TIETOJOHTAMISEN ROOLI UUDEN TIEDON HYÖDYNTÄMISESSÄ RISKIENHALLINNAN NÄKÖKULMASTA

CASE: BEC-huijauksen aiheuttaman haitan ennaltaehkäiseminen yritysten maksuliikenteessä

Lappeenrannan–Lahden teknillinen yliopisto LUT

Kauppatieteiden pro gradu -tutkielma

2024

Johanna Kiviranta-Mounier

Tarkastajat: Apulaisprofessori Henri Hussinki

Professori Kirsimarja Blomqvist

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT-kauppakorkeakoulu

Kauppatieteet

Johanna Kiviranta-Mounier

Tietojohtamisen rooli uuden tiedon hyödyntämisessä riskienhallinnan näkökulmasta

CASE: BEC-huijauksen aiheuttaman haitan ennaltaehkäiseminen yritysten maksuliikenteessä

Kauppatieteiden pro gradu -tutkielma

2024

110 sivua, 22 kuvaa, 3 taulukkoa ja 3 liitettä

Tarkastaja(t): Apulaisprofessori Henri Hussinki ja Professori Kirsimarja Blomqvist

Avainsanat: tietojohtaminen, tieto, tietoprosessi, tietomuutos, riskienhallinta, BEC-huijaus, tiedon oikeellisuus

Tieto nähdään yritysten tärkeimpänä resurssina, tuotannontekijänä, josta on itsestään tullut myös tärkeä tuote. Organisaation päätökset, suorituskyky ja menestys pohjautuvat tietoon. Jotta tiedosta on hyötyä, tulee sen oikeellisuus varmistaa. Uuden tiedon validointi ei kuitenkaan saa oletettua huomiota ja asemaa tietoprosessien kuvauksissa.

Tässä pro gradu -tutkielmassa tarkastellaan tietojohtamisen roolia uuden tiedon hyödyntämisessä riskienhallinnan näkökulmasta. Aihetta tutkittiin rahaliikenteeseen kytkeytyvien väärinkäytösten kautta. Tutkimus toteutettiin laadullisena haastattelututkimuksena ja aineisto analysoitiin Grounded Theory -tutkimustavan pohjalta syntyneellä Gioia-metodilla.

Tutkimuksen tulokset koottiin yhtenäiseksi viitekehykseksi, joka kuvaa tietojohtamisen roolia uuden tiedon hyödyntämisessä riskienhallinnan näkökulmasta. Viitekehys osoittaa miten yrityksiin kohdistuvia tietosyötteitä voi lähestyä ja miten niiden mahdollisilta negatiivisilta vaikutuksilta voi suojautua tietojohtamisen keinoin. Tutkimuksen tulokset osoittavat, että tietojohtamisen elementeillä on selkeä ja oleellinen rooli riskienhallinnassa, kun uuden tiedon käyttökelpoisuutta arvioidaan.

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

LUT Business School

Business Administration

Johanna Kiviranta-Mounier

The Role of Knowledge Management in Utilizing New Knowledge from the Perspective of Risk Management

CASE: Preventing Harm Caused by BEC fraud in Corporate Cash Flow

Master's thesis

2024

110 pages, 22 figures, 3 tables and 3 appendices

Examiners: Assistant Professor Henri Hussinki ja Professor Kirsimarja Blomqvist

Keywords: Knowledge management, knowledge, knowledge process, knowledge change, risk management, BEC fraud, correctness of information

Knowledge is seen as the most important resource of companies, a production factor, which itself has also become an important product. Organizational decisions, performance and success are based on knowledge. For the knowledge to be useful, its correctness must be ensured. However, the validation of new information does not receive the expected attention and position in the descriptions of information processes.

This master's thesis examines the role of KM in the utilization of new information from the perspective of risk management. The topic was studied through abuses connected to payments. The study was carried out as a qualitative interview study and the material was analysed using the Gioia method, which was born based on Grounded Theory.

The results of the research were compiled into a framework that describes the role of knowledge management in the utilization of new information from the perspective of risk management. The framework shows how to approach information inputs aimed at companies, and how to protect the organisation from their possible negative effects by means of knowledge management. The results of the research show that the elements of knowledge management play a clear and essential role in risk management when assessing the usability of new information.

Sisällysluettelo

Liitteet

Kuvioluettelo

Taulukkoluettelo

1 Johdanto

Maksamisen alue on murroksessa, jossa digitalisaatio ja uusien teknologioiden hyödyntäminen valtaa alaa yhä kiihtyvällä tahdilla. Tästä hyviä esimerkkejä ovat erilaiset API-ratkaisut (ohjelmistorajapintaratkaisut) kuten Payment Services Directive 2 (PSD2) -direktiivin EU-tasolla päätetyt ratkaisut ja pankkien omat vielä pidemmälle viedyt API-palvelut. PSD2 täydentää aiemmin voimaan tullutta ensimmäistä maksudirektiiviä. Direktiiveillä säädellään maksamisen palvelujen kehitystä ja sille asetettuja tavoitteita. Direktiivi on toiminut työkaluna yhtenäisen euromaksualueen, SEPA, saavuttamisessa (Single Euro Payments Area, SEPA). PSD2:n tavoitteena on tukea innovatiivista ja kilpailulle avoimempaa maksujärjestelmän kehittämistä. Open banking -termillä viitataan käynnissä olevassa kehityksessä asiakkaiden uusia mahdollisuuksia jakaa rahaliikenteeseensä liittyvää dataansa myös muille toimijoille kuin tilipankeille. Ohjelmistorajapintoihin perustuvat ratkaisut mahdollistavat tämän kehityksen. Ytimessä, samaan aikaan teknisen kehityksen rinnalla, ovat edelleen myös turvallinen maksaminen ja asiakkaiden tietojen turvaaminen. Maksuliike on jo monessa tilanteessa reaaliaikaista ja tämä suuntaus laajenee koko ajan uusiin maksamisen kanaviin ja palveluihin. Huomion arvoista kehityksessä on, että maksamisesta ovat katoamassa rajat. Digitalisaation tuomat ratkaisut mahdollistavat jo esimerkiksi EU:ssa lähes reaaliaikaisen maksamisen. Ei ole enää merkitystä lähteekö maksu Tampereelta Rovaniemelle vai Roomaan, perillä se on samassa aikataulussa, alle kymmenessä sekunnissa. (European Central Bank 2018 ja 2023; Palva 2015.)

Maksaminen on yhteiskunnassa tavanomaista jokapäiväistä toimintaa, jossa ovat mukana sekä kuluttajat, yritykset että julkiset toimijat. Rahankäyttöön kytkeytyy hyvin paljon turvallisuuteen ja väärinkäytöksiin liittyviä teemoja ja uhkia. Rahaliikenteen nopeutuessa digitaalisen kehityksen myötävaikutuksesta, myös maksujärjestelmien kontrolli ja turvaaminen muuttuvat vanavedessä. Maksamista ja sen digitaalista kehitystä tarkastellessa on huomioitava, että pääpaino on turvallisessa ja lailliseksi varmistetussa maksamisessa. Jotta maksaminen toteutuu oikein, on sen perustana käytettävä laadukasta maksutietoa. Tiedon on oltava teknisessä mielessä automaation hyväksymässä, standardin määrittelemässä muodossa,

mutta myös puhdasta ja koskematonta niin, että petosyritykset, kyberhyökkäykset tai muut väärinkäytökset eivät pääse sitä turmelemaan matkalla maksajalta saajalle. Digitalisaation maksamiseen tuomassa kehityksessä pääajuri tulee jatkossakin olemaan turvallisuus ja erilaisten uhkien kuten kyberhyökkäyksien sietokyky. (Takala 2022; European Central Bank 2023.) Finanssialalla tieto ja sen eheys sekä muuttumattomuus maksuprosessin aikana on aiemmin kuvatusti prosessien perusta ja kehityksen lähtökohta nyt ja tulevaisuudessa. Kuluttajien maksukäyttäytyminen, tarjolla olevat uudet maksutavat sekä maksamisen turvallisuus ovat usein fokuksessa uutisoinnissa ja myös EU:n päätöksenteossa. Tässä työssä keskitytään organisaatioiden väliseen maksamiseen, siinä piileviin huijausriskeihin ja niiltä suojautumiseen.

Tieto (knowledge) on organisoitua ja käyttökelpoista informaatiota, jolla on merkitys. Ilman hyödynnettävyyttä ja merkitystä kyseessä on organisoimaton informaatio (data). Tieto nähdäänkin kaikilla aloilla tänä päivänä yritysten tärkeimpänä resurssina. Näin ollen tiedon turvaaminen kaikissa tilanteissa on ensiarvoisen tärkeää organisaatioiden menestykselle. (Martelo-Landroguez, Navarro ja Cepeda-Carrión 2019; Randeree 2006; Bhatt 2000.) Kuten aiemmin todettu maksaminen koskettaa kaikkia toimijoita yhteiskunnassa. Maksutiedon virheettömyys ja eheys maksajalta saajalle on tärkeää kaikille osapuolille. Onnistunut ja tarkoituksen mukainen maksuliikenne lähtee käyntiin maksavasta tahosta, joka maksaa sopimuksen mukaisesti hankkimastaan tuotteesta tai palvelusta myyjälle eli saajalle.

Kun tutustuu tietojohtamista käsittelevään kirjallisuuteen, päästäkseen lähemmäs siinä käsiteltyjä tietojohtamisen riskejä, huomaa, että tiedon validoinnista on vaikea löytää tutkimuksia. Kun etsii tutkimuksia tiedon arvioinnista siitä näkökulmasta, että miten tiedon oikeellisuus ja todenperäisyys huomioidaan, ei löytynyt tutkimuksia, joissa näkökulma olisi ollut juuri tämä. Kun listataan tietojohtamisen tutkimusalueen riskejä, pääriskinä pidetään tiedon menettämistä esimerkiksi työntekijöiden eläköitymisen tai työpaikan vaihdon seurauksena. Tietoon liittyviä mahdollisuuksia voidaan myös hukata organisaation omien puutteellisten tallentamisen, tiedon hyödyntämisen ja siirtämisen prosesseissa. (Ilvonen, Thalmann, Manhart & Sillaber 2018.) Tietojohtamista käsittelevissä artikkeleissa ja teorioissa käsitellään todella vähän, jos ollenkaan, alkuperäisen tiedon oikeellisuutta. Pääasiassa riskiajattelussa

keskitytään tiedon tallentamiseen, siirtämiseen ja soveltamisen turvallisuuteen. Tavoitteena tutkimuksissa on pääasiassa mainittu kilpailukyvyn lisääminen ja välillä myös suorituksen parantaminen organisaatiossa. (Jennex & Zyngier 2007; Manhart & Thalmann 2015.) Vähemmän löytyy tutkimustietoa riskeistä ja tiedon oikeellisuuden varmistamisesta tiedon käyttöönoton yhteydessä eli siitä hetkestä, kun informaatio hyväksytään tiedoksi. Tässä vaiheessa tieto myös valitaan käytettäväksi osana organisaation tietoprosesseja ja siitä tulee osa organisaation tietopääomaa.

Uudessa toimintaympäristössä tiedon turvaaminen pitää saada toimimaan kaikilla tasoilla; organisaatiotasolla, yksilötasolla ja käytetyillä teknologia-alustoilla. Tiedon jakaminen yksilöiden välillä on tärkeässä roolissa tiedonkulun kokonaisuudessa. Yksilöiden asema tiedon validoinnissa ja sen siirtämisessä laajempaan käyttöön organisaatiossa on kaiken perusta. Yksilön päätös käyttää tietoa, olla käyttämättä tietoa, jakaa tietoa tai pitää sen itsellään on tietoprosessin käynnistävä kohta. (Ilvonen et al. 2018.) Aiheesta on vaikeaa löytää paljon tutkimuskirjallisuutta. Tämä vaikuttaa erikoiselta tutkimusaukolta, koska tieto on se, johon päätökset ja toiminnot ylipäänsä pohjautuvat. Eikö silloin tiedon oikeellisuus ole ensi arvoista? Tutkijat Jennex ja Zyngier kuvaavat tilannetta hyvin. Koska tietopääomaa pidetään tärkeänä monet tutkijat pitävät oletusarvona, että tiedon ja tietoprosessien turvallisuuden tärkeys on sisään leivottuna. Tämän takia tutkimuksissa katsotaan, että turvallisuutta ei tarvitse erikseen alleviivata. (Jennex ja Zyngier 2007.)

1.1 Tutkielman tausta ja tavoite

EU:n Single Euro Payments Area (SEPA) mahdollistaa erityisiä maksamisenkehitysaskelia, kun standardeista ja aikatauluista päätetään direktiivien osalta yhdessä. Tahtotila ja trendi nopeasta sekä sujuvasta makuliikenteestä on myös maailmanlaajuinen. Uusi SWIFT gpi (Global Payments Innovation) -maksustandardi mahdollistaa maailmanlaajuisesti nopean ja varman maksamisen useissa valuutoissa. Alusta varmistaa, että tietoa ei kadoteta tai se ei muutu matkalla maksajalta saajalle. Maksustandardi tukee rahoitusalaa takaamalla rahaliikenteen nopeuden lisäksi myös tiedon eheyden matkalla. (SWIFT 2023.)

Reaaliaikaisuudesta ja nopeudesta huolimatta rahaliikennettä monitoroidaan monelta kantilta. Finanssiala on tiukasti sidoksissa moniin regulaatioiden ja sääntelyn asettamiin vaatimuksiin. Kansallinen ja kansainvälinen regulaatio määrittelee pankkisektorille tarkat toimintaperiaatteet monilla osa-alueilla kuten vakavaraisuus, asiakkaan tunteminen (Know Your Customer, KYC) ja pakotteiden noudattaminen. Pakotteet rahaliikenteessä nimensä mukaan pakottavat olemaan vastaanottamatta tai maksamatta maksuja tiettyjen tahojen kanssa. Pakotteita asettavat esimerkiksi EU, YK ja USA:n valtionvarainministeriö. Pakotteet voivat kohdistua maahan, yritykseen tai henkilöön. Monitoroinnin seurauksena maksu voidaan pysäyttää lisätutkimuksia varten, palauttaa tai jäädyttää. (Botta & Nadeau 2022; Ulkoministeriö 2023.)

Samaan aikaan kun uudet teknologiat mahdollistavat nopean maksuliikenteen, ympärillä oleva maailma haastaa finanssialan kehitystä lisääntyvillä uhkakuvilla. Kansainvälisen maksuliikkeen volyymit kasvoivat vuonna 2021 27 % ja elpyivät näin koronan aiheuttaman erikoistilanteen jälkeen. Lähitulevaisuudessa odotetaan kuitenkin maltillisempaa kasvua johtuen negatiivisesta geopoliittisesta tilanteesta. Maksamisen tulevaisuutta muokkaavat erilaiset toimintaympäristössä vaikuttavat tekijät. Maailma on monimutkainen pelikenttä, jossa erilaiset sekä ennustettavat että yllättävät kehityssuunnat ja tapahtumat aiheuttavat haasteita. Joitakin esimerkkejä yllättävistä tilanteista, jotka vaikuttavat välillisesti maksuliikenteeseen suoraan tai toimitusketjujen kautta, ovat korona epidemia, Venäjän hyökkäyssota Ukrainaan ja Ever Given -konttilaivan jumiutuminen Suezin kanavaan. Enemmän etukäteen tiedossa olevia vaikuttavia elementtejä ovat esimerkiksi maailman politiikka, finanssialaan suuntautuva säätely ja rahaliikenteeseen suuntautuva rikollisuus. Luonnollisesti myös politiikka, säätely ja rikollisuuden uudet ilmentymät myös yllättävät finanssitoimijoita, mutta erilaisiin perustilanteisiin ja sykleihin pystytään varautumaan, niitä voidaan ennakoida ja niitä varten harjoitellaan. (Botta & Nadeau 2022; European Central Bank 2023.)

Rahalaitoksiin suoraan sekä erityisesti niiden asiakkaiden rahaliikenteeseen kohdistuu hyvin laaja kirjo erilaisia rikollisuuden muotoja. Kaikki verkossa ja mobiililaitteissa tapahtuvat rikollisuudenmuodot ovat kasvussa kuten kyberrikollisuus, myös tekoälyn hyväksikäyttö, sijoitushuijaukset, rakkaushuijaukset, tiedon kalastelu viestein, huijaussivustot ja BEC-

huijaukset. Finanssiala ry:n mukaan vuoden 2023 alkupuoliskolla huijauksien määrä on ollut kovassa nousussa. Suomalaisilta onnistuttiin huijaamaan 19,8 miljoonaa euroa, joka oli 9 miljoonaa euroa enemmän kuin 2022 vastaavana aikana. (Finanssiala ry 2023.)

Yksi yleinen petosmuoto on sähköpostitse toteutettu BEC-huijaus (business e-mail compromise). BEC-huijauksessa yritystä lähestytään sähköpostitse tarkoituksena esimerkiksi kalastella taustatietoja huijaustarkoituksessa varsinaiseen huijaukseen valmistautuessa, pyydetään maksusuoritusta kiireiseen erikoistilanteeseen vedoten (niin sanottu toimitusjohtajahuijaus) tai ilmoitetaan kauppakumppanin maksatustietojen eli tilinumeron ja pankin muutoksesta. Koska sähköposti on yksi yleisimpiä tapoja kommunikoida, ovat laajimmin käytössä olevat sähköpostiprotokollat kaikkien saatavilla ja näin ollen hyvin haavoittuvaisia rikolliselle käytölle. Sähköpostin avulla tehdyt petokset alkoivat, kun sähköpostin käyttö yleistyi 90-luvun puolivälissä ja on kasvanut siitä saakka yhä suuremmaksi haitaksi. Sähköpostin välityksellä tehdään monenlaisia maksamiseen liittyviä rikoksia. BEC-huijauksissa viestin lähettäjä esiintyy jonakin muuna tahona ja pyrkii näin hankkimaan tietoa kalastelemalla tai huijaamaan muulla tavoin. Sähköpostilla toteutettavalta rikollisuudelta on pyritty suojautumaan erilaisilla suodattimilla, jotka havaitsevat haitalliset viestit. Rikolliset kuitenkin näyttävät aina löytävän uusia keinoja asetettuja filttereitä. Työelämässä, sähköpostin ollessa monesti pääasiallinen kommunikointikanava yrityksen ja toimittajan välillä, ongelmaksi muodostuu erottaa oikea tieto väärästä. (Hitesh, Aniruddh, Aniruddh & Shubha (2022); FBI 2022.) Rahalliset menetykset ovat edelleen kasvussa, kun huijausviestit jatkavat kehityskulkuaan. Tekoälyn ja psykologisen manipuloinnin hyödyntäminen tekevät huijauksista kehittyneempiä ja tehokkaampia. Sosiaalisen median profiileja ja organisaatioiden verkkosivuja hyödynnetään huijauksiin kattavasti. (Limnell 2023.)

Erilaisista maksuliikenteen kohtaamista väärinkäytöksistä tässä työssä pureudutaan yrityksien kohtaamiin BEC-huijauksiin. Kuten aiemmin mainittu myös BEC-huijauksissa voivat rikollisten tavoitteet ja toimintatavat olla moninaiset. Tässä työssä keskitytään erityisesti BEC-huijauksien siihen ilmentymään, jossa yritykselle ilmoitetaan sähköpostitse kauppakumppanin tilinumeron muutoksesta. Toisin sanoen tilinumero, jolle on tarkoitus maksaa ei ole entuudestaan yrityksen maksunsaajarekisterissä ja näin ollen sille ei ole aiemmin

maksettu. Tilinumerotieto on joko täysin uusi eli kyseessä on uusi kauppakumppani tai pidempiaikainen kauppakumppani ilmoittaa muutoksesta aiemmin käytössä olleeseen tilinumeroon. Tutkielmassa kartoitetaan, mitä yrityksissä tapahtuu, kun maksatustiedon muutossyöte ilmoitetaan yritykseen sähköpostitse. Millainen tietoprosessi organisaatiossa on luotu uuden tiedon validoimiseen, kuinka merkittävänä riskinä huijaus nähdään ja millainen on tietojohtamisen rooli riskienhallinnassa ja validoinnissa.

