraaviin ehtoihin:

- Keskustelu nauhoitetaan. Äänitallenne tuhotaan, kun aineisto on tekstimuodossa.
- Opinnäytetyössä ei mainita nimiä, ikää tai sukupuolta. Työstä/roolista OP:ssa mainitaan parilla sanalla.
- Haastateltaville näytetään, mitä yksilöintitietoja opinnäytetyöhön sisällytetään, ja niitä voidaan muuttaa haastateltavan pyynnöstä.
- Keskustelun sisältöä tai vastauksia ei yksilöidä.
- Kysymyksiin ei ole pakko vastata. Vastauksen voi lähettää myös sähköpostilla, mikäli muiden läsnäolo haittaa kysymykseen vastaamista.

3. Haastateltavat

   Henkilö A sijoitusasiantuntija
   Henkilö B asiantuntija, vahinkovakuutukset
   Henkilö C tiimipäällikkö, vahinkopalvelut
   Henkilö D assistentti, assistenttipalvelut

Liite 3: Litteroitu haastatteluaineisto

Mitä hyvää verkkokurssissa on?

- hyvässä mielessä selkeä luokittelu, näki heti mitkä ovat turvaluokat, toistuivat, ei jäänyt epäselvyyksiä, muut samaa mieltä
- lyhyt ja ytimekäs, ei muisteta mitä tarkalleen luki, mutta ydinasia jäänyt mieleen mikä tärkeää: mihin ollaan velvollisia sitoutumaan, verkkokurssi on hyvä jos tämä oivallus tulee
- Turvaluokat selkeästi esitetty, oli helppo ymmärtää, mihin dokumenttiin tulee mikäkin luokitus
- Myös se kenelle voi jakaa jäi mieleen, minkä tiedon voi jakaa kumppanille, jäi mieleen että puhuttu tieto on myös tietoa, täytyy miettiä missä tilanteissa voi puhua mitäkin, muut samaa mieltä

Oliko tarve verkkokurssille hyvin perusteltu?

- tuli vahvistamaan tietosuojan tärkeyttä, lainsäädäntö tiukentuu, yksilön oikeusturva paranee,
- ei muista, miten oli perusteltu, koska asia tuntui ajankohtaiselta, ei kiinnittänyt huomiota
- ei tarvitse opetella ulkoa, ydin asia tuli tärkeänä esiin, ei kuitenkaan vielä osa omaa rutiinia
- voi katsoa aina uudestaan, turvaporukat jes jes

Olisiko tehtäviä pitänyt olla enemmän?

- tehtäviä pitää myös olla, riippuu asiasta, joissain asioissa pitää olla, ettei verkkokurssia suorita juosten, tässä ei tarvitse olla enemmän tehtäviä, OP:ssa monenlaisia verkkokursseja, mutta tässä ei tarvita, koska on niin selkeä, muut samaa mieltä
- joihinkin kursseihin täytyy keskittyä paljon enemmän, ja jos tehtäviä ei ole, niin miettii, että mites tää meni, kyllä toimii tehokkaasti oppimisvälineenä, tehtävät eivät jääneet mieleen
- muut: ei meillekään
  luontevat tehtävät, joutui vähän miettimään,
- soljui yhden osion päätteeksi, tällainen mielikuva, mutta voin olla väärässä, ei turhauttanut, pääsee eteenpäin
- sujuva, nopea

Muistatteko luokat vielä?

- Organisaation ylin, jota me ei nähdä, ja sitten luottamuksellinen, sisäinen (kaikki yhdessä), julkinen (kaikki yhdessä), SSL
- kaikkia muita käyttänyt paitsi julkista,
- ei tuoteta julkista, jos itse tuottaa niin luottamuksellista ja jopa salainen,
- julkista tietoa ei tarvitse jakaa, koska löytyy verkkosivuilta
- sanon asiakkaalle, että löydät sen sieltä, itse ei sitoudu mihinkään väärään silloin
- selkeä yksinkertaiselle ihmiselle
- niin pitää olla, OP:n sisällä tieto aina luottamuksellista, salaista ja sisäistä
- omassa työssä vain sisäistä, valmistelut palavereihin ja muuta, salainen oman tiimin henkilöstöhallintoon liittyviä asioita, omalla koneella, joten ei jaksa kirjoittaa luokkia (muut myötäilevät)

Tuleeko ristiriita ymmärryksen ja käytännön toiminnan kanssa?