Rikolliset käyttävät BEC-huijauksia laajasti ja huijausten määrät ovat alati kasvussa. Näistä aiheutuu organisaatioille suuria tappioita vuosittain. Sähköpostilla viestiminen on maailmanlaajuisesti tavanomaista toimintaa päivittäisessä liiketoimintaan liittyvässä kommunikoinnissa. Sähköposti on myös kanava, jossa huijaaminen ei aina vaadi erityistä teknistä osaamista. Kun huijaustilanteeseen lisätään tavanomaisen viestintäkanavan, sähköposti, lisäksi vielä yrityksissä vallitseva hektinen työtilanne, rikolliset pääsevät liian usein tavoitteisiinsa. Toteutuneista huijauksista koottuja tietoja tutkiessa huomaa, kuinka yrityksillä on edelleen paljon kehitettävää huijatuksi tulemisen ennaltaehkäisyssä. Alla muutamia esimerkkiuutisia BEC-huijausten aiheuttamista tappioista.

” Suomalaisia yritettiin huijata 76,9 miljoonan euron edestä vuonna 2023, ilmenee Finanssiala ry:n pankeilta keräämistä tiedoista. Edellisvuonna määrä oli 46,5 miljoonaa. Pankit saivat pysäytettyä ja palautettua 32,7 miljoonaa euroa huijareille menossa ollutta rahaa. Edellisvuonna määrä oli 14,1 miljoonaa. Yhteensä suomalaiset menettivät verkkorikollisille 44,2 miljoonaa euroa vuonna 2023.” (Palmgren 2024)

“Business email compromise scams caused the highest losses across all scam types in 2019 costing businesses AUD 132 million” (The ACCC 2020)

“In 2022, the IC3 received 21,832 BEC complaints with adjusted losses over $2.7 billion.” (FBI 2022)

Tässä Pro Gradu tutkielmassa tutkin yritysten tapoja hallita riskejä niiden validoidessa organisaation ulkopuolelta tulevan tiedon todenperäisyyttä. Tutkielmassa kerättyä ja analysoitua tietoa hyödynnetään laajentamaan ymmärrystä yritysten tavoista hallita riskejä niiden validoidessa organisaation ulkopuolelta tulevan tiedon todenperäisyyttä. Tavoitteena on ymmärtää paremmin käytössä olevat prosessit ja miten niihin on päädytty. Tutkielmassa tutkittavana organisaation ulkopuolelta tulevana tietosyötteenä toimii tilinumero, joka otetaan käyttöön tai hylätään. Riskinäkökulmaa katsotaan maksamiseen liittyvän rikollisen toiminnan eli BEC-huijausten näkökulmasta. Tässä tutkielmassa ei käsitellä organisaation sisältä tulevia petoksia eikä muita rahaliikenteeseen tai organisaatioihin kohdistuvia väärinkäytöksiä. Aihetta tutkitaan tieteellisestä näkökulmasta, joka tarkkailee tukittavan ilmiön mahdollisesti sisältämiä tietojohtamisen elementtejä. Aihetta lähestytään tutkitusmenetelmäkuvauksen (luku 3.) mukaisesti etsien empiirisen aineiston esiin nostamia teoreettisia yhtymäkohtia tietojohtamisen tutkimuskirjallisuudesta.

1.1.1 Tutkimusongelma ja tutkimuskysymykset

Tarkoitus on tutkia empirian kautta, löytyykö tietojohtamisen näkökulmille roolia tai käyttöä tiedon validointitilanteen riskien hallitsemisessa. Tutkielma myös kartoittaa miten oleellisena riskinä huijaukset nähdään organisaatiotasolla ja miten tätä riskiä hallitaan tietojohtamisen näkökulmasta. Alla kuvattuna tutkimusongelma ja alatutkimuskysymykset, jotka tukevat pääkysymyksen pohdintaa.

Tutkielman päätutkimuskysymys ja alakysymykset:

”Millainen on tietojohtamisen rooli riskienhallinnassa, kun organisaatiossa pyritään suojautumaan uuden tiedon käyttämiseen liittyviltä riskeiltä?”

Pääasiallisesti tutkittavaa tietojohtamisen roolia riskienhallinnassa tukevat alatutkimuskysymykset ovat:

”Miten uuden tiedon validoimiseen luotuun tietoprosessiin on organisaatiossa päädytty?

”Kuinka suurena riskinä huijaukset nähdään?”

”Millaisia vaikutuksia huijauksilla on organisaatiolle ja miten niistä selvitään?”

Ensimmäisellä alatutkimuskysymyksellä pyritään kartoittamaa, millaisia prosesseja uuden maksutiedon validoinnissa käytetään. Miten kyseiseen prosessiin on päädytty ja miten niitä kehitetään. Vaihtoehtoisesti, jos validointia ei tehdä pyritään selvittämään, miksi tähän on päädytty. Toisella alatutkimuskysymyksellä selvitetään, kuinka isona riskinä riskikartoituksissa maksamiseen liittyviä riskejä pidetään. Eli kuinka suuren painonarvon ne saavat yritysten riskienhallinnassa. Viimeisellä alakysymyksellä selvitetään, miten huijauksen uhriksi joutuminen on vaikuttanut organisaatioon ja miten tilanteesta on selviydytty.

1.2 Tutkimuksen lähtökohta ja rajaukset

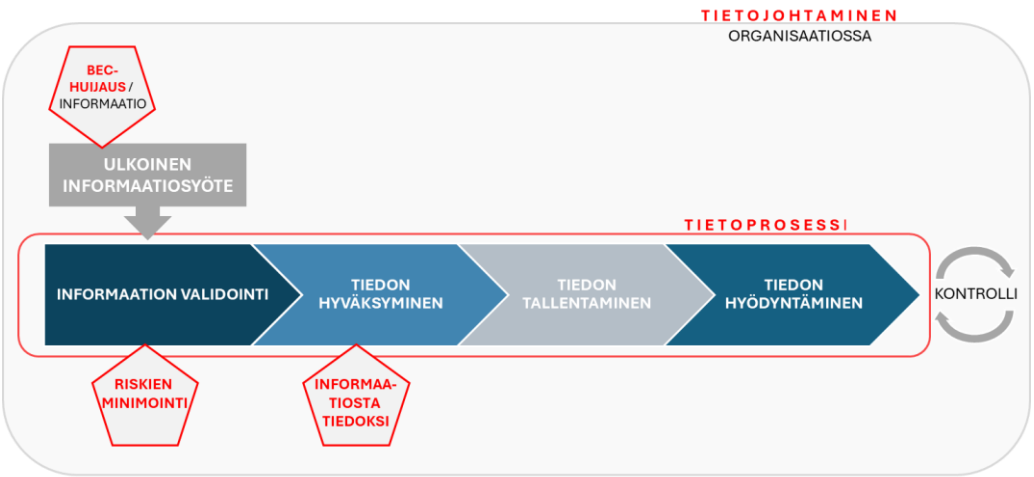
Olen työskennellyt maksamisen ja rahaliikenteen parissa jo pitkään. Koin aihealueen mielenkiintoiseksi tutkia, koska erilaiset huijaukset ovat rahaliikenteessä yleinen ilmiö. Teknologian kehittyessä myös huijausmahdollisuudet ovat murroksessa. Siinä missä alan kehitys luo uusia mahdollisuuksia palvella yhteiskunnan toimijoita laadukkaammin ja tehokkaammin, myös lieveilmiöt, kuten huijaaminen, muuttavat muotoaan teknologisen kehityksen edetessä ja alati muuttuvassa kansainvälisessä maksamisen ympäristössä. Kiinnostavaa on myös pohtia miksi huijaukset niin usein toimivat. Huijauksiin sortuminen on periaatteessa estettävissä, mutta kuitenkin käytännössä näin ei usein tapahdu. Miksi näin on ja voidaanko asiaan vaikuttaa? Aihe on tärkeä, jotta rahallisilta tappioilta ja mahdolliselta mainehaitalta vältyttäisiin, mutta myös rahaliikenteen parissa työskentelevien näkökulmasta. On raskasta tehdä työtä manipuloinnin ja huijatuksi tulemisen pelossa. Tietojohtamisen opintojeni aikana huomasin monesti pohtivani, miksi informaation tai tiedon validointi ei tuntunut olevan mukana tietoprosessien kuvauksissa eikä myöskään läsnä tietojohtamisen artikkeleissa. Käsittelin muutamissa kurssitehtävissäni tätä aihetta ja se kiehtoi minua niin paljon, että halusin sen elementiksi myös pro gradu tutkielmaani.

Finanssiala on erittäin kattava ja monisäikeinen kokonaisuus, myös rahaliikenne ja maksaminen ovat laajoja aihealueita. Tässä tutkielmassa tutkimuksen kohteena on tarkemmin maksamisen osalta hetki, kun maksava osapuoli tekee päätöksen tilinumeron käyttämisestä maksamiseen. Tutkielmassa sekä maksaja, että maksun saaja ovat organisaatioita. Kuten johdannossa on todettu erilaiset väärinkäytökset ovat vahvasti läsnä oleva uhka rahaliikenteessä. Näistä väärinkäytöksistä tässä tutkielmassa keskitytään riskitekijänä BEC-huijauksiin.

On myös hyvä huomioida, että ostolaskut kulkevat yrityksissä aina ostolaskujen hyväksymisprosessin kautta. Prosessin tarkoitus on varmistaa, että lasku on aiheellinen ja oikean sisältöinen. Laskut eivät koskaan mene maksatukseen ilman tämän prosessin läpäisemistä. Ostolaskujen hyväksynnässä on aina mukana henkilö, joka on sopinut kyseisen oston. Hänellä on tieto mitä on hankittu ja mitä on sovittu. Tämä prosessi ei ole tämän tutkielman tutkimuskohteena. Tässä tutkielmassa kohdistetaan huomio siihen yksittäiseen kohtaan tai hetkeen osana isompaa kokonaisuutta, jossa tilinumerotiedon todenperäisyys hyväksytään käyttöön tai vaihtoehtoisesti hylätään.

1.3 Teoreettinen tausta ja keskeiset käsitteet

Tässä luvussa esitellään tutkimuksen teoreettinen tausta tiivistetysti sekä hieman tarkemmin sen keskeiset käsitteet. Etsiessäni vastausta asettamalleni tutkimuskysymykselle ja alatutkimuskysymyksille muodostui tutkimukselle kuviossa 1. hahmoteltu teoreettinen tausta. Tästä teoreettisesta taustasta löytyi tutkittavan ilmiön sisältämät tietojohtamisen elementit sekä yhteys riskienhallintaan tietojohtamisen näkökulmasta. Kuvion jälkeen listasin lyhyet kuvaukset teoreettisen taustan pääkäsitteistä, jotka on kuviossa korostettu lihavoinnilla ja punaisella värillä.



Kuvio 1. Teoreettisen taustan keskeiset käsitteet

Teoreettinen tausta rakentuu kuviossa tietojohtamisen viitekehykseen sisään, jossa seurataan informaation validointia tiedoksi tai sen hylkäämistä BEC-huijauksena. Keskiössä on, mikä on tietojohtamisen rooli tieteenalana, kun tietoa validoidaan ja mahdollisilta uuden informaation tuomilta riskeiltä suojaudutaan.

Tietojohtaminen (knowledge management) on tieteenalana vakiintunut, mutta uudehko ala, joka keskittyy tiedon ympärille syntyviin johtamiskysymyksiin. Keskiössä ovat tietojohtamisen käytänteet kuten tiedon strateginen johtaminen ja organisaation tietomyönteinen kulttuuri ja käytänteet. Tehokas tiedon hyödyntäminen tietojohtamisen malleja ja välineitä hyödyntäen parantaa organisaation suorituskykyä pohjautuen tietoon ja osaamiseen. Tämä korostuu informaation määrän lisääntyessä nykyaikaisessa tietoyhteyskunnassa. (Laihonen, Hannula, Helander, Ilvonen, Jussila, Kukko, Kärkkäinen, Lönnqvist, Myllärniemi, Pekkola, Virtanen, Vuori & Yliniemi 2013; Kianto 2011.) Tietojohtaminen on oleellisen tiedon tunnistamista, tallentamista ja suojaamista, jotta tietoa päästään hyödyntämään organisaatiossa strategisesti (Perrot 2006, 524).

Tieto (knowledge) on organisoitua informaatiota, jolla on merkitys. Merkitys ilmenee ymmärryksenä eli kun tieto ymmärretään ja sitä osataan hyödyntää niin, että se vaikuttaa ajatteluun tai tekemiseen (Bhatt 2000, 16; Kianto 2011, 6). Kuviossa 1. ulkopuolelta tulleesta informaatiosyötteestä tulee tietoa siinä vaiheessa, kun se on validoitu eli hyväksytty merkitykselliseksi, oikeaksi ja käyttökelpoiseksi.

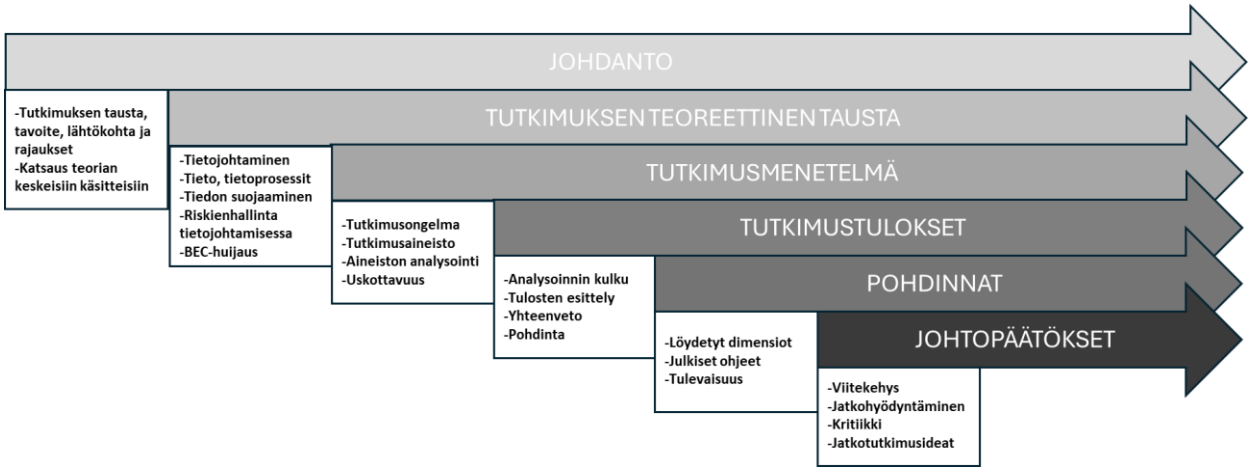
Tietoprosessit ovat erilaisia tapoja, joilla tieto organisaation sisällä liikkuu ja muuttuu. Esimerkkejä tietoprosesseista ovat tiedon hankkiminen, luominen ja hyödyntäminen. (Kianto 2011, 12.) Kuviossa 1. organisaatiossa käytössä olevaa tietoprosessia kuvaa polku ulkoisesta informaatiosyötteestä, tarkistetuksi tiedoksi, joka voidaan tallentaa ostoreskontraan tai vastaavaan järjestelmään ja hyödyntää.

Riskien minimointi ja riskiarvioi ovat oleellisia suorituskyvylle. Koska tieto on organisaatiolle tärkeä resurssi, monesti tärkein, organisaation tulisi turvata tietopääomansa. Tässä auttaa oman organisaation ja sen tietopääoman tunteminen. On hyvä varautua ja laatia riskiarviointi organisaation tietovarannosta, jossa tunnistetaan oleellinen tieto ja sitä kohtaavat uhat sekä mikä taho uhan aiheuttaa ja millä keinoilla. (Whitman & Mattord 2018; Jennex & Durcikova 2020.) Riskiarvioissa arvioidaan suojautumisen lisäksi, myös saavutettavissa oleva hyöty (Ilvonen, Jussila & Kärkkäinen 2015).

BEC-huijaus (business e-mail compromise) on yleinen sähköpostitse toteutettava huijaus. Uhria lähestytään sähköpostitse tarkoituksena kalastella tietoja huijaustarkoituksessa, pyydetään maksusuoritusta erityistilanteeseen vedoten tai ilmoitetaan kauppakumppanin tilinumeron muutoksesta. (Hitesh, Aniruddh, Aniruddh & Shubha (2022); FBI 2022.)

1.4 Tutkielman rakenne

Pro gradu -tutkielma koostuu kuudesta luvusta kuvion 2. mukaisesti. Tutkielma alkaa johdannosta, jota seuraa kuvaus teoreettisesta taustasta luvussa kaksi. Kuvion mukaisesti teoria rakentuu tietojohtamisen kontekstissa ja myös rikienhallintaa käsitellään tästä näkökulmasta.

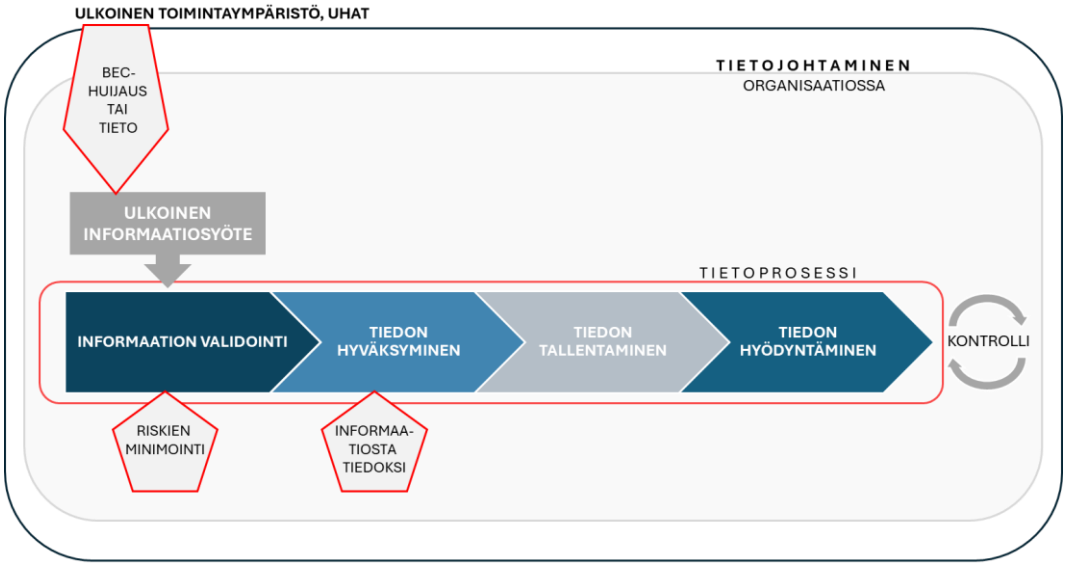


Kuvio 2. Pro gradu -tutkielman eteneminen

Kolmannessa luvussa esitellään tutkimuksessa käytetty tutkimusmenetelmä, joka sisältää tiedonhankintastrategian, tutkimuksen kulun, analyysimetodin ja tutkimuksen uskottavuuden elementit. Neljännessä luvussa esitellään tutkimustulokset. Viidennessä luvussa esitellään pohdinnat kolmen aineistoanalyysissä löydetyn dimension, virallisten ohjeiden ja tulevaisuuden näkökulmista. Viimeisessä, kuudennessa luvussa esitellään tutkimuskokonaisuudesta esiin nousseita näkökulmia kehitetyn viitekehyksen muodossa sekä esitellään ajatuksia tutkimuksen jatkohyödyntämisestä ja jatkotutkimusaiheista.

2 Tutkimuksen teoreettinen tausta

Luvussa kaksi esitellään tämän pro gradu -tutkielman teoreettinen tausta, joka on havainnollistettu kuviossa kolme. Tässä osuudessa esitellään tutkimuskirjallisuudesta tehtyjä löydöksiä, jotka tukevat tutkielman etenemistä kohti luvussa yksi kuvatun tutkimusongelman ratkaisua eli tutkimuskysymyksiin vastaamista. Teoriaosuus on koostettu etsimällä tietoa hakusanojen avulla akateemista tutkimustietoa tarjoavista lähteistä kuten Primo ja Google Scholar. Tietojohtamisen tutkimusalueen teorioita on ammennettu myös opinnoista ja opintomateriaaleista. Koska tutkittu aihealue oli ammattini kautta tuttu hain myös varmistusta omille tiedoilleni eri lähteistä kuten Euroopan Keskuspankin sivustot. Luettelo kaikista tutkielmassa käytetyistä lähteistä löytyy lähdeluettelosta.