- unohtuu silloin, jos ajattelee ettei tule koskaan jakamaan tietoa
- onko tarve laittaa, jos on vain omalla koneella?
- entä jos näyttää jollekin?
- en tule koskaan jakamaan kenellekään, enkä näytä myöskään, korkeintaan esimiehelle nojoo silloin pitäisi olla salainen, oma esimies tuntee porukat ja pääsy samoihin tietoihin
- ei tule ajatelleeksi aina

  Entä jos siirtyy muihin tehtäviin tai toiseen yritykseen? Tiedot siirtyvät jossain kohtaa jollekin toiselle.

- riippuu dokumentin luonteesta, osa tiedosta vanhenee, joten sitä ei jaeta

Miksi päätitte suorittaa kurssin?

- kurssi oli pakollinen
- ei ollut merkitty pakolliseksi
- mun mielestä kaikki, jotka liittyvät tietoturvaan ovat pakollisia, olisin suorittanut vaikkei olisi ollut pakollinen, täytyy pysyä ajan tasalla
- tarjoiltu mielettömän hyvin, kuukauden kurssit olleet hyviä, kamalan tylsä ala (turvallisuus), pieni juttu mutta tarjoillaan kuukauden kurssina, kolahti
- en huomannut kuukauden kurssia, oliko intrassa, tuli meille jakeluna,
- mäki mietin et oliko intran sivuilla jossain vaiheessa. Esimiehet laittoivat erikseen sähköpostia, ei muista kumman huomasi ensin
- jos kurssi olisi tehty toisin, esimiehet olisi joutuneet pakottamaan suorittamaan kurssin

Vaikuttiko kurssi yleisesti siihen, miten ajattelette tietoturvallisuudesta? (tietoturva ei ole pelkkiä sääntöjä…)

- en itse koe, että ennakkokäsitykset muuttuivat. Tiedostin ennen kurssia, että tietoturvaan liittyy tarkkuus ja täytyy olla huolellinen, kurssi palautti mieleen sen, että on tullut muutoksia ja lisää tiukennuksia. Näitä asioita miettii pitkään tietoisesti, kun tekee töitä.
- Verkkokurssi on hyvä muistutus
- mielestäni nämä pitäisi suorittaa pakollisena joka vuosi, eikä joka toinen vuosi
- mietin ihan samaa, 2 vuotta on pitkä sykli
- mun mielestä olen suorittanut nämä joka vuosi
- toimii tosi hyvänä muistuttajana, esim. siinä, että jokaiseen dokumenttiin tulee merkitä turvaluokka
- se jää helposti tekemättä
- dokumenttipohjissa on hyvä olla valmiina luokat, helpompi lisätä luokka
- kuitenkin mielessä, ei sitä tahalteen jätä pois
- asia on mielessä koko ajan. Asiakas täytyy tunnistaa, koska asiakkaiden kanssa puhutaan usein puhelimessa vahinkoasioista. Omassa tekemisessä täytyy terästäytyä myös palavereiden ja paperisten dokumenttien osalta.

Vaikeuttaako tietoturvaohjeistusten suoraan noudattaminen työskentelyä?

- en osaa sanoa, kun jotenkin nytkin miettii niin tarkkaan

- en minäkään, ja äkkiseltään luulisi että ei kun muistan millä alalla ollaan, täällä pitää olla skarppina (muut samaa mieltä)

- tapaamisissa kumppanin kanssa pitää tietää keitä on tulossa ja mitä tietoa käsitellään, ei tule mukaan tyyppejä, joista ei tiedetä mitään.
- vaikka luokitusta ei olisi, tiedetään, miten toimitaan eli ohjeistus ei siltä osin vaikeuta työskentelyä
- en osaa sanoa, mutta menee aika pitkälti noin.

Ärsyttävätkö säännöt/ohjeet?

- pankissa täytyy tietää nämä asiat.
- varmasti jotkut kokevat ohjeet tällä tavoin.
- tämä on niin säännelty ala, luovuus ei voi kukkia täällä
- turhautuminen voi tulla siitä, että tääkin pitää muistaa merkitä, taas yksi asia joka pitää muistaa
- uskon, että kaikki ymmärtää tärkeyden

Soveltuuko kurssi kaikille työntekijöille? Ymmärtävätkö kaikki sisällön, tärkeyden jne.?

- iso merkitys siinä, miten asiat tarjoillaan, ja tässä onnistuttiin siinä. Kevyesti voi lähestyä painavaa asiaa
- kukaan ei ole ainakaan sanonut, että ärsyttää. Sopii myös konttoreissa suoritettavaksi
- riippuu mitä tekee. Jos ei ikinä tarvitse mitään paperilappua kirjoittaa, niin tuntuu turhalta
- toki voisi tehdä eri työntekijöitä varten yksityiskohtaisemman verkkokurssin sisällöllisesti, mutta tuoko se lisäarvoa? Menee liian tarkalle tasolle ja verkkokurssista voi tulla kuivakka. Jokainen ymmärtää, miten luokittelu vaikuttaa omaan työhön.
- tärkein on se, että ihmiset ymmärtävät

Seuraavaksi, katsotaan miltä verkkokurssi näyttää

- miellyttävä ääni puhujalla

Mitä jos tulevaisuudessa koko työpaikan tietoturva-verkkokurssi jaettaisiin 5-10 min pituisiin lyhyempiin kursseihin. Kumpi olisi parempi, se vai kaikki samassa, jolloin kesto on 1,5-2h?

- lyhyet pätkät siinä mielessä helpompia, puolentoista tunnin kurssiin tulee keskeytyksiä, ja joku asia menee ohi. Miten vireystaso pysyy yllä, ajatukset harhailevat työasioihin (muut samaa mieltä)
- Keskittyminen säilyy
- löytää helpommin ajan kurssin suorittamiselle
- mielenkiinto säilyy, asenne parempi

konttoreissa mukavampi ottaa asiakas. Jos suorittaa puolentoista tunnin kurssia niin tämä ei ole mahdollista

Miten verkkokoulutuksen voisi tulevaisuudessa järjestää, jos ottaa huomioon sen, että pakolliset verkkokurssit koskevat koko OP Ryhmää? Voisiko verkkokurssin lisäksi järjestää jotain?

- verkkokurssiin liittyvä tekeminen voisi olla yksi tapa oppia, ja jää tehokkaasti mieleen. Toteuttaminen voi olla raskasta, kun henkilöstökin on hajautunut niin isolle alueelle. Käytännön toteutus voi olla vaikeaa.
- virtuaalilasit on jo keksitty
- osastot tai tiimit voisivat ostaa ”escape room paketin”, joka liittyisi turvallisuuteen

Tuleeko mitään mieleen verkkokurssin ulkoasuun liittyen?

- ulkoasu on hyvä (muut samaa mieltä), houkuttelee yksinkertaisuudella, hyvät kuvat
- todella selkeä
- aiemmassa kurssissa oli näyteltyjä osioita, tää on vähän helpompi
- Näytellyissä osioissa näytettiin, miten vierailija otetaan vastaan, ja vierailijaa ei saa jättää yksin
- Op:ssa oltiin testattu sitä, kuinka vapaasti rakennuksessa pääsee liikkumaan ilman kulkuoikeuksia niin ettei jää kiinni. Oli päässyt sellaisiin paikkoihin, joihin ei missään nimessä pitäisi päästä
- tekstin määrä oli sopiva

Omat johtopäätökset: Muuten visuaalisesti ja sisällöllisesti hyvä kurssi, mutta tulevaisuudessa voisi järjestää jotain extraa? Lisäksi kurssin voisi suorittaa vuosittain, mikä muistuttaa luokittelun tärkeydestä

- satunnaisesti voi järjestää, koska kurssit ovat toistuvia
- lyhyt kurssi ei ole ajankäyttökysymys, vuosittain puolentoista tunnin kurssia ei voi suorittaa, mutta 5-20 min kurssin voi.
- Rahanpesu-verkkokurssi pitää konttoreissa suorittaa joka vuosi, ja se on jo niin iskostunut, että osaa asiat
  Pitäisikö joissain kursseissa olla enemmän tehtäviä? Tämä vaikuttaa kurssin kestoon.
- riippuu aiheesta, mutta tässä verkkokurssissa en mennyt eteenpäin ennen, kun olin katsonut koko sisällön, kysymykset hyviä kun joutuu miettimään mitä edellisellä sivulla oli