Kuvio 3. Tutkimuksen teoreettinen tausta

Tässä luvussa käsitellään ensin (2.1) tietojohtamista tienteenalana, tieto ja tietoprosessi käsitteet sekä tiedon suojaamisen aihealuetta. Tämän jälkeen toiseksi (2.2) riskien hallintaa tietojohtamisen kontekstissa, BEC-huijauksia sekä viranomaisohjeistuksia liittyen huijauksiin. Viimeisenä (2.3) koonti tietojohtamisen roolista riskienhallinnassa.

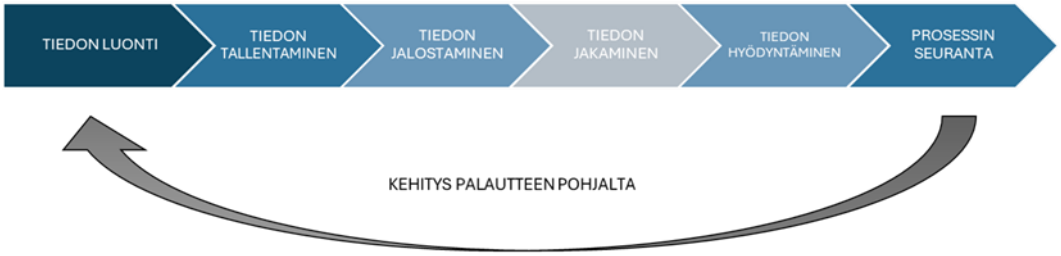
2.1 Tietojohtaminen

Tietojohtaminen on osa laajempaa tieteenalojen vuoropuhelua, koska tieto on luonteva ja tärkeä osa kaikkea tekemistä alasta ja tilanteesta riippumatta. Tietojohtamisen sisällä on erilaisia painopisteitä. Voidaan keskittyä olemassa oleviin resursseihin, tietoprosessin elementteihin, oppimiseen, tiedon jakamiseen, työkaluihin ja niin edelleen. (Perrot 2006.)

Tietojohtamisen käytänteitä voi kuvata johtamistapana ja johtamisen kulttuurina, joka tukee tietoprosesseja. Tietojohtamien on kiinteä osa monia organisaation johtamisen paikkoja, kuten strateginen johtaminen, vallalla oleva johtamisenkulttuuri tai henkilöstöhallinto. Tietojohtaminen on ajattelutapa, joka yhdistää tiedon, tietoprosessien kautta, organisaation johtamisenkysymyksiin. Tietojohtamisen keskiössä on arvonluominen tiedon avulla, vaikka se on eräänlainen taustavaikuttaja. Tietojohtaminen ei ole erillinen funktio, vaan se on ennemminkin ja parhaimmillaan sisäänrakennettuna organisaation toimintatapoihin. Kun tietojohtaminen on osa organisaatiokulttuuria, puitteet tietopohjaiselle arvonluonnille on luonnostaan olemassa kaikessa tekemisessä. Kun organisaation supervoima on, sisäänrakennetut tietojohtamisen periaatteet, organisaatio on herkkä myös tunnistamaan ja purkamaan tietojohtamisen esteistä, jos niitä ilmenee. (Kianto 2011; Laihonen et al. 2013.) Tietoprosessien ja tietojohtamisen keinojen ero on, että tietoprosessit syntyvät organisaatioihin tekemisen kautta esimerkiksi tietoa jaetaan, vaikka siitä ei olisi erikseen suunniteltu tai päätetty. Johtamisen käytänteet taas systemaattisesti tukevat tiedon hallintaa ja käyttöä tietoperusteisen johtamisen kautta. Tietojohtamisen työkaluilla parannetaan tietoresurssien ja tietoprosessien käyttöä ja toimintaa kokonaisuutena. Esimerkiksi miten parantaa tiedon hyödyntämistä tai miten välttää tietoon liittyviä riskejä. (Andreeva & Kianto 2012.)

Tietoprosessia kannattaa katsoa sisäänrakennettuna tietojohtamisen elementtinä, joka toteuttaa itseään luonnollisen osana toimintaa. Kuvio 4. on yksi tapa osoittaa tietoprosessin etenemistä alkaen tiedon luomisesta, jatkuen tiedon keräämisen ja tallentamisen prosesseihin, tiedon jalostamiseen, tiedon jakamiseen ja hyödyntämiseen. Toimivassa tietojohtamisen ympäristössä prosessia monitoroida sen käytettävyyden ja tiedon oleellisuuden näkökulmista. Jatkuvasti kehittäen palautteen pohjalta ja muuttuva maailma huomioon ottaen. Prosessin

syötteistä, toteutuksista ja lopputuloksista vastaavat tietotyöläiset. (Davenport & Völpel 2001.)



Kuvio 4. Tietojohtamisen prosessikuvaus (mukaille Davenport & Völpel 2001, 217).

Tiedonhallinta on mukana prosessin kaikissa vaiheissa. Tietoprosessit ovat jatkuvasti liikkeessä. Tämä tekee hallintaprosessista dynaamisen ja jatkuvan tehtävän. Organisaatio ja sen jäsenet ovat näin ollen mukana useissa prosesseissa saman aikaisesti. (Alavi & Leidner 2001.) Myös tietojärjestelmien tiedonhallintaan tulee katsoa tietojohtamisen kautta. Tiedon turvallisuuteen liittyvän osaamisen ei tulisi antaa olla hajallaan organisaatiossa niin, että asiantuntijoiden osaaminen jää heidän hiljaiseksi tiedokseen. Tämä osaaminen tulisi valjas-taa tehokkaammin osaksi organisaation suunnittelua, päätöksenteko ja rutiineja. (Belsis, Spyros & Evangelos 2005.) Akhavan ja Zahedi (2014) havaitsivat, että yksi menestymiste-kijöistä tietojohtamisessa on organisaation tietorakenne. Miten tietoon liittyvät liiketoimin-taa tukevat prosessit ja menettelytavat on suunniteltu ja toteutettu. Tietorakenne voidaan nähdä myös käytössä olevana ohjenuorana, joka pitää sisällään ohjeistuksen ja standardit, joita on päätetty seurata tavoitteiden saavuttamiseksi. Tämän logiikan tulee olla samanaikai-sesti tarkoituksen mukainen ja riittävän tarkka, mutta myös muutettavissa tilanteiden muut-tuessa. Tiedon jakamista on hyvä stimuloida tarjoamalla sille aikaa ja tapoja toteutua. Ta-voitteena tulisi olla tiedonjakamisen rutinointi luontevaksi osaksi toimintaa. Psykologisesti turvalliseen ja inspiroivaan organisaatiokulttuurin panostaminen johdon toimesta luo he-delmällisen maaperän tiedonjakamiselle. (Akhavan & Zahedi 2014.)

Tiedon turvaamisessa ovat tärkeässä roolissa sekä tekniset työkalut että organisaation suuntaviivat ja yksilöt. Tietämyksen jakaminen ja kasvattaminen sekä uuden tiedon luominen ovat seurausta yksilöiden välisistä sosiaalisista prosesseista. Tietojärjestelmien tulisi tukea tätä prosessia edistämällä parhaaseen lopputulokseen pääsemistä. Tutkijat keskittyvät listaamaan viisi tietojohtamisen prosessia, joita tietohallinnanjärjestelmien tulisi sisältää tukeakseen tietoturvallisuutta. (Belsis et al. 2005.) Ensimmäinen on personointi, jossa tietoa jaetaan henkilöiden välisessä kontaktissa kuten keskustelut tai chatit. Kun fokuksessa on organisaation tietopääomaa uhkaavat asiat, on tärkeää löytää kommunikointikanavat tätä osaamista omaavien yksilöiden välille organisaation sisällä. Jotta organisaation tietojärjes-telmät ja käytänteet hioutuvat toimiviksi on myös käytetyllä kielellä merkitystä. Kaikkien pitää ymmärtää käytössä oleva terminologia ja käsitteet saman sisältöisinä. Toisena, myös kodifiointivaihe vaatii tarkkaa suunnittelua, jotta tieto tallennetaan järjestelmiin oikein, myös tässä yhtenevä terminologia on tärkeää. Tietojärjestelmien hyödyntäminen ja apu on välttämätöntä nykyisessä tietotulvassa ja jotta kussakin tilanteessa hyödynnettävää tietoa ylipäänsä kyetään löytämään ja poimimaan käyttöön aina tarvittaessa. Kolmannessa vai-heessa, kun jossa tietovarannosta tehdään löytöjä, tietoa haetaan ja etsitään käyttötarkoi-tuksen mukaisesti. Tietoa haetaan ja yhdistellään eri tietolähteistä myös organisaation ulko-puolisista lähteistä täydentämään organisaation omaa tietoa. Neljännessä vaiheessa uusi tieto on tulos yksilöiden tiedoista nousevien tietolöydösten yhdistymisestä ja jalostumisesta uudeksi tiedoksi. Tämä nähdään tietojohtamisessa kilpailukyvyn edellytyksenä. Viimeinen askel on seuranta. Rikollisten huijausyrityksiltä suojautuminen vaatii tauotonta seurantaa, kuten aiemmin on jo useasti mainittu rikolliset eivät pysähdy. Täysin uusia ja taidokkaam-min toteutettuja huijauksia esiintyy koko ajan. Siinä missä teknologia mahdollistaa tehok-kuutta ja nopeutta laajalla rintamalla se tarjoaa tätä kaikkea myös rikollisille. (Belsis et al. 2005; Milton, Shadbolt, Cottam & Hammersley 1999.)

Goode & Lacey (2022) painottavat, että tietoturva sekä tietoprosessien heikkoudet ja haavoittavuudet kannattaa nähdä oleellisen osana tietojohtamista. Jennex ja Zyngier (2007) huomioivat muiden tutkijoiden tapaan, että tietojohtamista käsittelevissä artikkeleissa ja teorioissa käsitellään todella vähän, jos ollenkaan, turvallisuutta. Pääasiassa keskitytään tiedon tallentamiseen, siirtämiseen ja soveltamiseen. Tavoitteena tutkimuksissa on pääasias-sa mainittu kilpailukyvyn lisääminen ja välillä myös suorituksen parantaminen organisaa-tiossa.

He tulkitsevat, että tietojohtamisen näkökulmasta turvallisuusnäkökulmia voidaan pitää eräänlaisina esteinä, koska niiden huomioonottamisen voi nähdä haittana tiedon jaka-miselle. Organisaation tietopääomaa pidetään tärkeänä, joten monet tutkijat pitävät tämän kautta itsestään selvänä, että tiedon ja tietoprosessien turvallisuuden tärkeys on annettu tekijä. Tämän takia tutkimuksissa katsotaan, että turvallisuutta ei tarvitse erikseen alleviivata. Koetaan, että turvallisuus on prosesseissa ja tietojärjestelmissä sisäänrakennettua. (Jennex ja Zyngier 2007.)

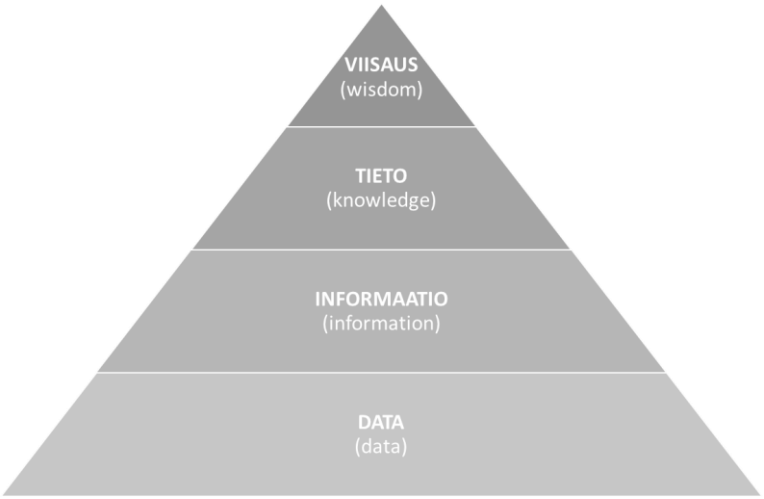
Kasvavassa määrin myös maailman digitalisoituminen haastaa tietojohtamisen perinteisiä teorioita, kun tavat kommunikoida muuttuvat esimerkiksi kasvotusten tapahtuvasta keskusteluista ja palavereista online palavereihin ja chat-keskusteluihin. (Ilvonen, Thalmann, Manhart & Sillaber 2018, 239)

Perrot (2006, 524) kuvaa tietojohtamista oleellisen tiedon tunnistamiseksi, tallentamiseksi ja suojaamiseksi, jotta tietoa päästään hyödyntämään organisaatiossa strategisesti. Tämä tieto-johtamisen kuvaus osoittaa tietojohtamisen alueen laajuuden. Tietojohtamisen elementeillä on toiminnallista vaikutusta, mutta myös erittäin voimakas strateginen vaikutus päätöksen tekoon, kun punnitaan mahdollisuuksia ja uhkia. Kyseessä on jatkuva prosessi, koska ympä-ristö muuttuu alati ja tietoa kertyy koko ajan. Tiedon korostuminen tärkeimpänä resurssina on kummunnut nopeasti muuttuvasta ja vaativasta ympäristöstä ja korostuu jatkossakin. Tiedon merkityksellisyys ja oikea-aikainen käyttö sekä tietojohtaminen korostuvat jatkossa-kin. (Perrot 2006.)

2.1.1 Tieto

Tieto on tietojohtamisen ytimessä. Tieto syntyy organisoidusta informaatiosta, joka kytkeytyy yksilön, joka on tiedon haltija, näkemyksiin ja ymmärrykseen. Tieto tai tietämys on dynaamista ja kontekstiin sidottua. Tieto syntyy yksilöiden ja organisaatioiden välisessä sosiaalisessa vuorovaikutuksessa ja se on riippuvaista tietystä ajasta ja paikasta. Jos dataa tai informaatiota ei laiteta kontekstiin, ne ovat vain irrallisia muruja, jotka eivät muodosta tietoa. Tiedolla on merkitys, jota pyritään välittämään. Datasta ja informaatiosta tulee

merkityksellistä ja hyödynnettävissä olevaa tietoa vasta, kun yksilöt tulkitsevat sitä, asettavat sen kontekstiin ja liittävät sen mukaan olemassa oleviin tietokokonaisuuksiin. Tiedon tai tietämyksen voi ajatella tästä vielä kehittyvän edelleen viisaudeksi. Data jalostuu matkalla viisaudeksi kuviossa 5. kuvatusti, kun sitä työstetään eteenpäin yhdistämällä, analysoimalla ja kun siihen liitetään näkemyksiä. (Nonaka 1994; Nonaka, Toyama, & Konno, 2000; Laihonen et al. 2013; Rowley 2007; Bhatt 2000.)



Kuvio 5. DIKW-malli (mukaillen Rowley, 2007, 164).

Tieto nähdään kaikilla aloilla tänä päivänä yritysten tärkeimpänä resurssina. Tieto on korvannut muut perinteisemmät resurssit. Näin ollen tiedon turvaaminen kaikissa tilanteissa on ensiarvoisen tärkeää organisaatioiden menestykselle. (Martelo-Landroguez, Navarro ja Cepeda-Carrión 2019; Randeree 2006; Bhatt 2000.) Koska tieto nähdään organisaation arvokkaimpana resurssina, on myös tietojohtamisen tutkimus kasvattanut suosiotaan viime vuosikymmeninä. Halu tietää enemmän, tietää tarkemmin ja analysoida miten tietoa voidaan hyödyntää paremmin, ovat alati kasvussa. (Hussinki, Kianto, Vanhala & Ritala 2017.) Sen lisäksi, että tieto on voimavara ja mahdollisuuksien luoja, sen ympärillä on myös havaittavissa riskejä. Tiedon riskitekijät on vähemmän tutkittu alue, kuin tiedon hyödyntämistä käsittelevät aihealueet. (Durst, Hinteregger & Zieba 2019, 8.)

Tieto voidaan erotella kahteen eri tyyppiin eksplisiittiseen ja hiljaiseen tietoon. Eksplisiittinen tieto on kodifioitua ja sitä on suhteellisen helppo käsitellä esimerkiksi tallentaa, siirtää ja jakaa. Hiljainen tieto taas on henkilöiden henkilökohtaista tietoa kuten subjektiiviset näkemykset, kokemukset ja intuitio. Hiljainen tieto on juurtunut toimintaan, rutiineihin, tapoihin, arvoihin ja tunteisiin, joten sitä on näin ollen vaikeampi käsitellä ja saattaa esimerkiksi kirjalliseen muotoon. Hiljaisen tiedon jakaminen vaatii vastaanottajalta kykyä omaksua tarjolla olevaa tietoa. Sekä eksplisiittinen että hiljainen tieto ovat merkityksellisiä uuden tiedon luomisessa. Tieto syntyy näiden kahden tietotyypin välisen vuorovaikutuksen kautta. (Nonaka et al. 2000.)

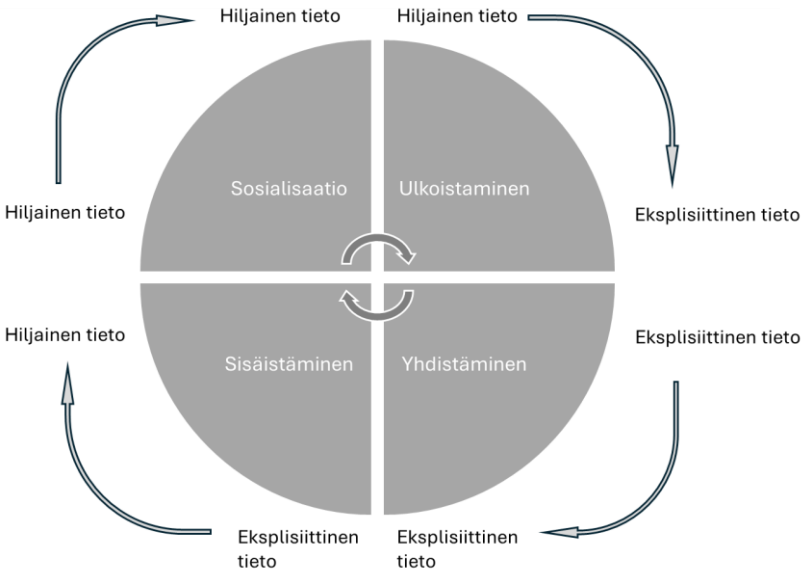
Kun mietitään tietoon liittyviä riskejä kunkin organisaation näkökulmasta, täytyy tunnista mikä on organisaatiolle olennaista tietoa. Tärkeä tieto tulee tunnistaa tietoprosessin kaikissa osissa ja riskienhallintatoimenpiteet tulee kohdistaa tämän perusteella oikein. Oleellista on aina ottaa huomioon hiljainen tieto. (Jennex, Durcikova & Ilvonen 2022.)