Liite 4: Luokiteltu haastatteluaineisto

Ilmaisu	Pelkistetty ilmaisu / tutkijan tulkinta	Luokka
hyvässä mielessä selkeä luokittelu, näki heti mitkä ovat OP:n turvaluokat, toistuivat, ei jäänyt epäselvyyksiä	Asia ilmaistu selkeästi ja asiaa toistettiin	Verkkokurssin sisältö
tehtäviä pitää myös olla, riippuu asiasta, joissain asioissa pitää olla ettei verkkokurssia suorita juosten, tässä ei tarvitse olla enemmän tehtäviä, OP:ssa monenlaisia verkkokursseja, mutta tässä ei tarvita, koska on niin selkeä	Tehtävien määrä riippuu verkkokurssin aiheesta	Verkkokurssin sisältö
joihinkin kursseihin täytyy keskittyä paljon enemmän, ja jos tehtäviä ei ole, niin miettii että mites tää meni, kyllä toimii tehokkaasti oppimisvälineenä, tehtävät eivät jääneet mieleen	Tehtävät ovat tehokas oppimisväline, kurssin tehtävät eivät jääneet mieleen	Verkkokurssin sisältö
muut: ei meillekään	Tehtävät eivät jääneet mieleen	Muisti
luontevat tehtävät, joutui vähän miettimään,	Tehtävät olivat luontevia ja eivät olleet liian helppoja	Verkkokurssin sisältö
soljui yhden osion päätteeksi, tällainen mielikuva, mutta voin olla väärässä, ei turhauttanut, pääsee eteenpäin	Tehtävät seurasivat tieto-osiota, kurssissa pääsee eteenpäin	Verkkokurssin sisältö
sujuva, nopea	Verkkokurssi oli sujuva ja nopea	Verkkokurssin sisältö
Organisaation ylin, jota me ei nähdä, ja sitten luottamuksellinen, sisäinen (kaikki yhdessä), julkinen (kaikki yhdessä), SSL		
iso merkitys siinä, miten asiat tarjoillaan, ja tässä onnistuttiin siinä. Kevyesti voi lähestyä painavaa asiaa	Painavaa asiaa lähestytty kevyesti	Verkkokurssin sisältö
kukaan ei ole ainakaan sanonut, että ärsyttää. Sopii myös konttoreissa suoritettavaksi	Verkkokurssi sopii pankin toimihenkilöille, ei ole ärsyttävä	Verkkokurssin sisältö
lyhyet pätkät siinä mielessä helpompia, puolentoista tunnin kurssiin tulee keskeytyksiä, ja joku asia menee ohi. Miten vireystaso pysyy yllä, ajatukset harhailevat työasioihin (muut samaa mieltä)	Lyhyet verkkokurssit helpompia, koska ei tule keskeytyksiä, vireystila pysyy eivätkä ajatukset harhaile työasioihin	Keskittymiskyky
Keskittyminen säilyy	Keskittyminen säilyy kun kurssi on lyhyt	Keskittymiskyky
löytää helpommin ajan kurssin suorittamiselle	Ajankäytön suunnittelu helpompaa	Ajankäytön haasteet
mielenkiinto säilyy, asenne parempi	Mielenkiinto säilyy kun ja asenne on parempi	Asenteet
konttoreissa mukavampi ottaa asiakas. Jos suorittaa puolentoista tunnin kurssia niin tämä ei ole mahdollista	Vaikea ottaa asiakkaita jos suorittaa puolentoista tunnin kurssia	Ajankäytön haasteet
ei muisteta mitä tarkalleen luki, mutta ydinasia jäänyt mieleen mikä tärkeää: mihin ollaan velvollisia sitoutumaan, verkkokurssi on hyvä jos tämä oivallus tulee	Ymmärretään asian tärkeys ja mihin sitoudutaan	Tietoisuus