2.1.2 Tietoprosessit

Kianto (2011, 12) kuvaa tietoprosesseja tiedon tavoiksi liikkua ja uusiutua organisaatioissa. Kirjallisuudessa on kuvattu paljon erilaisia tietoprosesseja, mutta tyypillisimmillään kuvataan tiedon hankkimisen, luomisen ja hyödyntämisen keinoja. Alavi ja Leidner (2001, 114) kuvaavat tietojohtamisen neljää tietoprosessia seuraavasti; tiedon luominen, tiedon siirtäminen, tiedon varastointi ja hakutoiminnot sekä tiedon soveltaminen ja hyödyntäminen. Prosessit täydentävät ja mahdollistavat toistensa toteutumisen luoden tietojohtamisen kokonaisuuden. Tässä teoriassa nähdään organisaatio tietojärjestelmänä, joka kattaa sekä kognitiivisen että sosiaalisen ulottuvuuden rakentaen niistä toisiinsa kietoutuvan sarjan toimintoja. (Alavi & Leidner 2001.) Tietojohtaminen on tietoprosessi, jossa tietoa luodaan (knowledge creation) eli organisaatiolla on kyky luoda uusia ideoita ja ratkaisuja. On hyvä muistaa, että aina ei ole tarvetta luoda pyörää uudelleen vaan uuden luominen voi olla myös vanhan uudelleen soveltamista tai panostamista eri osa-alueisiin. Pitää löytyä myös kyky arvioida (knowledge validation) käytössä olevaa tietoa ja osaamista, onko tieto validia tai tarvitaanko uutta osaamista muutoksien myötä. Kolmanneksi tieto tulee kyetä esittämään (knowledge presentation) tehokkaasti organisaation eri osastoille ja jäsenille sekä jakamaan (knowledge

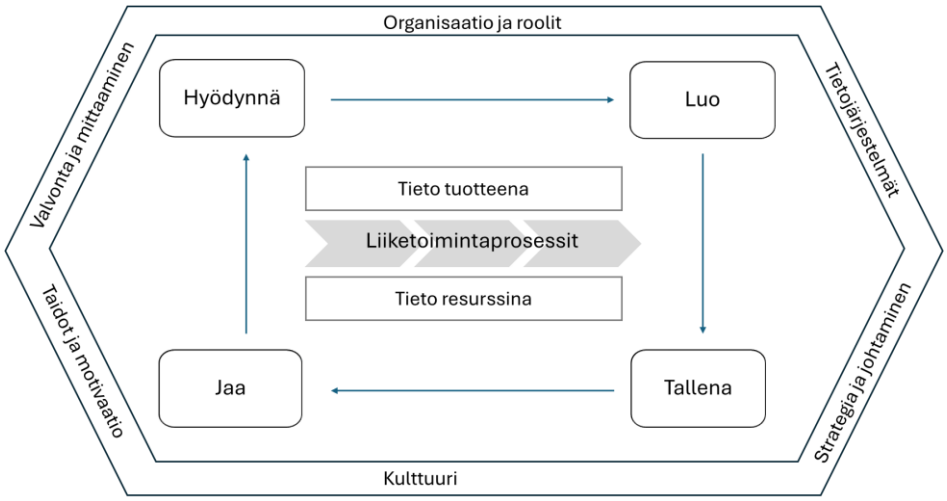
distribution) kattavasti. Viimeiseksi tiedon ja osaamisen tulee olla hyödynnettävissä ja sovellettavissa (knowledge application) organisaation prosesseissa. Tämä tietojohtamisen kiertokulku edesauttaa pitämään yllä ydinosaamista oppimalla, reflektoimalla, poisoppimalla ja uudelleen oppimalla. (Bhatt 2001.)

Nonakan et al. (2000, 5) mukaan tiedon luominen on prosessi, joka sisältää kolme elementtiä. 1) SECI-mallissa, jota kuvio 6. havainnoi, luodaan uutta tietoa hiljaisen ja eksplisiittisen tiedon vuorovaikutuksessa. Hiljaista tietoa rakennetaan ja muunnetaan prosessissa laajemmaksi kokonaisuudeksi laadultaan ja määrältään. Tämä tapahtuu neljällä eri tavalla: sosialisaatio, ulkoistaminen, yhdistäminen ja sisäistäminen. Tiedon sosialisaatiossa (socialization) hiljainen tieto välittyy yksilöiden välisessä vuorovaikutuksessa. Ulkoistamisessa (externalization) hiljainen tieto muutetaan eksplisiittiseksi tekemällä siitä tulkittavaa kuten ohjeet tai prosessikuvaus. Tässä vaiheessa tiedon käytettävyys laajenee isommalle joukolle. Tämä mahdollistaa uuden tiedon luomisen. Yhdistämisessä (combination) edellisessä vaiheessa ulkoistettu eksplisiittiseksi muunnetusta tiedosta on mahdollista koota suurempia kokonaisuuksia yhdistämällä uutta tietoa vanhaan tietoon tai muihin tietoihin. Tässä vaiheessa tietoa voidaan ryhtyä analysoimaan tarkemmin. Tiedon käytettävyys kasvaa. Viimeisenä SECI-mallissa tulee sisäistäminen (internalization). Tässä vaiheessa eksplisiittinen tieto saavuttaa tason, jossa se sisäistetään ja ymmärretään. Tässä prosessissa tieto sisäistyy jälleen henkilökohtaiseksi ymmärrykseksi ja muuttuu yksilökohtaiseksi hiljaiseksi tiedoksi, jota voi jälleen jakaa eteenpäin sosialisaation kautta ja niin edelleen. Malli korostaa miten yksilöiden välillä tapahtuva tiedon jakaminen keskusteluissa ja ylipäänsä kaikessa vuorovaikutuksessa mukaan lukien uudemmat tavat kommunikoida kuten chatit, luovat organisaatiolle uutta tietoa. SECI on spiraali, jossa tieto kehittyy prosessin edetessä spiraalissa vaiheesta toiseen aina uudelleen lisäten ja rikastuttaen edetessään organisaation tietopääomaa. 2) BA on vaihe, jossa organisaation tietoa luodaan ja jaetaan hyödynnettäväksi. Vaihe korostaa vuorovaikutuksen merkitystä tiedon luomisen mahdollistajana. 3) Tietovarat ovat organisaatiokohtaisia resursseja. Nämä resurssit toimivat tiedon luomisessa syötteinä, tuloksina ja välittäjinä. Tietotaito, organisaatiokulttuuri ja brändi ovat esimerkkejä tietovaroista. (Nonaka et al. 2000.)



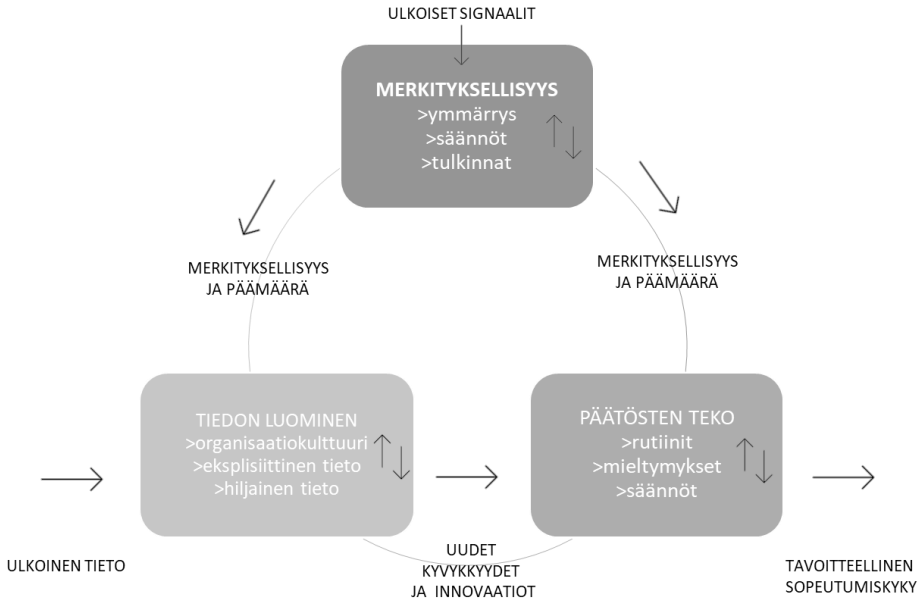
Kuvio 6. SECI-malli (mukaillen Nonaka et al. 2000, 12).

Tehokas ja toimiva tietojohtaminen kietoutuu yrityksen ydinliiketoiminnan ympärille. Organisaation tietoprosessin tulee olla hyödyksi liiketoiminnan avainprosesseille. Heisig (2009, 15) on listannut, että tiedon systemaattinen hyödyntäminen pitää sisällään neljä vaihetta tiedon luonnin, säilyttämisen, jakamisen ja käyttämisen eli hyödyntämisen. Tieto on käytössä oleva resurssi ja osa liiketoimintaa, mutta myös liiketoiminnasta syntyvä sivutuote. Tätä sivutuotetta voi myös hyödyntää toistuvasti ja parhaimmillaan myös muussa käytössä, kuin missä se on alun perin syntynyt. Millaista tietoa syntyy ja millaisessa muodossa sitä hyödynnetään, on yrityksen määriteltävissä omien tarpeiden mukaan. Heisigin GPO-WM Framework (kuvio 7.) tuo esiin myös mahdollistaja näkemyksen. Sen mukaan toimivaan tietojohtamiseen vaikuttavat organisaatiossa kattavasti mahdollistajat, joita ovat yrityksen kulttuuri, organisaatio ja sen sisällä olevat roolit, yrityksen strategia ja johtajuus, työntekijöiden taidot ja motivaatio, millainen kontrolli organisaatiossa vallitsee ja miten toimintoja ja suoritusta mitataan sekä millaista teknologiaa käytetään. Onnistumisen nähdään olevan kiinni kaikista näistä mahdollistajaosa-alueista, mutta kombinaatiot ja painopistealueet vaihtelevat organisaatiosta toiseen. (Heisig 2009.)



Kuvio 7. GPOWM Framework -rakenne (mukaillen Heisig 2009, 15)

Kun viestit organisaation ulkopuolelta ovat epämääräisiä, organisaatiossa yhteisesti koettu merkitys tekemiselle ja päämäärä vähentävät epävarmuuden tunnetta. Yhteinen merkityksellisyyden ilmapiiri ei kuitenkaan ole muuttumaton, vaan se päivittyy ympäristön muutosten ja tilanteiden mukaan. Tämä liike on tärkeää, jotta organisaatio voi varmistaa, että sen tavoitteet pysyvät ajan tasalla ja kuitenkin sen toivotun lopputuloksen mukaisina muuttuvassa ympäristössä. Merkityksellisyyden ja päämäärän puitteissa organisaatio hyödyntää kyvykkyyksiään sekä kehittää niitä ja luo uutta osaamista. Näiden avulla se pyrkii saavuttamaan tavoitteensa. Prosessissa tulee vastaan myös puutteita osaamisessa ja saatavilla olevassa tiedossa. On oleellista tunnistaa nämä tietotarpeet eli puutteet käytössä olevassa tiedossa tai osaamisessa, jolloin herätteenä ulkoiseen impulssiin organisaation jäsenet lähtevät korjaamaan tunnistettuja puutteita. (Choo 2001; Laihonen et al.2013.) Korjausliikkeessä hyödynnetään muun muassa eksplisiittisen ja hiljaisen tiedon jakamista, eri tietojen linkittämistä toisiinsa ja ulkoista tietoa. Lopputuloksen syntyy uutta tietoa ja uutta osaamista. Näillä innovaatioilla saatetaan luoda uusia tuotteita ja palveluita tai parannetaan tietoprosesseja kuten lisätään tehokkuutta, ongelmaratkaisukykyä ja suorituskykyä. Prosessin nähdään parantavan organisaation toimintakykyä pitkällä aikavälillä, mutta koska uudistamisessa on aina myös riskejä, vaaditaan mukaan myös päätöksentekoa. Choon (2001) luoma organisaation tiedonhallinnan -malli kuviossa 8. sisältää kaikki kolme edellä kuvattua elementtiä; ulkoisen signaalin tarpeesta muutokselle, tiedon luomisen ja päätöksenteon.



Kuvio 8. Organisaation tiedonhallinta -malli (mukaille Choo 2001, 200)

Organisaation kulttuuri määrittää lähtökohdat, uusi tieto tarjoaa uusia vaihtoehtoja ja lopuksi kokonaisuudesta muodostuu päätös aktivoida uusia toimintatapoja ja muuttaa aiempaa tekemistä. Usein päätöksentekoprosessi mukailee organisaation tuttuja tapoja arvioida, vertailla ja tehdä päätöksiä tämän pohjalta. Toisaalta välillä tilanne on niin uusi, että se luo uutta totuttuihin sääntöihin ja toimintaperiaatteisiin organisaatiossa. Tässä prosessissa organisaatiot myös lähenevät tavoiltaan toisiaan, kun kaikki reagoivat ympäristöön mukautumalla. Organisaatiot oppivat sopeutumaan ympäristön vaikutuksiin osana iteratiivista tiedonkäsittelyprosessia. (Choo 2001.)

2.1.3 Tiedon suojaaminen ja turvaaminen

Aiemmissa luvuissa kävimme läpi tietojohtamisenalueen peruselementtejä liittyen tietoon yleensä sekä tietoprosseihin. Tietojohtamisen artikkelit ja kirjallisuus käsittelevät paljon juuri näitä teemoja tiedon eri muodoista, tiedon jalostamisesta ja uuden luomiseen, säilyttämiseen, jakamiseen ja lopulta tiedon hyödyntämiseen. Kirjallisuudessa tiedon käyttöä mietitään myös pääasiassa tavanomaisten toimijoiden näkökulmista kuten organisaation jäsenet, asiakkaat tai sidosryhmien edustajat (Goode & Lacey 2022.) Näitä perusasioita on käsitelty myös tämän teoriaosuuden alkupäässä. Tutkimusongelmaan pureutuminen, vaati kuitenkin

kaivautumista syvemmälle kirjallisuuteen. Tiedon validointiin oli tarjolla huomattavasti vähemmän teoreettista aineistoa. Tietojohtamisen tutkimuksessa, uudempana ilmiönä, saa kuitenkin kasvavaa huomiota organisaation tiedon ja tietoprosessien suojaaminen ja turvaaminen (Goode & Lacey 2022; Murray & Durcikova 2014; Jonnex & Zyngier 2007).

Yleistäen tietojohtamisen tutkimusalueen perinteisenä riskinä on pidetty tiedon menettämistä esimerkiksi eläköitymisen ja työpaikan vaihdon tai menetyksen seurauksena. Tietoon liittyviä mahdollisuuksia hukataan myös organisaation omien puutteellisten tallentamisen, tiedon hyödyntämisen ja siirtämisen prosesseissa. (Ilvonen et al. 2018.) Ulkoisina riskeinä tiedon suojaamisessa keskitytään pääasiassa vain näkökulmiin, joissa tietoa ei jaettaisi vääärille tahoille tai liikaa niin, että siitä saatava hyöty menetettäisiin (Manhart &Thalmann 2015). On tunnistettu, että on olemassa kirjo erilaisia malleja, joilla voi ohjata organisaation toimintaa ja päätöksentekoa, mutta ne eivät yleensä tunnista virheiden ehkäisemisen tärkeyttä. Haitallisten ongelmien taustalla on kuitenkin yleensä tietovirhe, jota ei ole tunnistettu riittävän ajoissa. Ongelman juurisyy löytyy yleensä inhimillisistä prosesseista ei niinkään teknologisista haavoittuvuuksista. (Sveen, Rich & Jager 2007.) Jos taas katsotaan asiaa tietoturvan näkökulmasta, keskitytään luottamuksellisen tiedon suojeluun, tiedon eheyteen ja käytettävyyteen. Organisaatiossa käytössä olevien tietoprosesseihin liittyvien teknologioiden turvallisuus on totta kai tärkeää, mutta on hyvä tunnistaa, että se ei ole riittävä taso riskejä arvioitaessa. Suuri riski ovat työtekijät. Osaava henkilöstö on avainasemassa myös uhkientorjunnassa siinä missä muutenkin tietoprosesseissa. (Ilvonen, Jussila & Kärkkäinen 2015; Eslamkhah & Seno 2019.)

Ympäristössä, jossa uhat suuntautuvat organisaatiota, sen työntekijöitä ja asiakkaita vastaan, korostuu tietojohtamisen prosessien turvallisuuden ja prosessiin osallistuvien osaamisen varmistaminen. Henkilöstö on avainasemassa, kun suunnitellaan tietoon liittyviltä riskeiltä suojautumista. Organisaation tulee onnistua kasvattamaan tietoisuutta niin, että kaikki ymmärtävät riskit ja organisaation käytänteet suojautumiselle. Tämä vaatii tiedottamista, koulutusta ja riittävää pätevyyttä perustuen kunkin henkilön työtehtäviin. Rikollisten toimintaa edesauttavat ja helpottavat puutteet työntekijöiden osaamisessa ja riskien ymmärtämisessä, heikkoudet tietoprosesseissa, epäjohdonmukaisuus tiedonkulussa tai päätöksenteossa.

Organisaation tietojohtamisen prosesseissa ei saisi olla huomiotta jääneitä kuolleita kulmia, jotka mahdollistavat väärinkäytökset. (Goode & Lacey 2022; Prislan, Mihelic, & Bernik 2020.)

Wittman ja Mattord (2018) kuvaavat kirjassaan tietopääoman turvaamisen taktiikkaa suojautumisella uhilta kahden suuntaisesti. Ensinnäkin pitää tuntea oma organisaatio. Pitää tuntea oma tietovaranto ja mikä siinä on oleellisinta toiminnalle. Pitää tuntea koko tietoprosessin osalta käytetyt järjestelmät, toimintatavat ja mekanismit. Pitää myös tunnistaa haavoittumiselle alttiit kohdat ja mahdolliset puutteet. Toiseksi pitää tunnistaa uhat. Millaisia uhkia tietopääomaan kohdistuu ja missä kohtaa tietoprosessia uhkia voi ilmetä. Pitää myös pyrkiä tunnistamaan vihollinen mahdollisimman hyvin. Näin tunnistaa organisaatiolle tärkeän tiedon ja omat prosessit ja millaisia vihollisia eli uhkia voi tulla vastaan ja miten niiltä on paras suojautua. Jennex & Durcikova (2020) jatkavat, että tässä tunnistus- ja varautumisprosessissa oleellista on riskiarviointi. Oman organisaation tietovarannon tunnistus ja sitä kohtaavat uhat sekä mikä taho uhan aiheuttaa ja millä keinoilla. (Whitman & Mattord 2018; Jennex & Durcikova 2020.)

Goode & Lacey (2022) kuvaavat kiinnostavasti tietoa, joka koskee organisaation heikkouksia ja haavoittuvuuksia termillä dark knowledge. Kuvattuja heikkoja kohtia voi löytyä toimijoista, prosesseista sekä toimintaperiaatteista. Organisaation kannalta olisi tärkeää tunnistaa omat pimeät kulmat laajasti, ja joko poistaa ne tai mikäli tämä ei ole täysin mahdollista niin vähintään lisätä prosessiin läpinäkyvyyttä ja kontrollointia. Tästä voi käyttää esimerkkinä maksamiseen liittyvä työtehtävä, joka on aiemmin ollut mahdollista toteuttaa yhden henkilön toimesta, mutta vaatiikin jatkossa toisen ihmisen hyväksynnän. Dark knowledge -konsepti pitää sisällään sisäiset uhat, joissa organisaation jäsen tai asiakas tunnistaa heikkouden ja päättyy hyödyntämään sitä omaksi hyväkseen. Toinen vaaratekijä ovat ulkoiset toimijat kuten kilpailijat ja rikolliset. Ulkoinen toimija voi käyttää havaittuja heikkoja ja haavoittuvia kohtia esimerkiksi teolliseen vakoiluun tai rikoksen toteuttamiseen. (Goode & Lacey 2022.)

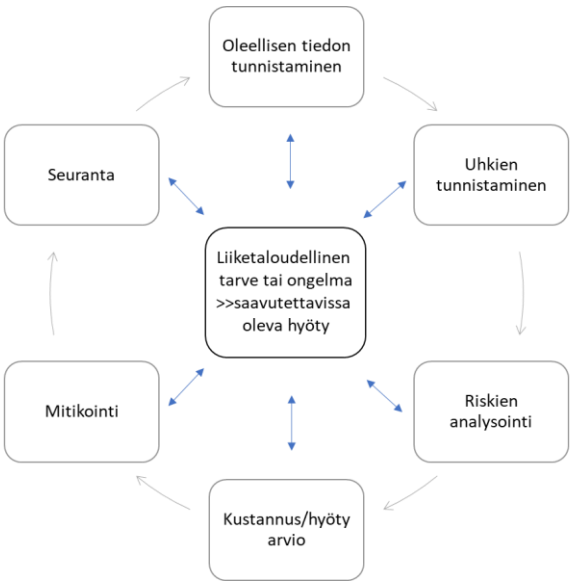
2.2 Riskienhallinta tietojohtamisen kontekstissa

Työssä pureudutaan tietojohtamisen rooliin riskienhallinnassa, kun organisaatiossa pyritään suojautumaan uuden tiedon käyttämiseen liittyviltä riskeiltä. Miten onnistutaan havaitsemaan ulkoisista tietosyötteistä ongelmat tai tiedoissa tai osaamisessa olevat puutteet ja käynnistää korjausliike ajoissa.