Turvaluokat selkeästi esitetty, oli helppo ymmärtää, mihin dokumenttiin tulee mikäkin luokitus	Ymmärretään käytännössä, miten dokumentit turvaluokitellaan	Tietoisuus
tuli vahvistamaan tietosuojan tärkeyttä, lainsäädäntö tiukentuu, yksilön oikeusturva paranee,	Ymmärretään ohjeistuksen yhteys lainsäädäntöön	Tietoisuus
ei muista, miten oli perusteltu, koska asia tuntui ajankohtaiselta, ei kiinnittänyt huomiota	Perustelua ei muisteta	Muisti
ei tarvitse opetella ulkoa, ydin asia tuli tärkeänä esiin, ei kuitenkaan vielä osa omaa rutiinia	Asia on ymmärretty, mutta ei vielä siirtynyt omaan toimintaan	Tietoisuus
kaikkia muita käyttänyt paitsi julkista	Osataan yhdistää asia omaan työhön	Käyttäytyminen
ei tuoteta julkista, jos itse tuottaa niin luottamuksellista ja jopa salainen	Osataan yhdistää asia omaan työhön	Vaikutus omaan työhön
julkista tietoa ei tarvitse jakaa, koska löytyy verkkosivuilta	Osataan yhdistää asia omaan työhön	Vaikutus omaan työhön
selkeä yksinkertaiselle ihmiselle	Selkeys	Verkkokurssin sisältö
niin pitää olla, OP:n sisällä tieto aina luottamuksellista, salaista ja sisäistä	Osataan luokitella tietoa	Tietoisuus
riippuu dokumentin luonteesta, osa tiedosta vanhenee, joten sitä ei jaeta	Osataan käsitellä tietoa oikein	Tietoisuus
mun mielestä kaikki, jotka liittyvät tietoturvaan ovat pakollisia, olisin suorittanut vaikkei olisi ollut pakollinen, täytyy pysyä ajan tasalla	Suorittaisi kurssin vaikka ei olisi ollut pakollinen	Tietoisuus
en itse koe, että ennakkokäsitykset muuttuivat. Tiedostin ennen kurssia, että tietoturvaan liittyy tarkkuus ja täytyy olla huolellinen, kurssi palautti mieleen sen, että on tullut muutoksia ja lisää tiukennuksia. Näitä asioita miettii pitkään tietoisesti, kun tekee töitä.	Tietoisuus siitä, että tietoturvaan liittyy tarkkuus ja huolellisuus. Tietoisuus siitä, että säännöt muuttuvat	Tietoisuus
Omassa tekemisessä täytyy terästäytyä myös palavereiden ja paperisten dokumenttien osalta.	Omissa toimintamalleissa on parannettavaa	Käyttäytyminen
en minäkään, ja äkkiseltään luulisi että ei kun muistan millä alalla ollaan, täällä pitää olla skarppina (muut samaa mieltä)	Tietoisuus siitä, että alaan liittyy tiukat tietoturvavaatimukset	Tietoisuus
uskon, että kaikki ymmärtää tärkeyden	usko siihen, että henkilöstö pitää tietoturvaa tärkeänä asiana	Arvot
toki voisi tehdä eri työntekijöitä varten yksityiskohtaisemman verkkokurssin sisällöllisesti, mutta tuoko se lisäarvoa? Menee liian tarkalle tasolle ja verkkokurssista voi tulla kuivakka. Jokainen ymmärtää, miten luokittelu vaikuttaa omaan työhön.	Eri rooleissa oleville voisi tehdä oman verkkokurssin, mutta se ei välttämättä tuo lisäarvoa	Verkkokurssin sisältö