Johtaminen on osa organisaation tapaa toimia ei yksittäinen toimenpide tai prosessi, jota toteutetaan. Muuttuvassa ympäristössä organisaation uudistumiskyky ja ketteryys korostuvat. Tietojohtamisen työkalut tukevat organisaatiota tunnistamaan hallussa oleva oleellinen tieto, miten tietoa voidaan käyttää ja kuinka opitaan uutta. Tavoitteellinen tietojohtaminen antaa pohjan ketterästi muuttaa toimintaa, kun ympäristö antaa impulsseja muutostarpeille. Kuten aiemminkin viitattu tietojohtamisen tutkimuskirjallisuudessa yleensä keskitytään kilpailukyvyn optimointiin. (Kianto 2011; Jennex ja Zyngier 2007.) Tässä tutkielmassa tarkastellaan tietojohtamista suorituskyvyn- ja arvonluonninnäkökulmista. Miten tietojohtamisen välineillä voidaan tukea uudistumiskykyä ja parantaa suorituskykyä yllättävissäkin tilanteissa kuten rikollisten huijausyritykset.

Paljon siitä, että organisaation tieto on turvassa, on kiinni yksilöistä. Teknologialla ei saa järjestettyä aukotonta turvaa. Organisaation vastuulla on, että on olemassa juurrutetut toimintaohjeet ja prosessikuvaukset, joita pidetään ajan tasalla. Vastuuta ei voi siirtää työntekijöille, mutta heidän valmiustasonsa ja kyvykkyytensä ratkaisevat loppupelissä tilanteen. (Hinde 2003; Agazzi, 2020.) Organisaation jäsenten jatkuva koulutus on avainasemassa, kun suojaudutaan erilaisilta tietosyötteissä esiintyviltä vääriltä tiedoilta. On myös hyvä luoda toimenkuvia, joissa vastuualueelle kuuluu väärän tiedon tunnistaminen. Isossa organisaatiossa näitä positioita voi olla useammissa tiimeissä, jolloin henkilöt voivat muodostaa asiantuntijaverkoston, jossa jakaa kokemusta ja tietoa esiintyvistä vääräntiedon syötteistä organisaatiossa. Myös teknologian tukea tarvitaan muun muassa sähköpostien suodattamisessa ja disinformaation tunnistamisessa, mutta ikävä kyllä pelkät tietojärjestelmät eivät poista ongelmaa, vaan yksilöt ovat työssä avainasemassa. Koulutus, selkeät toimintaohjeet ja kokemus ovat avain asemassa suojautumisessa. (Jennex et al. 2022.)

Kuten jo aiemmin on todettu, tiedossa tärkeää on sen merkityksellisyys organisaatiolle. Kun lähdetään miettimään tiedon turvaamista erilaisilta riskeiltä, on keskiössä tiedon oleellisuus organisaation toiminnalle. Ovatko riskit tietyn tiedon osalta merkittävät toiminnan kannalta. Tai vaihtoehtoisesti voiko tiettyyn tietoon kohdistuvat uhat aiheuttaa merkittäviä ongelmia. Kun on mietitty suojautumisen tarpeita toiminnan ja ongelmien kannalta tulee myös arvioida, mikä on muutoksilla saavutettavissa oleva hyöty. Alla kuviossa 9. on kuvattuna riskiarvioinnin seitsemän osa-aluetta. (Ilvonen et al. 2015.)



Kuvio 9. Tietopääoman riskiarviointiprosessi (mukaillen Ilvonen et al. 2015, 5).

Toisessa vaiheessa tulee tunnistaa organisaatiolle oleellinen tieto. Tämä on tärkeää, kun mitataan saavutettavaa hyötyä. Mikä tieto aiheuttaa vaarantuessaan suurimman menetyksen tai haitan esimerkiksi organisaation maineelle. Ketkä ihmiset esimerkiksi työskentelevät tämän tiedon parissa. Kolmanneksi tulee miettiä mitä uhkatekijöitä organisaation oleelliseen tietoon saattaa kohdistua. Tähän kuuluu haavoittuvuuksien tunnistaminen ja toimijat, joista voi olla uhkaa. Toimijoita on sekä sisäisiä että ulkoisia. Neljänneksi edellisessä vaiheessa tunnistetut uhat analysoidaan. Arvioinnissa huomioidaan eri uhkien todennäköisyyttä ja

aiheutuvan haitan vakavuutta. Viidenneksi arvioidaan hyödyt ja kustannukset eli saavutettavien etujen arvoa verrataan prosessissa tehtävien muutosten kustannuksiin. Kyseeseen voi esimerkiksi tulla ohjelmiston hankkiminen. Kuudennessa eli mitikointi vaiheessa valitaan tavat, joilla riskejä lähdetään hallitsemaan entistä paremmin. Lopputuloksen on valinnat toteutettavista riskienhallinta keinoista ja suunnitelma toteutuksesta. Viimeisenä vaiheena toteutetaan uhkaympäristön jatkuva seuranta. Tarkkaillaan ja havainnoidaan tietoprosessin toimivuutta, prosessiin osallistuvien toimintaa, tiedon välittymistä, ohjeiden noudattamista, teknologianmuutoksia ja toimintaympäristöä. Mikäli havaitaan muutoksia, käynnistetään tarvittaessa riskien uudelleen arviointi. (Ilvonen et al. 2015.) Riski huijauksen uhriksi joutumisesta on operatiivinen riski. Toteutustapoja maksuliikkeessä on monia. Rikollinen manipuloi joko maksajaa tai maksun saajaa. Tällöin maksaja toteuttaa maksun vilpittömin aikein. Rikollinen saattaa myös hankkia tietoonsa maksutiedot ja toteuttaa maksun itse tai maksu saadaan kaapattua niin, että siihen vaihdetaan maksuohjeen yksityiskohtia kuten tilinumero. (Louisot & Ketcham 2014.)

Kuten aiemmin on tuotu esiin ei teknologialla pysty suojautumaan riskeiltä, vaan ihmiset ovat isossa roolissa. Kyberrikollisuudessa on läsnä sama tilanne se ei ole vain teknologia-asia, vaan se on ”ihmisasia”. Kyberrikollisuutta pitää ymmärtää, jotta siltä voi suojautua. Ymmärtäminen tarkoittaa osapuolien kuten syyllisten, uhrien, tekotapojen ja suojautumiskeinojen tuntemista. Varautumisessa on jälleen vahvasti läsnä uhkien tunnistaminen ja riskien arviointi. Kokonaisuudessa teknologian ymmärtäminen on loppujen lopuksi helpompaa kuin ihmisten ymmärtäminen. Rikollisten motiivit voivat olla monenlaisia kuten jännitystä ja hauskanpitoa tylsistymisen tilalle, poliittinen tai vastaava vakaumus tai rahallinen hyöty. Rikollisten motivaatioiden moninaisuus tekee kyberrikollisuuden torjunnasta haastavaa. (Spicer 2019; Ilvonen et al. 2015.)

Virheellinen tieto korruptoi prosessin, tuhlaa aikaa ja haittaa päätöksentekoa. Maailma muuttuu nopeasti ja tietotulva on loputon. Uutta tietoa pitää kuitenkin pyrkiä hyödyntämään koko ajan. Nykymaailmassa organisaatioiden on oltava entistä nopeampia ja joustavampi pysyäkseen mukana muutoksessa sekä organisaation sisällä että sen toimintaympäristössä. Muutoksessa ei pysytä perässä vain huomioimalla teknologioiden kilpajuoksua alati

kehittävämpiin ratkaisuihin vaan myös organisaatiokulttuurin ja yksilöiden on pysyttävä kyydissä. Monimuotoisuus myös tietoprosesseihin vaikuttavissa tekijöissä voidaan nähdä rikastuttavana tekijänä tiedon luomisen, jakamisen ja hyödyntämisen näkökulmasta. Organisaation kulttuuri ja tietoelementit voidaan nähdä erottamattomina toisistaan ja ne vaikuttavat sorituskykyyn yhdessä. Nopeasti muuttuvassa ympäristössä tiedon oleellisuus tulee kyetä varmistamaan ennen hyödyntämistä. Näin ollen tiedon laatuun liittyvää validointia tulee tehdä koko ajan tietosyötteiden käsittelyn yhteydessä. Mikäli havaitaan huomattavia tietoon liittyviä muutoksia toimintaympäristössä, tulee olla valmius ketterästi arvioida tilannetta. Organisaation toiminnan kannalta on ensiarvoisen tärkeää, että yrityksessä tunnistetaan väärä tieto hyvissä ajoin ennen sen päätymistä hyödynnettäväksi. Sen lisäksi, että näin vältetään taloudelliset menetykset ja työntekijät eivät kärsi manipuloinnin ja huijatuksi tulemisen negatiivisia psykologisia vaikutuksia myös mahdolliselta mainehaitalta vältytään. (Bhatt 2000; Intezari, Taskin & Pauleen 2017; Zieba & Durst 2019.)

Riskien hallinnassa nähdään, että koneoppimisen ja tekoälyn luomilla mahdollisuuksilla voidaan parantaa petosyritysten havaitsemista ja niiltä suojautumista. Uutta teknologiaa voidaan hyödyntää löytämällä parhaat suojautumiskeinot sekä järjestelmille ja sekä omalle tietopääomalle, että asiakkaiden tiedoille. Tekoäly mahdollistaa myös tehokkaampaa automatiikkaa ja sen kautta tunnistaa ja poistaa inhimillisiä virheitä sekä epäoleellista ja väärää tietoa. Uudet teknologiat ovat myös tehokkaampia tunnistamaan ihmisten välisiä yhteyksiä ja verkostoja. Tämä auttaa tunnistamaan rikollista toimintaa tehokkaammin. (Palgrave & Nature 2019.) Kuten yleisesti niin myös rahaliikenteessä tekoäly mahdollistaa ja tulee mahdollistamaan rahaliikenteen kasvavan automatisoinnin ja sitä kautta optimoinnin. Tekoälyn avulla voidaan analysoida poikkeavuuksia ja tunnistaa petoksiin viittaavia käyttäytymismalleja entistä tehokkaammin. Tämä tekninen kehitys tukee toimijoiden ja asiakkaiden suojelemista petoksilta entistä tehokkaammin. (Tello 2023).

Finanssialalla nähdään myös uuden teknologian mahdollisuudet asiakkaan tuntemisprosesseissa (Know your customer, KYC). KYC-prosessien vaativuus lisääntyy koko ajan ja muutos sisältää alati kasvavan määrän prosessoitavaa tietoa, jonka tulee olla laadukasta ja ajantasaista. Tiedon ajantasaisuus ja oikeellisuus ovat säätelyn asettamia edellytyksiä.

Kehittyneemmän teknologian avulla saadaan laadukkaampi ja näin vaatimuksia vastaava lopputulos. Rahalaitosten työntekijöiden aikaa vapautuu suunnittelulle ja kehittämiselle valvonnasta. Tukijoiden mukaan on arvioitu, että vaatimusten mukaiset KYC-prosessit kustantaa noin 70 miljardia dollaria vuositasolla. Paremmille ja tehokkaammille prosesseille on siis myös kulunäkökulmasta käyttöä. (Palgrave & Nature 2019.)

Tekoälyn ja koneoppimisen hyödyntämiseen liittyy kuitenkin myös hidasteita, esteitä ja tarkkaan pohdittavia näkökulmia. Organisaatiolla täytyy olla oikeanlaista käytettävissä olevaa dataa. Monesti data on hajallaan organisaatioissa ja tallennettuna erilaisissa muodoissa eri järjestelmiin. Lainsäädännössä ja finanssialan säännöstelyyn liittyy myös paljon tiedon jakoon liittyviä rajoitteita. Ongelma on myös ammattitaitoisen työvoiman puuttuminen ja sen puute ylipäänsä työmarkkinoilla. Yksi rajoite on, että koneoppimista ei voi vain napsauttaa päälle, vaan sen tuominen vanhemman teknologian rinnalle vaatii paljon testaamista ja sovittelua. Muutokset prosesseissa vaativat toimivuuden arviointia ja jatkokehitystä. Myös tekoälyn tuottamat prosessit vaativat ihmisen valvontaa ja eettistä arviointia. Kuten laajemmassakin kontekstissa, myös finanssialla tulee huomioida tekoälyn käyttöön liittyvät eettiset näkökulmat kuten vastuullisuus automaattisessa päätöksenteossa. Kun yllä mainitut riskit huomioidaan ja esteet taklataan, tekoäly tulee tarjoamaan ennennäkemättömiä työkaluja riskien hallintaan ja ennakointiin. (Palgrave & Nature 2019; Tello 2023.)

Tietoon liittyvillä riskeillä tulisi olla merkittävä asema organisaatioiden rikienhallinnassa kaikenlaisissa organisaatioissa. On aloja, joissa niiden luonteen vuoksi ja regulaatioiden sääteleminä, asiaan kiinnitetään enemmän huomiota. Hyvä esimerkki on pankkiala. Tietoon liittyvien riskien tutkiminen laajasti avaisi mahdollisuuden laajempaan tilannekuvaan riskinäkökulmasta. Tässäkin tärkeää on fokusointi oleelliseen. Mikä on kunkin organisaation kannalta tärkeintä riskien ennakoimisen näkökulmasta. Tietoon liittyvien riskien johtamisessa (knowledge risk management) tavoitellaan kykyä tunnistaa kriittiset riskit ja oppia hallinnoimaan niitä mahdollisimman tehokkaasti. Durst et al. (2019,8) näkevät tietoon liittyvien riskien johtamisen tuntemisen olevan vielä alkumetreillä. Heidän mukaansa tutkimuksia tarvitaan vielä lisää, jotta saadaan eheämpi kokonaiskuva riskien hallinnasta tietojohtamisen näkökulmasta. (Durst et al. 2019.)

2.2.1 BEC-huijaus käsite ja ongelman laajuus sekä oleellisuus

Verkkorikollisuus on päivittäinen uhka kaikenkokoisille organisaatioille, joiden toiminnassa tarvitsee toteuttaa maksuja. Voinee siis sanoa, että uhka on ajankohtainen kaikille organisaatioille koosta riippumatta. Yksi tämän tyyppisen taloudellisen uhan ilmenemismuoto on Business Email Compromise (BEC). FBI tunnisti BEC-huijaukset ensimmäistä kertaa vuonna 2013. Organisaatio myös antoi huijaustyypille sen nimen. BEC-huijauksessa sähköpostin välityksellä toteutetaan tietojenkalastelua tai väärän tiedon ujuttamista organisaation käyttöön. Lähestymistapoja ovat joko manipulointi tai sähköpostienvaihtoon on onnistuttu tunkeutumaan teknologian avulla. BEC-huijauksia kohdistuu myös kuluttajiin, mutta tässä tutkimuksessa keskitytään vain yrityksien kohtaamiin BEC-huijauksiin. Rikollisten tavoitteena on taloudellisen hyödyn saavuttaminen. BEC-huijaus ei aina vaadi laajaa teknistä osaamista tai erityistä kokemusta petoksien toteutuksesta, jos verrataan esimerkiksi haittaohjelmilla tehtyihin hyökkäyksiin. (Saud Al-Musib, Mohammad Al-Serhani, Humayun & Jhanjhi 2021; Atlam & Oluwatimilehin 2023; Nisha, Bakari, & Shukla, 2021; FBI 2022; Mansfield-Devine (2016).)

Vaikeusasteen skaala on BEC-huijauksissakin laaja. Yksinkertaisimmillaan työkaluna toimii huijaustarkoitukseen avattu ja nimetty sähköpostiosoite ilman erityistä taustatyötä liittyen viestin vastaanottavaan henkilöön, organisaatioon tai viestin väitettyyn viestin lähettäjään liittyen. Toisessa ääripäässä taas tutkitaan tarkasti viestin lähettäjän ja vastaanottajan yhteydet toisiinsa, sekä yksilö että organisaatiotasolla. Käytössä saattaa myös olla osapuolten kirjautumistietoja, jotka on saatu käyttöön haittaohjelmilla varastamalla tai hankkimalla niitä pimeästä verkosta (dark web). (Mansfield-Devine 2016.) Pimeä verkko on internetin osa, jossa voi toimia anonyymisti ja salassa (F-Secure 2023). Jos rikollisilla on pääsy osapuolten väliseen viestien vaihtoon varastetuilla käyttäjätiedoilla he pystyvät myös imitoimaan tapaa, jolla osapuolet kommunikoivat keskenään. Helposti toteutettavat huijaukset ovat yleisimpiä ja vaikeammat tuottoisampia rikollisille. (Mansfield-Devine 2016.)

BEC-huijaukset ovat kansainvälinen ongelma, joiden seurauksena kärsitään huomattavia taloudellisia tappioita. FBI:n mukaan toukokuun 2018 ja heinäkuun 2019 välisenä aikana tunnistetut huijausten aiheuttamat tappiot maailman laajuisesti kasvoivat 100 prosenttia juuri BEC-huijausten vuoksi. Vuonna 2022 FBI: nin Internet Crime Complaint Center vastaanotti 21 832 ilmoitusta BEC-huijauksista, joista koitui 2,7 miljardin USD tappiot (FBI 2022). Taloudellisten tappioiden lisäksi erilaisilla huijauksilla on huomattava vaikutus uhreiksi joutuviin työntekijöihin. Tutkimuksissa on huomattu, että huijauksilla on uhreille vakavia inhimillisiä vaikutuksia. Tämä johtuu huijausten toteutusten sisältämistä manipuloivista ja huijattavien henkilökohtaisesti psykologisesti vaikuttavista elementeistä. Erilaisissa huijaustyypeissä kohteena voivat olla iso joukko ihmisiä (esimerkiksi tietyn pankin asiakkaat), tarkasti valikoitu ryhmä (esimerkiksi organisaation talousosaston työntekijät) tai yksittäinen henkilö. (Cross & Gillett 2020; Archie, Turner & Wybitul 2020; Pienta, Thatcher, & Johnston 2020.)

BEC-huijauksen historia on suhteellisen lyhyt, mutta huijaustyyppi on kehittynyt historiansa aikana nopeasti ja muuntautuu edelleen nopeasti. Nopea kehittymin haastaa huijauksen tunnistamiseen käytettävät keinot. Havaitseminen on hyökkääjien käyttämien muuttuvien keinojen takia vaikeaa ja tässäkin ongelmassa on ryhdytty hakemaan apua myös koneoppimisen tarjoamista mahdollisuuksista. (Atlam & Oluwatimilehin 2023.)

2.2.2 BEC-huijaukselta suojautuminen

Jotta BEC-huijauksien aiheuttamilta taloudellisilta menetyksiltä ja henkisiltä kolhuilta voisi välttyä on niiltä aktiivisesti suojauduttava. Työntekijät on tärkeä kouluttaa tunnistamaan BEC-hyökkäykset. Heidän tulee ymmärtää, miten BEC-huijaus toimii ja miten rikolliset rakentava hyökkäyksensä. Koulutus tuo varmuutta olla epäleväinen myös kiireessä, kasvattaa huomioimaan viestien ansat ja kasvattaa ylipäänsä vastuuntuntoa. Pelkkä koulutus ei kuitenkaan riitä, koska rikolliset parantavat ja muuttavat jatkuvasti taktiikkaansa. Tämä tekee huijausten tunnistamisesta erittäin vaikeaa. Yrityksessä on tärkeää kiinnittää huomiota myös työohjeisiin ja sääntöihin. Työohjeet antavat selkeän henkisen ja konkreettiset tuen, kun työnkuvasta riippumatta voi noudattaa organisaation menettelytapoja poikkeuksetta. On myös hyvä rakentaa teknistä puolustusta. BEC-huijauksia ei isolta osalta pidetä teknisesti edistyneinä. Huijauksilta pystyttäisiin osittain suojautumaan niinkin yksinkertaisesti, kuin

lisäämällä yrityksen toimintatapoihin salattujen sähköpostiviestien käyttö, muutokset validoitaisiin puhelinsoitolla tai Teams-tapaamisella. Jo näillä toimilla huijarin työtä vaikeutettaisiin huomattavasti. (Agazzi, 2020.)

Wittman ja Mattord (2018) tunnistavat myös, että paras keino välttyä huijatuksi tulemiselta on henkilökunnan kouluttaminen, jatkuva ja ajantasainen tiedottaminen ja prosessien kontrollointi. Tietojärjestelmissä kontrolli on esimerkiksi sitä, että toiminnon toteuttamisessa tarvitaan kahta henkilöä, yksin ei voi muutosta tai vastaavaa toteuttaa. Yksilötasolla tapahtuvia organisaation tietovarantoihin vaikuttavia uhkia ovat esimerkiksi käyttäjän manipulointi (social engineering), tietojen kalastelu (phishing) ja Advance-fee fraud (AFF), jossa pyydetään ennakkomaksua, jotta saat esimerkiksi voittamasi arpajaispalkinnon tai perinnön. (Wittman & Mattord 2018.) Jennex & Durcikova (2020) näkevät yhtenä uhkan tulokulmana yksilöiden käyttäytymiseen liittyvän uhan, organisaation jäsenet voivat tulla manipuloiduksi. Tämä on hyvin tyypillinen osa myös BEC-huijauksissa, kuten aiemmin todettiin.

Tärkeässä roolissa on arvioida tietolähteen luotettavuus. Tätä arvioidessa arviota tekevän yksilön osaaminen on avainasemassa. Perusteellisesti suunnitellut prosessit, hyvä koulutus ja luonnollisesti myös kokemus mahdollistavat yksilöille parhaat työkalut tunnistaa epäilyttävät tilanteet. Tiedon jakaminen on tärkeässä roolissa. Toisilta oppiminen, hyvien käytänteiden kopioiminen ja erilaisten näkökulmien sekä kokemusten jakaminen ovat hyviä työkaluja uudistaa käytänteitä ja tapoja. Jakaminen edesauttaa myös organisaatiotason oppimista. (Bhatt 2000; Daghfous, Belkhodja & Angell 2013; Jennex et al. 2022.)

Monet seikat korostavat monivaiheisen tunnistamisen tärkeyttä, kujan juoksussa alati kehittyvien huijausten tunnistamisessa. Organisaatioiden on tärkeää luoda omat prosessit ja säännöt, joista ei ole lupa poiketa ja jotka ovat irralliset sähköpostiliikenteestä. Varmistettavaa viestiä ja sen sisältö ei näin ollen käytetä varmistamisprosessissa, vaan siihen käytetään muita keinoja. Rahaliikenteeseen liittyvään sähköpostiin pitää aina suhtautua varauksella ja siinä listattuihin tietoja, kuten puhelinnumerot, ei tulisi käyttää viestin aitouden varmistamisessa. (FBI 2022.) Myös erikoistilanteita on tutkittu. Organisaatiot ovat helpompia uhreja

niiden tietoprosesseihin kohdistuville uhille, silloin kun toimintaympäristössä on poikkeava tilanne kuten COVID-19 aiheuttama muutos normaaliin toimintaympäristöön vuosina 2020–2021. Erikoistilanteet kannattaa huomioida organisaatioissa ja ennakoida prosesseissa, että erikoistilanteissa on enemmän uhkia, joten ne vaativat erityishuomioita. Jennex, Durcikova ja Ilvonen (2022.)

2.2.3 Viranomaisohjeistus huijauksilta suojautumiseen

Viralliset tahot ohjeistavat organisaatioita varovaisuuteen huijausten ja erilaisten kyberuhkien välttämiseksi. Alla olevassa taulukossa 1. on listattuna kuuden eri tahon ohjeita:

- Europol on EU:n lainvalvontaviranomainen, joka tukee EU:n jäseniä rikollisuuden torjunnassa. (https://www.europol.europa.eu/sites/default/files/documents/fi_0.pdf)
- Traficomin (liikenne- ja viestintävirasto) yksi osa on Kyberturvallisuuskeskus, jonka tehtävä Suomessa on muun muassa kyberturvallisuuden kehittäminen. (https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/laskutushuijaukset-lisaantyvat-kesaisin-nain-suojaudut-huijauksilta?toggle=Ohjeita%20organisaatioille)
- Poliisia taulukossa edustaa CYBERDI (Cybercrime prevention, awareness raising and capacity building by RDI on modern cyber attacks), joka on Jyväskylän Ammattikorkeakoulun ja Poliisiammattikorkekoulun yhteisprojekti. (https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212/Opas_Kyberrikos+on+poliisiasia.pdf?t=1616740405258)
- FBI on Yhdysvaltain liittovaltion keskusrikospoliisi. (https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf ja https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise)
- Interpol (International Criminal Police Organization) on kansainvälinen rikospoliisiorganisaatio, jossa on 196 jäsenvaltiota. (https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud)

- Finanssiala ry on Suomessa toimivien finanssialan yritysten toimialajärjestö. (https://www.finanssiala.fi/uutiset/varo-varmista-varoita-kampanja-digihuijausten-maara-kasvoi-selvasti-vuoden-2022-jalkipuoliskolla/)

Taulukko 1. Virallisten tahojen ohjeet huijausten välttämiseen

ORGANISAATIO	RISKIN TUNNISTAMINEN	TOIMENPITEET	KULTTUURI	KONTROLLI	VARAUTUMINEN
Europol EC3	Riskien tiedostaminen ja varautuminen	Ohjeet, käytännöt, prosessi, tarkkuus ja koulutus	Tietoisuus, toimenpiteiden noudattaminen ja ajantasaisuus	Raportointi, päätökset ja käytetty teknologia ajan tasalla	Mitä tietoa on lupa näyttää ja jakaa organisaation ulkopuolelle
Liikenne- ja viestintävirasto Traficomin Kyberturvallisuus-keskus	Riskien tiedostaminen ja vaikutusten ymmärtäminen	Koulutus, säännöt, uusien toimittajasuhteiden perustamisen ohjeistus	Vankkojen käytänteiden noudattaminen	Valvonta, raportointi, esihenkilön tuki ja järjestelmien & tietoturvan ajantasaisuus	Varovaisuus tiedon jaossa (some, nettisivut)
Poliisi	Perehtyneisyys koko organisaation tasolla, haavoittuvuuksien tunnistaminen	Kyberturvallisuuden jatkuva arviointi ja kehittäminen	Kyberturvallisuuden merkityksen ymmärtäminen osana riskienhallintaa	Päätöksentekoprosesessi, sovittu politiikka ja dokumentoitu ympäristö (prosessit, lokitiedot)	Sovitun politiikan noudattaminen
FBI	Riskien tiedostaminen	Ohjeet ja niiden tarkka noudattaminen	Tarkkaavaisuus	Tarkista ja varmista	Älä jaa liikaa tietoa (some)
Interpol		Tiedottaminen organisaatiossa ja tiedon validointi	Varuillaan oleminen	Tietoturvan ja ohjelmien ajantasaisuus sekä varmistaminen	Älä jaa liikaa tietoa
Finanssiala	Riskien tiedostaminen	Varo, varmista ja varoita muita	Terve epäluulo	Varmista	Älä jaa liikaa tietoa

Vertailun helpottamiseksi taulukko 1. on jäsennelty viiden pääteeman mukaan riskin tunnistaminen, toimenpiteet, kulttuuri, kontrolli ja varautuminen. Teemat on otsikoitu peilaten haastattelukysymysten pääteemoja, haastatteluaineiston analyysissä suodattuneita dimensioita ja ohjeista ilmenneitä elementtejä.

Pääasiallisena lähtökohtana ohjeissa oli riskien tunnistaminen. Organisaation tulisi tunnistaa omasta toiminnastaan riskit, uhat ja haavoittuvat kohdat sekä ymmärtää mahdolliset vaikutukset organisaation toiminnalle. Toimenpiteinä suojautumiselle suositeltiin henkilöstön koulutusta, tiedottamista, selkeitä ja ajantasaisia toimintaohjeita, mukaan luettuna säännöt, sekä tarkkaavaisuus ja tiedon varmistaminen. Finanssiala kiteytti hyvin mistä on kysymys: varo, varmista ja varoita. Toimenpiteistä, jotka voi katsoa organisaation kulttuuriksi turvallisuuden kontekstissa, mainitaan muun muassa ohjeiden ja sääntöjen noudattaminen, tarkkaavaisuus ja kyberturvallisuuden merkityksen ymmärtämien osana riskienhallintaa. Ohjeissa suositellaan myös monenlaisia kontrollielementtejä kuten tietojen varmistaminen,

käytetyn teknologian ajantasaisuuden seuranta, raportointi, dokumentoidut ja valvotut prosessit. Viimeisenä korostetaan varautumista eli sitä, että organisaatio ei itse aseta itseään haavoittuvaan asemaan. Tässä erityisesti ohjataan kiinnittämään huomiota siihen mitä organisaatio kertoo itsestään nettisivuilla tai miten työntekijöitä ohjeistetaan kertomaan roolistaan ja työstään sosiaalisen median kanavilla.

2.3 Tietojohtamisen rooli riskienhallinnassa

Aiemmin tässä luvussa 2. on kuvattu, kuinka tieto on voimavara ja mahdollisuuksien luoja, mutta on todettu myös, että tiedon tärkeyden lisäksi ja sen takia, tiedon ympärillä on myös havaittavissa monenlaisia riskejä. Tiedon riskitekijät on vähemmän tutkittu alue, kuin tiedon hyödyntämistä käsittelevät aihealueet. (Durst, Hinteregger & Zieba 2019.)

Ulkoiset uhat kohdistuvat organisaatiota tietopääomaa vastaan monilla tavoilla. Tietojohtamisen prosessien turvallisuuden ja prosesseihin osallistuvien osaamisen varmistaminen korostuu näissä tilanteissa. Osaava henkilöstö on avainasemassa, kun kehitetään organisaation tietoon liittyviltä riskeiltä suojautumista. Organisaatiolle vahingollista toimintaa mahdollistavat puutteet työntekijöiden osaamisessa ja riskien ymmärtämisessä, heikkoudet tietoprosesseissa, epäjohdonmukaisuus tiedonkulussa tai päätöksenteossa. Organisaation tietojohtamisen prosesseista tulisi tunnistaa heikot kohdat, jotka mahdollistavat väärinkäytökset. (Goode & Lacey 2022; Prislan, Mihelic, & Bernik 2020.) Taulukossa 1. listatuissa virallisissa ohjeissa usein lähtökohtana on juuri riskien tunnistaminen.

Tietoon liittyvillä riskeillä tulisi olla keskeinen asema organisaatioiden rikienhallinnassa. Tietoon liittyvien riskien laajempi tutkiminen ja tunteminen tarkentaa tilannekuvaa riskienhallinnannäkökulmasta. Tietoriskien johtamisessa (knowledge risk management) tavoitteena on kriittisten riskien tunnistaminen ja niiden mahdollisimman hyvä hallinnointi. Tutkimuksia tarvitaan aiheesta lisää, jotta saadaan parempi kokonaiskuva riskien hallinnasta tietojohtamisen näkökulmasta. (Durst et al. 2019.)

Jennex ja Durcikova (2014) toteavat luennossaan, että tietojärjestelmien tarjoamat turvallisuusaspektit tulisi integroida tietoprosesseihin. Samaan aikaan tietoa on kuitenkin myös pystyttävä hyödyntämään tehokkaasti. Organisaatiolle on tärkeää tunnistaa tietoriskit ja arvioida niiden haitallisuus organisaatiolle. Tavoitteena on löytää hyväksyttävä taso niin, että painotetaan tärkeitä ja oleellisia asioita huomioiden kustannustehokkuus. Riskejä on tärkeä hallita, mutta riskiarviossakin on priorisoitava. Tämä tasapaino mahdollistaa tiedon tehokkaan hyödyntämisen. Päätöksenteon tueksi tarvitaan tietoresurssien systemaattinen arviointi arvon, haavoittuvuuden ja uhkien näkökulmasta. On löydettävä tasapaino käytettävyyden ja kontrollin välillä. (Jennex & Durcikova 2014; Prislan et al. 2020.)

Tiedon turvaaminen tulisi sisällyttää laajemmin tietojohtamisen tutkimuksiin. Käytännössä ei ole riittävää, että asiaa tarkastellaan teknisten ratkaisujen kautta, kuten käyttöoikeuksien ja suojauksennäkökulmista. Tiedon turvaamista tulee tutkia laajemmin osana tietojohtamista ja tietoprosesseja. Tietojohtamisen kontekstissa turvallisuuden olisi hyvä keskittyä riskien analysointiin. Riskienhallinnan olisi hyvä olla osa organisaation tietojohtamisenkokonaisuutta ja keskittyä tietopääoman turvaamiseen. Riskienhallinnan tulisi olla myös tietojohtamisen näkökulmasta jatkuva prosessi, jolla on vahva johdon tuki. Näin toteutettuna riskienhallinnassa on mahdollisuus onnistua. (Jennex ja Zyngier 2007.)

Seuraavassa luvussa 3. kuvataan tarkemmin pro gradu -tutkimuksessa käytetty tutkimusmenetelmä sekä haastatteluaineiston analyysimenetelmä.

3 Tutkimusmenetelmä

Tässä luvussa kuvataan, miten Pro Gradu tutkielman empiirinen osuus toteutettiin. Käydään läpi tutkimusongelma, tutkimusmenetelmän valinta, aineiston keruu ja analysointi sekä tutkimuksen luotettavuus. Tutkielman aihe perustui opintojeni aikana huomaamaani tukimusaukkoon, jota halusin tarkastella itselleni läheisen aihepiirin eli maksamisen kontekstissa.

3.1 Tutkimusongelma ja tutkimuskysymykset

Kuten luvussa 1.1.1. kuvattiin, tämä tutkimus etsii empiiristen tutkimuslöydösten kautta vastauksia kuviossa 10. esitettyihin tutkimusongelmiin. Haluan selvittää miten, jos mitenkään, tietojohtaminen kytkeytyy yrityksen riskienhallintaan tilanteessa, jossa luodaan keinoja suojautua uuden tiedon käyttöön liittyviltä riskeiltä maksamisessa.

Kuvio 10. Tutkimusongelma ja alatutkimuskysymykset

Ensimmäisellä alatutkimuskysymyksellä kartoitetaan, onko uuden maksutiedon validoinnissa käytössä prosessia. Jos prosessi on käytössä, miten siihen on päädytty tai, mikäli validointia ei tehdä, miksi tähän on päädytty. Toisella alatutkimuskysymyksellä selvitetään, millainen painoarvo maksamisen riskeillä on organisaation riskikartoituksessa. Viimeisellä

alakysymyksellä halutaan tietää, millaiset vaikutukset huijauksen uhriksi joutumisella on. Tutkimuksen lähtökohdat ja rajaukset on kuvattu luvussa 1.2.

3.2 Tutkimusaineiston hankinta ja tutkimuksen kulku

Tämän pro gradu tutkimus toteutettiin laadullisena eli kvalitatiivisena, haastattelututkimuksena. Näin toteutettuna oli mahdollista tutkia ilmiötä lähemmin suoraan haastattelemalla ihmisiä, jotka työskentelevät kansainvälisten yritysten talousosastoilla. Tämä mahdollisti myös paremmin analyysin, joka pohjautui haastateltavien käytännön kokemuksiin, tuntemuksiin ja näkökulmiin. Haastattelu mahdollisti myös lisäkysymykset, joilla pystyi tarkentamaan vastauksia sekä täsmentämään kysymyksiä tarvittaessa. Halusin tutkimuksessa myös suosia lähelle menevää tarkastelua, sillä aihealue oli entuudestaan minulle tuttu ammattini kautta. (Kallinen & Kinnunen; Saunders, Lewis, & Thornhill, 2016, 568–569; Hirsijärvi & Hurme 2022.) Haastattelut toteutettiin puolistrukturoituina ja niissä haastateltiin kuuden eri organisaation jäsentä.

Käytettyä haastattelumenetelmää voi kutsua puolistrukturoiduksi- tai teemahaastatteluksi. Haastattelu eteni aina teeman ja alateemojen mukaisesti tarkoituksena ohjailla haastattelijana mahdollisimman vähän ja antaa haastateltavien puhua näkemyksensä vapaasti. Tarkoituksena oli pitää vuorovaikutus keskusteluomaisena, vaikka kysymykset olivat valmiiksi laadittuja. Kysymyksiä pystyi myös joustavasti jättämän väliin tai muuntelemaan tilanteen mukaan. (Hirsijärvi & Hurme 2022.) Teemat olivat kaikissa haastatteluissa samat, mutta kysymykset eivät olleet tismalleen samat eikä järjestys ollut aina sama. Puolistrukturoitujen haastatteluiden lopulliseen toteutukseen tuli 21 etukäteen pohdittua kysymystä. Kymmenen näistä olivat teeman mukaisia pääkysymyksiä ja yksitoista etukäteen mietittyjä täsmentäviä kysymyksiä. Lopuksi kaikilta haastatelluilta kysyttiin, haluaisivatko he vielä lisätä jotakin, mitä ei jo ollut teemanmukaisessa keskustelussa tullut esille. Tämä antoi haastatelluille mahdollisuuden palata aiempiin vastauksiin tai lisätä uutta. Tutkimuskysymykset löytyvät tutkielman lopusta liitteestä I.

Haastattelut toteutettiin Teams -tapaamisina, jotka tallennettiin sekä äänitallenteena että transkriptiona. Haastattelun jälkeen transkriptiot puhtaaksikirjoitettiin niin, että poistettiin änkytykset, täytesanat ja sanakatkokset. Näin toimien tekstistä saatiin sujuvampaa lukea. Aina, jos transkriptiosta jäi epäselväksi mitä oli sanottu, tarkistettiin kohta äänitallenteelta. Haastateltaviksi haluttiin valita yrityksiä koon ja kansainvälisyyden mukaan. Lisäksi haluttiin, että yritykset toimivat eri toimialoilla. Näin valittiin kohdeorganisaatioiksi kuusi keskisuurta yritystä, joiden liikevaihto oli vuonna 2022 yli 100 000 000 EUR. Kansainvälisyyden kriteerinä käytettiin joko sitä, että konsernilla on tytäryrityksiä tai toimittajia Suomen ulkopuolella. Näin varmistettiin, että yrityksellä on maksuja Suomen ulkopuolelle. Tämä oli tärkeää, koska maksamiseen kytkeytyvässä huijaamisessa edelleen usein toimitaan englannin kielellä. Haastatteluja tehtiin kussakin yrityksessä yksi. Kaikki kuusi haastateltua henkilöä työskentelivät talousosastolla ja olivat tekemisissä yrityksen rahaliikenteen kanssa.

Vaikka haastatteluun tutkimustapana liittyy myös haittoja, kuten haastattelijan osaamattomuus ja aika- ja aikatauluhaasteet haastatteluajansopimisessa ja ajankäyttö haastatteluihin ja litterointiin, se kuitenkin sopi menetelmävaihtoehdoista parhaiten tutkimuksen toteutukseen (Hirsijärvi & Hurme 2022). Tässä tutkimuksessa ei ilmennyt erityisiä haasteita haastateltavien valinnassa ja haastatteluaikojen sopimisessa.

Alla oleva taulukko 2. kuvaa haastatteluaineiston laajuutta. Taulukossa on listattuna haastattelujen kestot minuutteina ja litteroitujen sivujen määrät kutakin haastattelua kohden. Aineistonkeruun ensimmäisessä vaiheessa valitsin kahdeksan kriteereihin sopivaa organisaatiota. Alusta asti olin päättänyt tehdä kuusi haastattelua, mutta valitsin varalle kaksi lisävaihtoehtoa. Toisessa vaiheessa soitin haastateltaville ja kysyin kiinnostuksesta osallistua pro gradu -tutkielmani haastatteluun. Kuvasin puhelimessa opintojeni sisältöä, tutkimuksen teemaa ja toteutusta. Haastattelun osalta painotin, että 1) haastatteluun ei tarvitse valmistautua, 2) haastattelu tallennetaan, sekä 3) aineosto käsitellään anonymisoituna, eikä organisaatiota ja haastateltavan henkilöllisyyttä ilmaista tutkielmassa. Puhelun aikana sovin kalenterista sopivan ajankohdan haastattelulle. Kolmannessa vaiheessa, heti puhelun jälkeen, lähetin saateviestin ja tutkielmaa koskevan tietosuojailmoituksen sähköpostitse sekä Teams -kutsun haastatteluun. Kirjallisiin saatesanoihin ja tietosuojailmoitukseen voi tutustua tarkemmin

tutkielman lopussa liitteessä II ja III. Näissä dokumenteissa ilmaistiin myös haastateltavan suostumus haastatteluun osallistumiseen. Haastatteluihin varattiin kalenterikutsussa aikaa tunti, mutta kuten alla oleva taulukko 2. osoittaa niihin meni enimmillään 42 min.