tärkein on se että ihmiset ymmärtävät	Tärkeintä on ymmärrys	Tietoisuus
selkeä luokittelu, näki heti mitkä ovat OP:n turvaluokat, toistuivat, ei jäänyt epäselvyyksiä, muut samaa mieltä	Ei jäänyt epäselvyyksiä, selkeys	Tietoisuus
lyhyt ja ytimekäs, ei muisteta mitä tarkalleen luki, mutta ydinasia jäänyt mieleen mikä tärkeää: mihin ollaan velvollisia sitoutumaan, verkkokurssi on hyvä jos tämä oivallus tulee	Tiedetään, mihin on sitouduttu ja mitkä ovat velvollisuudet	Tietoisuus
Turvaluokat selkeästi esitetty, oli helppo ymmärtää, mihin dokumenttiin tulee mikäkin luokitus	Asia on esitetty ymmärrettävästi	Verkkokurssin sisältö
Myös se kenelle voi jakaa jäi mieleen, minkä tiedon voi jakaa kumppanille, jäi mieleen että puhuttu tieto on myös tietoa, täytyy miettiä missä tilanteissa voi puhua mitäkin, muut samaa mieltä	Ymmärretään, miten tiedon luokittelu ja käsittely näkyy omassa työssä	Tietoisuus
sanon asiakkaalle, että löydät sen sieltä, itse ei sitoudu mihinkään väärään silloin	Asiakasta osataan neuvoa ja toimia samalla tietoturvasääntöjen mukaan	Käyttäytyminen
omassa työssä vain sisäistä, valmistelut palavereihin ja muuta, salainen oman tiimin henkilöstöhallintoon liittyviä asioita, omalla koneella, joten ei jaksa kirjoittaa luokkia (muut myötäilevät	Salainen tieto on vain omalla koneella, joten luokittelu siinä tilanteessa koetaan turhaksi	Kyseenalaistus
unohtuu silloin, jos ajattelee ettei tule koskaan jakamaan tietoa	Tietoturvaohjeistusten unohtaminen	Muisti
onko tarve laittaa jos on vain omalla koneella?	Kyseenalaistetaan tarpeellisuus	Kyseenalaistus
en tule koskaan jakamaan kenellekään, enkä näytä myöskään, korkeintaan esimiehelle nojoo silloin pitäisi olla salainen, oma esimies tuntee porukat ja pääsy samoihin tietoihin	Ei tule koskaan jakamaan tietoa paitsi esimiehelle	Kyseenalaistus
ei tule ajatelleeksi aina	Tietoturvaohjeistukset saattavat unohtua	Muisti
toimii tosi hyvänä muistuttajana, esim. siinä että jokaiseen dokumenttiin tulee merkitä turvaluokka, se jää helposti tekemättä	Verkkokurssi muistuttaa säännöistä/ohjeista	Muisti
dokumenttipohjissa on hyvä olla valmiina luokat, helpompi lisätä luokka	Tietoturvaohjeistuksia ei voi noudattaa jos se ei ole käytännössä mahdollista	Käyttäytyminen
kuitenkin mielessä, ei sitä tahalteen jätä pois	Toimitaan tahattomasti ohjeiden vastaisesti	Muisti
asia on mielessä kokoajan. Asiakas täytyy tunnistaa, koska asiakkaiden kanssa puhutaan usein puhelimessa vahinkoasioista.	Tietoturvallisuus on kokoajan läsnä työssä	Tietoisuus
tapaamisissa kumppanin kanssa pitää tietää keitä on tulossa ja mitä tietoa käsitellään, ei tule mukaan tyyppejä, joista ei tiedetä mitään.	Tapaamisissa täytyy etukäteen tietää, mitä tietoa käsitellään ja keitä on tulossa	Tietoisuus
vaikka luokitusta ei olisi, tiedetään, miten toimitaan eli ohjeistus ei siltä osin vaikeuta työskentelyä	Osataan toimia turvallisesti vaikka luokitusta ei ole	Tietoisuus
turhautuminen voi tulla siitä, että tääkin pitää muistaa merkitä, taas yksi asia joka pitää muistaa	Ärsyttää, että pitää muistaa tehdä monta asiaa	Muisti
riippuu mitä tekee. Jos ei ikinä tarvitse mitään paperilappua kirjoittaa, niin tuntuu turhalta	Säännöt turhauttavat, jos ei koskaan tarvitse käsitellä dokumentteja	Vaikutus omaan työhön
Op:ssa oltiin testattu sitä, kuinka vapaasti rakennuksessa pääsee liikkumaan ilman kulkuoikeuksia niin ettei jää kiinni. Oli päässyt sellaisiin paikkoihin, joihin ei missään nimessä pitäisi päästä	Henkilöstö ei aina puutu tilanteisiin, jotka saattavat vaarantaa tietoturvallisuuden	Asenteet
tarjoiltu mielettömän hyvin, kuukauden kurssit olleet hyviä, kamalan tylsä ala (turvallisuus),pieni juttu mutta tarjoillaan kuukauden kurssina, kolahti	Turvallisuutta pidetään tylsänä aiheena, mutta kurssi sai aiheen vaikuttamaan mielenkiintoiselta	Verkkokurssi
jos kurssi olisi tehty toisin, esimiehet olisi joutuneet pakottamaan suorittamaan kurssin	Esimiehet olisivat joutuneet pakottamaan henkilöstöä suorittamaan kurssin, jos toteutus olisi ollut toisenlainen	Verkkokurssi
mielestäni nämä pitäisi suorittaa pakollisena joka vuosi, eikä joka toinen vuosi	Verkkokurssi pitäisi suorittaa säännöllisin väliajoin	Muisti
pankissa täytyy tietää nämä asiat.	Oletus on se, että tietoturvasta välitetään ja ollaan tietoisia	Tietoisuus
varmasti jotkut kokevat ohjeet tällä tavoin.	Jotkut kokevat ohjeet ärsyttävinä	Asenteet
tämä on niin säännelty ala, luovuus ei voi kukkia täällä	Pankki-ala on säännelty ala, ja toiminnassa täytyy noudattaa sääntöjä	Tietoisuus
en huomannut kuukauden kurssia, oliko intrassa, tuli meille jakeluna,	Isossa organisaatiossa viestintä on haasteellista, ja kaikista muutoksista ei edes tiedetä	Viestintä
mäki mietin et oliko intran sivuilla jossain vaiheessa. Esimiehet laittoivat erikseen sähköpostia, ei muista kumman huomasi ensin	Intraa ei aina lueta, mutta esimiesten viestit luetaan	viestintä