Taulukko 2. Tiedot haastatteluista

Haastattelu	Kesto min	Litterointi (sivut)	Muoto
H1	37	12	äänitallenne, transkriptio
H2	33	14	äänitallenne, transkriptio
H3	42	18	äänitallenne, transkriptio
H4	35	18	äänitallenne, transkriptio
H5	33	18	äänitallenne, transkriptio
H6	25	18	äänitallenne, transkriptio

Neljännessä vaiheessa suoritin ensimmäisen haastattelun, jota käytin pilottina. Kerroin myös haastateltavalle, että kyseessä on ensimmäinen haastateltu, jossa samalla pilotoin kysymykset ja tulen kysymään palautetta lopuksi. Häneltä kysyin lisäkysymyksenä lopuksi, että kokiko hän haastattelun riittävän laajaksi ja lisäisikö hän jotakin. Palautteeksi sain, että aihe on ajankohtainen ja hyvin oleellinen. Haastateltava piti haastattelua kattavana.

(H1) ”Musta todella hyviä kysymyksiä. Hyvä ja oleellinen aihe, että kyllä mun mielestä on ihan hyvin kattavasti tuossa.”

Viidennessä vaiheessa analysoin pilottihaastattelun. Ensimmäisestä haastattelusta ja tallenteen kuuntelusta ennen seuraavia haastatteluja opin, että voin edetä rauhallisemmin ja, että kysymykset kannattaa esittää lyhyinä. Muokkasin myös kysymyksiä näiden kokemusten perusteella. Nämä opit otin mukaani seuraaviin haastatteluihin. Kuudennessa vaiheessa toteutin loput haastattelut. Jokaisen haastattelun jälkeen litteroin transkriptiot ja aloitin koodauksien työstämisen.

3.3 Aineiston analysointi

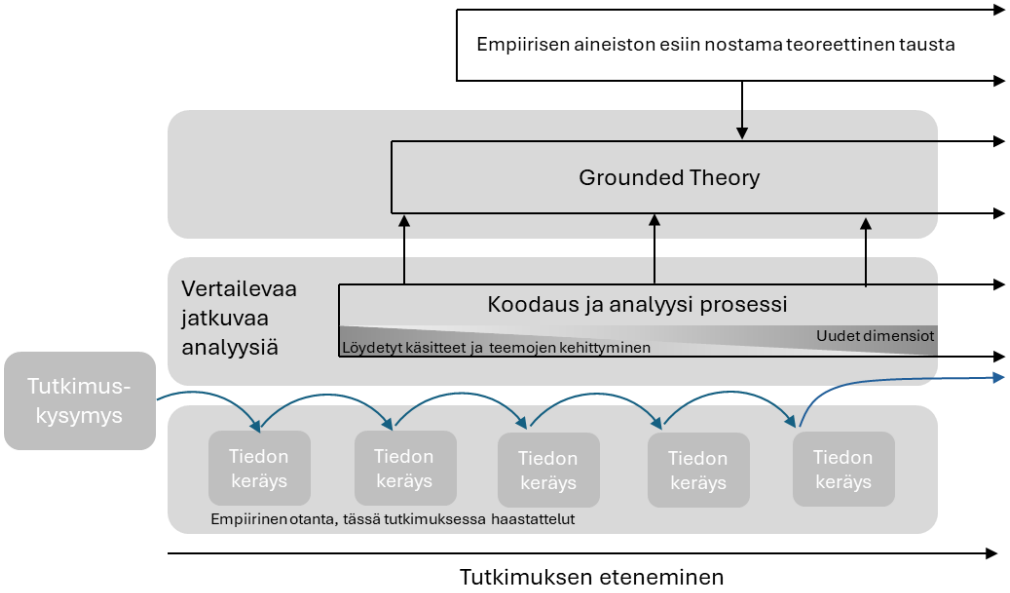
Tutkimuksen aineiston analysointi tehtiin Grounded Theory tutkimusmetodologiaan pohjautuvalla Gioia metodilla. Aineistoa lähestyttiin induktiivisen päättelyprosessin kautta. Haastatteluaineisto koodattiin ensimmäisen tason termeihin, josta jatkettiin toisen tason teemoihin ja lopuksi uusiin dimensioihin.

Grounded Theory -tutkimustapa nojautuu empiiriseen aineistoon ja sen analyysistä nouseviin vastauksiin. Gioian metodissa tutkija kohtelee tutkittavia kohteita, tässä tutkimuksessa haastateltavia, asiantuntijoina. Tutkimuskysymykseen haetaan vastausta empiirisestä tutkimusaineistosta ja etsitään uskottavia teoreettisia pisteitä teorian ja käytännön yhtymäkohdista. Tavoitteena on saattaa monimutkainen kvalitatiivinen aineisto yksinkertaisempaan teoreettiseen muotoon, kuten viitekehyksesi, malliksi tai teoriaksi. (Magnani & Gioia 2023.)

Tutkimuksen empiirisen aineiston analyysissä hyödynnettiin Grounded Theory -tutkimustapaa aineistolähtöiseen analyysiin, jossa pääaineistona käytettiin puhtaaksikirjoitettuja ja tallennettuja haastatteluja. Glaser ja Strauss kuvasivat kehittämänsä Grounded Theory -nimisen laadullisen tutkimustavan vuonna 1967. He loivat tutkimustavan vertailevan analyysin toteutustyökaluksi, koska kokivat että käytössä olleet tutkimustavat eivät ottaneet riittävästi huomioon yhteiskunnallisten ilmiöiden monimutkaisuutta. He myös halusivat osoittaa, että laadullinen tutkimus voidaan toteuttaa kurinalaisesti. He kokivat, että teorian kehittämisen tulisi pohjautua syvällisemmin empiiriseen tietoon eli tutkijan ja tutkittavan vuorovaikutukseen esimerkiksi tarkkailun tai haastattelun keinoin. (Glaser & Strauss 1967.) Sittemmin Glaser ja Strauss lähtivät kehittämään metodia toisistaan eroaviin suuntiin, ja ajan kanssa myös muut ovat jatkokehittäneet Grounded Theory -tutkimustapaa. Ei siis ole yhtä Grounded Theory- menetelmää, jota kaikki noudattavat, vaan erilaisia versioita. (Dey 2007.) Grounded Theory -tutkimustapa kehitettiin sosiologian tutkimuskysymysten selvittämiseen, mutta tutkimustapa on sittemmin levinnyt myös laajempaan käyttöön esimerkiksi psykologiaan ja taloustieteisiin, johon sitä tässä tutkimuksessa sovellettiin (Anttila 1998).

Grounded Theory -tutkimustapa sopii tutkimuksiin, joissa on tarjolla vähän aiempaa täsmällistä tietoa, esiintyy tutkimusaukko tai jossa on tarvetta uudelle näkökulmalle. Grounded Theory -tutkimustavassa johtotähtenä kulkee empiirinen aineisto. Tutkimusaineiston lisäksi ymmärretään, että tutkimuksen johtoajatus muodostuu ilmiön tutkimuksessa ilmenneiden seikkojen lisäksi tutkijan kokemuksen ja teorioiden tuntemuksen kautta. Lähestymistapa ottaa näin ollen huomioon tukijan vaikutuksen tutkimukseen, jolloin tutkimuksessa on aina läsnä empiirisestä aineistosta tehtyjen havaintojen lisäksi myös asiayhteys ja tietty subjektiivisuus. (Kallinen & Kinnunen; Saunders 2016, 568–569; Birks & Mills 2015, 12.; Glaser & Strauss 1967; Corbin & Strauss 2008.)

Grounded Theory -tutkimustapaan kuuluu menetelmäkokonaisuus, jossa on kolmivaiheinen koodausprosessi. Edempänä oleva kuvio 11. havainnoi, miten ensimmäisellä tasolla tietoa kerätään, seuraavaksi tieto koodataan ja kategorisoidaan koodien mukaan ja analysoidaan sekä lopuksi tavoitteena on luoda teoria tai malli. Kuvio osoittaa missä vaiheessa tutkimuselementit astuvat mukaan ja missä vaiheessa empiirisen tutkimuksen havaintoja lähdetään peilaamaan olemassa olevaan tutkimuskirjallisuuteen. On tärkeää valita tarkkaan pääasialliset tiedon lähteet, sekä muut tietolähteet, jotta saadaan täsmällistä tietoa tutkittavasta ilmiöstä. Tässä tutkielmassa pääasialliset tietolähteet ovat haastateltavat kansainvälistäliiketoimintaa harjoittavien suomalaisten keskisuurten yritysten talousosastolla työskentelevät henkilöt sekä tukimateriaalina virallisten tahojen antamat ohjeet huijaustilanteilta suojautumiseen. Tutkimuksen edetessä tunnistetaan vihjeitä, selvennetään havaittuja tutkimusaukkoja ja peilataan tulkintoja kerättyyn tietoon ja valittuihin teorioihin. Tutkimustavassa on mukana jatkuvaa vertailevaa analyysiä, kun kerättävää tietoa verrataan aiemmin kerättyyn tietoon. Tietoa koodataan vertailun edetessä ja lopulta koodit voidaan jaotella eri luokkiin. Tavoitteena on havaita johdonmukaisuuksia sekä eroavaisuuksia ja tätä kautta jalostaa luokkia. Analyysivaiheessa etsitään kerätystä tiedosta rakenteita ja esille nousseiden asioiden yhdistäviä tekijöitä, joista päätellään lainalaisuuksia ja parhaimmillaan luodaan malli tai teoria. (Chun Tie, Birks & Francis 2019.)



Kuvio 11. Grounded Theory (GT) tutkimusmetodologian kuvaus (mukaillen Wagner, Lukassen & Mahlendorf, 2010, 7).

Grounded Theory -tutkimustavassa on myös tärkeässä roolissa niin sanottu tutkijan teoreettinen herkkyys. Tällä kuvataan sekä tutkijan teoreettista taustaa, että kokemusta. Tässäkin tutkimuksessa yhtenä osatekijänä on tutkielman laatijan oma ammatillinen ja henkilökohtainen aiheen tuntemus sekä opinnoissa kerätty teoreettinen tausta. (Birks & Mills 2015.) Grounded Theory -tutkimusmetodin laadukasta käyttöä voi tarkastella kolmen osa-alueen kautta. Ensinnä tutkijan taidot vaikuttavat lopputulokseen, siihen että prosessi etenee loogisesti ja tutkimuksessa tehdyt päätökset ja päätelmät ovat perusteltuja. Toiseksi tutkimustavan valinnan ja käytön tulee vastata asetettuihin tutkimuskysymyksiin. Viimeiseksi tutkimustavan käyttö vaatii tarkkuutta, ja tämä voi osoittaa esimerkiksi täsmällisillä kirjauksilla koodauksien ja luokittelujen avulla. (Chun Tie, Birks & Francis 2019.)

Grounded Theory -tutkimusmetodissa on myös haastavia elementtejä. Tutkittaviin organisaatioihin voi olla vaikea päästää suorittamaan tukimusta niin laajasti, kuin mitä tutkimus vaatisi. Pääsy voi olla haastavaa niin pitkäksi ajaksi kuin pääsyä tarvitsisi, tai niin useita käyntikertoja kuin haluaisi tai tavoittaa niin useita ihmisiä tai saada tietoja eri osastoilta

halutulla laajuudella. Tässä tutkimuksessa tämä ei ollut ongelma, koska otos oli organisaatiokohtaisesti yksi haastateltava ja yksi haastattelukerta. Grounded Theory -tutkimusmetodissa on tyypillistä liikkua analyysin teon ja tiedonkeruun välillä useamminkin. Haastatteluja voisi järjestää toisen kierroksen vielä tarkennetuilla kysymyksillä, kun ensimmäisen kierroksen haastattelujen koodauksen jälkeen. (Locke 2003.) Tähän ei kuitenkaan tämän tutkielman puitteissa ollut tarvetta, vaan tutkimus toteutettiin yhdellä haastattelukierroksella. Tutkielman syvyyden ja kattavuuden kannalta yksi kuuden haastattelun kierros oli riittävä. Kvalitatiivisissa tutkimuksissa tätä kutsutaan harkinnanvaraiseksi näytteeksi. Kun tavoitteena on etsiä uusia näkökulmia tai luoda uusia malleja, voidaan jo pienemmästä määrästä haastattelemalla saada kattavasti uutta tietoa. (Hirsijärvi & Hurme 2022.) Haastattelut tallennettiin ja transkriptiot puhtaaksikirjoitettiin tutkimuskäyttöä varten. Koodaus toteutettiin manuaalisesti Excelin avulla.

Tässä tutkimuksessa käytetty, Grounded Theoryn pohjalta syntynyt, laadullisen tutkimuksen analyysitapa on Gioian methodi. Gioian metodi tähtää tutkimuksen laadun näkökulmasta kurinalaisuuteen, vaikka pääfokus on luovuudessa matkalla uuden teorian tai mallin löytymiseen. Metodille nimensä antanut tutkija Gioia kokee, että ympäröivä maailma tarvitsee tutkimustapaa, jossa lähdetään liikkeelle tutkittavien kokemuksista käyttäen heidän terminologiaansa. Hän kutsuukin haastateltavia tietoisiksi agenteiksi, jolla hän tarkoittaa esimerkiksi, että he ovat asiansa, tekemisensä ja päätöstensä parhaita asiantuntijoita. Haastateltavat voivat kertoa miksi tekevät kuten tekevät, mitä ajattelevat ja miltä heistä tuntuu. Tutkijan rooli on raportoida haastatteluista kerättyä dataa ja etsiä datasta ulottuvuuksia ja niiden kautta ilmiötä selittävä teoria. Ensimmäisestä tasosta jatketaan toiselle tasolle, jossa ensimmäisen tason käsitteet kehittyvät systemaattisesti toisen tason teemoiksi, analyysiksi tutkitusta ilmiöstä. (Gehman, Glaser, Eisenhardt, Gioia, Langley, & Corley 2018.)

Ensimmäisessä vaiheessa tutkimusdatasta etsitään yhteyksiä ja eroavaisuuksia toisiinsa ja lähdetään hahmottelemaan toisen tason teemoja. Pyritään tunnistamaan rakenteita ja yhteyksiä, joista lähtee kehittymään teoreettisemmat datasta nousevat teemat. Prosessin aikana datasta muodostuu rakennekuva tietokokonaisuudesta, joka kuvaa datan jalostumista tiedoksi ja matkaa kohti uuttaa teoriaa tai mallia. Prosessi toimii todisteena tutkimuksen laadusta

dokumentoimalla edellä mainittua kurinalaisuutta datan käsittelyssä, analysoinnissa ja sen pohjalta tehtävissä päätelmissä. Gioian metodin mukainen analysointi auttaa osoittamaan tutkimuksen luotettavuuden. Metodi on myös tehokas tapa osoittaa kuinka tai miksi tutkittava ilmiö tapahtuu. Ennen kaikkea metodi on työkalu systemoida tutkijan ajattelua tutkimusta tehdessä. (Gehman et al. 2018.)

3.4 Tutkimuksen uskottavuus

Laadullisen tutkimuksen luotettavuutta verrataan usein kvalitatiiviseen tutkimustapaan, jota pidetään täsmällisempänä ja helppona toistaa ja mitata. Laadullisen tutkimuksen luotettavuutta tarkastellaan erityisesti tutkimusprosessin luotettavuuden kautta. Luotettavuuden sijaan voi asian nähdä uskottavuutena. Kyse ei ole mittauksen luotettavuudesta kuten kvalitatiivisessa tutkimuksessa, vaan ennemminkin uskottavuudesta koko tutkimuksen toteutusta ja analyysiä kohtaan. Prosessin dokumentoinnin kautta arvioidaan, että tutkija onnistuu tulkitsemaan tutkittavia oikein sekä muodostamaan ilmiöön ja merkityksiin yhdistyvät käsitteet tarkasti tutkimusdataan eli tukittavien käsityksiin perustuen. Laadullisessa tutkimuksessa on otettavaa huomioon, että tutkija on itse osa tutkimusmenetelmää. Laadullisessa tutkimuksessa tutkimuksen tieteenfilosofinen suuntaus on sosiaalinen konstruktionismi. Tämä tarkoittaa, että tutkittava ilmiö rakentuu sosiaalisessa vuorovaikutuksessa. Siitä miten ihmiset, mukaan lukien tutkimuksen tekijä, tulkitsevat ympärillään tapahtuvia asioita ja kommunikoivat tulkinnoistaan. Tämä, sosiaalisen vuorovaikutuksen läsnäolo, usein tuottaa vaihtelevampaa ja monimutkaisempaa tietoa kuin kvantitatiivinen data. (Saunders et al. 2016; Eskola & Suoranta 1998.)

Aineiston merkittävyyttä ja riittävyyttä sekä analyysin kattavuutta arvioitaessa, voi ajatella, että aineisto voisi aina olla laajempi ja analyysi kattavampi tai tutkimuksen voisi toistaa pidemmällä aikajänteellä analysoidakseen ilmiön pysyvyyttä. Tutkimuksen laajuutta rajaavana tekijänä tässä tutkimuksessa on, että kyseessä on pro gradu -työ. Aineiston riittävyys samoin kuin analyysi on mitoitettu pro gradun laajuudelle sopivaksi. Tutkimuksessa toteutettiin kuusi puolistrukturoitua haastattelua, joista saatiin tutkimuksen laajuus huomioon ottaen runsaasti tietoa ja näin ollen riittävä tutkimusaineisto analysoitavaksi, jotta tavoitettiin saturaation periaate. Aineisto osoitti, että tutkimusongelman kannalta ei tarvittu uutta tietoa.

Eskola ja Suoranta (1998, 48) kuvaava saturaation saavuttamista tilanteeksi, jossa vastauksia on riittävä määrä, kuin mikä on tutkimuksen kannalta välttämätöntä. Kuusi puolistrukturoitua haastattelua olivat myös laadulliselle tutkimukselle sopiva harkinnanvarainen näyte. Tarkkaan harkitut ja valitut haastateltavat ja heidän edustamansa yritykset tarjosivat sopivan pienen, mutta tutkimukseen hyvin osuvan laadukkaan näytteen. Laadukkuus mahdollisti perusteellisemman analyysin toteuttamisen. (Eskola & Suoranta 1998; Saunders et al. 2016.)

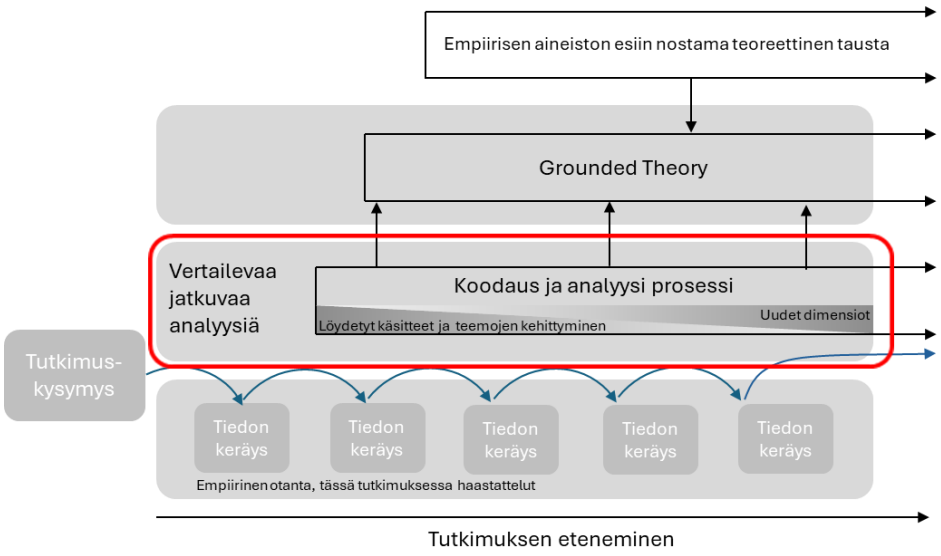
Kvalitatiivinen haastattelututkimus mahdollisti ilmiön tutkimisen läheltä, haastattelemalla ihmisiä, jotka työskentelevät kansainvälisten yritysten talousosastoilla. Näin sain tarkkaa aineistoa haastateltavien käytännön kokemuksista, tuntemuksista ja näkökulmista. Tutkimuksen aineiston analysointiin valikoitui Grounded Theory tutkimusmetodologia ja se toteutettiin Gioia metodia mukaillen. Grounded Theory -tukimustapa ja Gioia metodi sekä niiden käyttö on kuvattu tarkemmin aiempana luvussa 2.4. Grounded Theory -tutkimustapa ja Gioia-metodi sopivat tutkimukseen hyvin, koska ne perustuvat aineistolähtöiseen analyysiin ja tukevat analyysin toteuttamista kurinalaisesti. Tutkimuksen punainen lanka on toivotusti empiirisessä aineistossa, mutta analysointi haastatteluaineistosta koodauksen kautta mahdolliseen teoriaan dokumentoidaan systemaattisesti Gioia-metodia mukaillen. Näin pyrin saavuttamaan tutkimukselle tärkeän uskottavuuden panostamalla tutkimusprosessin luotettavuuteen.

Grounded Theory -tutkimusmetodin laadukkaassa käytössä lopputulokselle on tärkeää, että tutkijan taidot riittävät tutkimustavan käyttämiseen. Tässä tutkimuksessa käytän Grounded Theory -tutkimusmetodia ensimmäistä kertaa tässä laajuudessa. Koen, että onnistuin tutkimuksen pro gradu laajuuden mukaisesti analysoimaan aineiston. Erityisesti sekä ajatusprosessiani ja koodaamista tukivat luomani pääaihealuejaot, jotka esitellään seuraavassa luvussa 3. osana tutkimustuloksia. Systemaattisella empiirisen tutkimustiedon käsittelyllä, tulkinnalla ja käsitteellistämisellä Gioia-metodia mukaillen löydettiin myös vastaus tutkimuskysymykseen. (Chun Tie, Birks & Francis 2019.)

Tutkittu ilmiö, rahaliikenteeseen liittyvä huijaaminen ja rikollisuus, ja ilmenemisympäristö, globaali rahaliikenne ja jopa finanssiala, on hyvin laaja ja kansainvälinen. Aihealueelta löytyy paljon tutkittavaa. Näitä ilmiöitä voisi tutkia laajemmin, monilla eri tavoilla ja erilaisista näkökulmissa. Tässä pro gradu tutkimuksessa keskitytään aiemmin rajatun mukaiseen tutkittavaan ilmiöön ja siitä muodostettujen tutkimuskysymysten vastauksien löytämiseen. Tutkimus ei ole toistettavissa, vaan se on sidottu tähän ajanhetkeen, haastateltujen kokemuksiin ja rooliin sekä tutkijan tutkimusotteeseen juuri nyt. Luvussa 6 esitän pohdintojani tutkimuksen ja analysoinnin aikana kehittyneistä lisätutkimusaihioista.

4 Tutkimustulokset

Tutkimuksen aineiston analysointi toteutettiin Grounded Theory tutkimusmetodologiaan perustuvaa Gioia metodia mukaillen. Aineiston analyysitapa on esitelty tarkemmin luvussa 3. Alla olevassa kuviossa 12. punaisella ympyröity alue kuvaa vaihetta, jossa tieto koodataan ensin ensimmäisen tason käsitteiksi, joista kehitetään toisen tason teemat. Lopuksi teemat yhdistetään dimensioiksi.



Kuvio 12. Koodaus ja analyysiprosessi (mukaillen Wagner et al., 2010, 7).

4.1 Tutkimusaineiston analysoinnin kulku

Tutkimuksen aineiston analysointi toteutettiin Grounded Theory tutkimusmetodologiaan perustuvaa Gioia metodia hyödyntäen. Pääasiallisena teoreettisen otantana toimivat kuudessa yrityksissä talousosastolla työskenteleville henkilöille tehdyt kuusi haastattelua. Kunkin haastattelun jälkeen tallennetut transkriptiot puhtaaksikirjoitettiin aiemmin 3. luvussa kuvatusti. Haastatteluaineistosta tehtiin sitä käsiteltäessä muistiinpanoja ja lainauksia kerättiin Exceliin. Lainaukset kirjattiin haastattelu kysymysten teemojen mukaan. Lainauksista koostui 149 rivin Excel-taulukko. Tässä vaiheessa työkaluna oli yksi iso Excel-taulukko ja yksi välilehti, johon keräsin oleellisia suoria lainauksia tutkimuksen raportointia varten.

Kysymykset toimivat koottujen lainausten otsikkoina. Puolistrukturoiduissa haastatteluissa esitettiin 21 etukäteen pohdittua kysymystä. Kymmenen näistä olivat tutkimusongelman teeman mukaisia pääkysymyksiä ja yksitoista kysymystä täsmensivät pääkysymyksiä. Tämän vaiheen aikana ja jälkeen aineistoa koodattiin Excelissä ensimmäisen tason konsepteiksi. Samalla myös suodatettiin runsaasta datasta esiin tulleita lainauksia ja koodeja kohdistaen huomio tutkimusongelmaan.

Seuraavassa vaiheessa Gioian methodin mukaisesti haastattelukäsitteistä koottiin 15 toisen tason teemaa. Tässä vaiheessa palastelin Excel-taulukon eri välilehdille, jotka perustuivat edelleen haastattelun pääkysymysten aiheisiin. Pääkysymyksiä oli alun perin kymmenen, mutta tässä vaiheessa aiheotsikoita oli jäljellä neljä, jotka vielä harkinnan jälkeen kutistuivat kolmeen. Ensimmäisessä vaiheessa harkitsin pitäväni aiheet; Mitä muutoksia BEC huijauksen uhriksi joutuminen on tuonut ja millainen on huijauksen tai huijatuksi joutumisen psykologinen vaikutus työntekijöihin erillään, mutta koodaamisen edetessä ne asettuivat yhteisen otsikon alle. Näin muodostuivat alla olevalla taulukolla 3. listatut analyysin lopulliset kolme pääaihealuetta, jotka seuraavat tutkimuksen alatutkimuskysymyksien suunnan näyttäjinä. Tutkimuskysymykset kuvattiin tarkemmin luvussa 1.1.1:

”Miten uuden tiedon validoimiseen luotuun tietoprosessiin on organisaatiossa päädytty?

”Kuinka suurena riskinä huijaukset nähdään?”

”Millaisia vaikutuksia huijauksilla on organisaatiolle ja miten niistä selvitään?”

Taulukko 3. Koodauksen jäsentelyn pääaihealueet

KOODAUKSEN JÄSENTELYSSÄ KÄYTETYT PÄÄAIHEALUEET (pohjautuen haastattelukysymyksiin)	TOISEN TASON TEEMAT	DIMENSIOT
TIEDON VALIDOINTIPROSESSIIN VAIKUTTAVAT TEKIJÄT	6	3
HUIJAUSTEN ROOLI OSANA ORGANISAATION RISKIENHALLINTAA	4	1
HUIJAUKSEN UHRIKSI JOUTUMISEN VAIKUTUKSET	5	3

Pääaihealueiden alle ovat suodattuneet haastatteluiden lainauksista kootut ensimmäisen tason konseptit. Pääaihealueet muodostuivat rinnakkain 15 toisen tason teeman kanssa, joiden jakaantuminen pääaihealueiden välillä näkyy yllä olevassa taulukossa 3. Tiettyjen kysymysten vastaukset käyvät tutkimuksessa ilmi, mutta eivät olleet koodauksessa mukana, koska tälle ei ollut tarvetta. Esimerkiksi kysymys, ” Jos validointiprosessia ei ole käytössä, miksi tähän ratkaisuun on päädytty?”, osoittautui turhaksi, koska kaikilla haastatelluilla yrityksillä oli olemassa validointiprosessi.

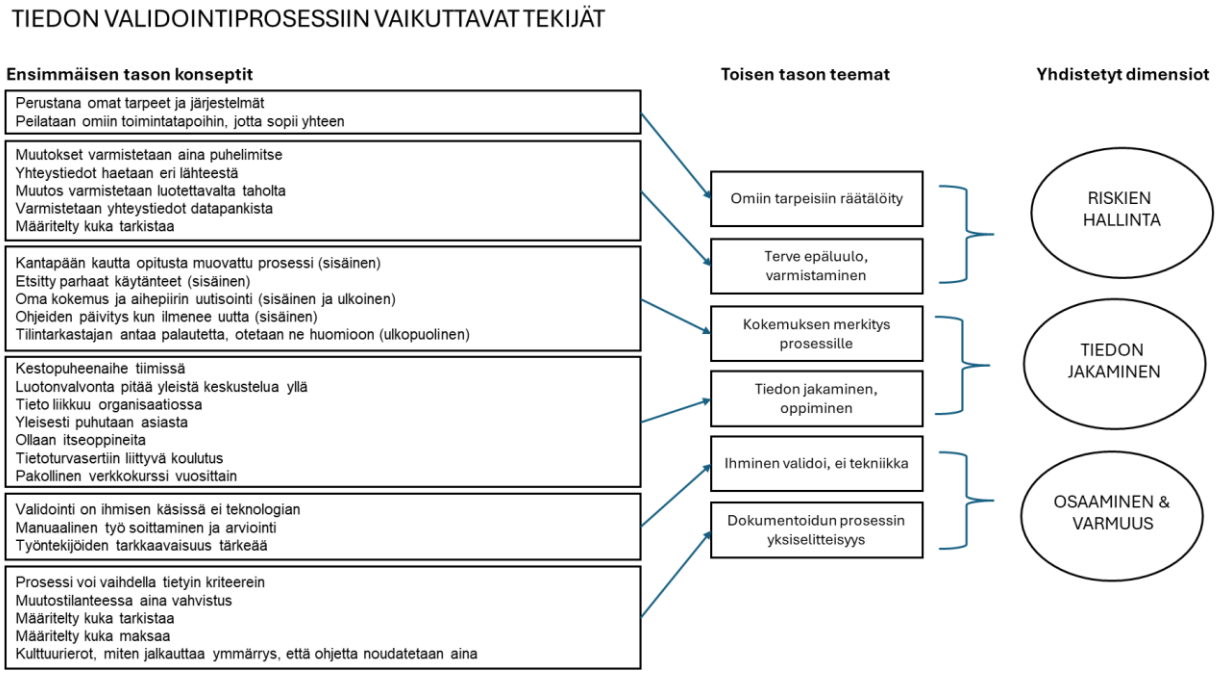
Viimeisessä analysointivaiheessa kolmen eri pääaihealueen alle jakautuneet toisen tason teemat yhdistettiin dimensioiksi. Näitä ulottuvuuksia muodostui tutkimuksessa kolme: tiedon jakaminen, osaaminen & varmuus sekä riskien hallinta.

4.2 Tulosten esittely

Tässä luvussa käydään tarkemmin läpi taulukossa 3. listatut kolme pääaihealuetta. Analyysin aikana muodostui sekä koodausta tukemaan, että tutkimusongelmaan: *”Millainen on tietojohtamisen rooli riskienhallinnassa, kun organisaatiossa pyritään suojautumaan uuden tiedon käyttämiseen liittyviltä riskeiltä?”,* keskittyen kolme pääaihealuetta. Ensimmäisenä käsitellään tiedon validointiprosessiin vaikuttavat tekijät luvussa 4.2.1, seuraavaksi huijausten rooli osana organisaation riskienhallintaa luvussa 4.2.2 ja viimeisenä huijauksen uhriksi joutumisen vaikutukset luvussa 4.2.3.

4.2.1 Tiedon validointiprosessiin vaikuttavat tekijät

Alla oleva kuvio 13. esittelee ensimmäisen pääaihealueen, tiedon validointiprosessiin vaikuttavat tekijät. Kuva osoittaa miten haastatteluaineistosta suodattui Gioian metodia mukaillen kooditasojen kautta tiedon validointiin vaikuttavat dimensiot. Nuolet kuvioissa 13. osoittavat miten ensimmäisentason konseptit ryhmittyvät toisen tason teemoiksi ja siitä edelleen teemat yhdistyvät ulottuvuuksiksi. Tämä luku vastaa ensimmäiseen alatutkimuskysymykseen: *”Miten uuden tiedon validoimiseen luotuun tietoprosessiin on organisaatiossa päädytty?”*



Kuvio 13. Tiedon validointiprosessiin vaikuttavat tekijät (mukaillen Corley & Gioia, 2004, 184)

Ensimmäisen tason konsepteista rakentui kuusi toisen tason teemaa: organisaation omat tarpeet, terve epäluulo ja varmentaminen, kokemuksen merkitys prosessille, tiedon jakaminen ja oppiminen, ihminen validoi ja dokumentoidun prosessin yksiselitteisyys)

Kaikissa kuudessa haastatellussa organisaatiossa oli määritelty prosessi tilitiedon tarkastamiseen. Tärkein punainen lanka käytetyssä prosessissa oli, että se oli 1) *organisaation omiin tarpeisiin räätälöity*. Virallisten tahojen ohjeita tai aiheesta mahdollisesti tarjolla olevia ulkopuolisia koulutuksia ei aktiivisesti seurattu. Ennemminkin seurattiin kyberuhkiin ja huijauksiin liittyvää uutisointia yleisellä tasolla ja muutamassa vastauksessa muisteltiin, että jotakin ulkoisia ohjeita on joskus kyllä nähty. Omat prosessit on rakennettu oman liiketoiminnan tarpeisiin, omiin järjestelmiin sopiviksi ja niin, että sopivat yhteen yrityksen toimintatapojen kanssa. Halutaan, että on toimiva prosessilla, jolla saadaan riittävä varmuus tiedon oikeellisuudesta, mutta sen on oltava myös tehokas kokonaisuuden näkökulmasta.

(H1) ”Ollaan itseoppineita, yritetty miettiä mikä on meidän kannalta, järjestelmien ja prosessien kannalta järkevät tavat toimia. Sen kautta, että kun tosiaan on muutama tällainen keissi ollut. Sitä kautta opittu, että miten on järkevä varmistella näitä.”

Prosesseissa korostuivat 2) *terve epäluulo ja sitä kautta varmentamisen tarve*. Validointi prosessit sisälsivät elementtejä kuten, tiedon varmistaminen, roolit kuten kuka tarkastuksen tekee ja kuka päivittää maksunsaajan uudet tiedot rekisteriin. Haastatteluissa keskityttiin olemassa olevien toimittajien ilmoittamiin tilitietojen muutoksiin. Näissä tapauksissa toimintatavat olivat melko yhtenäisiä. Kaikissa haastatelluissa yrityksissä varmistettiin muutos toisesta lähteestä sekä toista kanavaa käyttäen. Pelkän sähköpostilla lähetetyn muutosilmoituksen perusteella, ei tehty muutoksia maksunsaajarekiosteriin. Yleisin tapa varmistaa sähköpostilla tullut tieto oli soittaminen. Puhelun soittaa joko sovittu henkilö talousosastolta, ostaja, talousjohtaja tai vastaava. Entuudestaan toisilleen tutut henkilöt hyödynnetään prosesseissa, eli tuttu henkilö soittaa hänelle tutulle henkilölle varmistuspuhelun.

(H2) ”Mitä kautta se meille tulee, että on se sitten laskulla tai paperisena tai sähköpostilla, niin meillä on ollut sopimus prosessista. ”Me varmistetaan se vielä jollain toisella tavalla, sieltä toimittajalta. Joko soittamalla sinne firmaan, ei sellaiseen numeroon, joka näkyy siinä kyseisessä viestissä, vaan johonkin muuhun. Katsotaan jostain ihan oikeasti, vaikka nettisivuilta tai vanhoista sähköposteista, niin joku muu numero. Tai sitten vaihtoehtoisesti sähköpostilla, mutta ei vastata siihen sähköpostiin, vaan lähetetään ihan uusi viesti.”

Prosessi ei usein ollut kaikkien kauppakumppanien kanssa samanlainen, eroja ilmeni erityisesti kotimaisten ja ulkomaisten toimittajien välillä. Ulkomaisten tahojen kanssa nähdään kohonnut riski, joka vaatii eritystä varovaisuutta. Kotimaisten toimittajien kassa muutokset on tyypillisesti helppo varmistaa ja ylipäänsä yleisin laskutustapa, verkkolaskutus, koetaan turvallisena. On hyvä huomioida, että haastateltavat tarkoittavat verkkolaskutuksella aitoa verkkolaskua, joka lähetetään, käsitellään ja vastaanotetaan konekielisenä. Aineisto on digitaalista ja rakenteisessa muodossa eli toteutetaan sovitun standardin mukaisesti (Tieke 2023). Standardisoitu muoto mahdollistaan verkkolaskun automatisoinnin pankkiyhteysohjelmien ja taloushallinnonjärjestelmien välillä eri organisaatiosta toiseen. Verkkolasku ei näin ollen ole esimerkiksi sähköpostilla lähetetty lasku. Useammalla tuli myös esiin, että tietosia riskejä otetaan pienempien summien kanssa. Tämäkin vain siinä tapauksessa, että tilinumeron muutoksen varmistaminen ei ole yrityksistä huolimatta onnistunut sovitulla tavalla eli tyypillisimmin puhelimitse. Tilanne analysoidaan ja jos muuten kaikki tilanteessa täsmää otetaan tietoinen riski summan ollessa pieni.

Kysyttäessä eroavuuksista prosesseissa uusien kauppakumppaneiden kanssa rahaliikenteen aloittamistilanteessa, toimintatavoissa oli paljon enemmän eroavaisuuksia vastauksien välillä. Huijausriskiä näissä tielanteissa pidettiin pienempänä, koska kumpikin osapuoli hyötyy tilanteesta. Toimittaja on tehnyt kaupat ja saa sopimuksen mukaisen korvauksen toimittamastaan tavarasta tai palvelusta. Kauppasopimuksilla ei yleensä määritelty pankkiyhteyksiä, mutta joskus ne voivat olla annettuina tietoina jo sopimuksen tekovaiheessa. Uuden toimittajan perustaminen tarvittaviin järjestelmiin oli oma prosessinsa. Näissä prosesseissa oli erilaisia tapoja eri yrityksissä. Tähän prosessiin kuuluvia elementtejä olivat esimerkiksi tuntemisprosessi (KYC), sanktio- ja pakotetarkistukset, yhteystietojen- ja maksutietojen tallentaminen sekä toimittajan ESG-arvio. Ensimmäisen laskun saapuessa toimittiin toisissa yrityksissä vastaavasti kuin muutostilanteissa eli tilitieto vielä erikseen varmistettiin soittamalla.

Kaikissa haastatteluissa tuli korostetusti esiin 3) *kokemuksen merkitys prosessin* muotoutumiselle. Siinä missä ulkopuolisia ohjeita ei tunnettu ja niitä ei aktiivisesti seurattu niin kokemukseen luotettiin. Prosessin kuvattiin muotoutuneen omien kokemusten kautta, kantapään kautta opittuna ja sisäisesti parhaita käytänteitä hioen. Ulkopuoliset impulsseja kuitenkin tunnistettiin, kuten aihepiirin uutisointi ja tilintarkastajalta saadut palautteet. Täysin ei siis umpiossa nähty prosessin syntyneen ja siitä todisteena sekin, kuinka kaikki toimivat hyvin saman kaltaisesti toisiinsa nähden. Kokemusten merkitys ja kunkin yrityksen toimintaympäristöt muokkaavat lopulta validointi prosessista kullekin yritykselle oman laisensa.

(H4) ”Kantapään kautta päädytty tähän. Meillä on kaksi tapausta ollut, jonka jälkeen osataan olla hereillä. Ensimmäisessä tapauksessa menetettiin vähän rahaa.”

Prosessin kehityksessä tärkeään rooliin nostettiin myös 4) *tiedon jakaminen ja oppiminen.* Toisissa yrityksissä oli vuosittaisia verkkokursseja tai vastaavia suoritettavia tehtäviä, mutta pääroolissa oli aiheen ympärillä käyty keskustelu. Aihetta pidettiin kestopuheenaiheena ja koettiin, että tieto ja oppi siirtyvät näissä keskusteluissa. Mainittiin myös kuinka tietyn työnkuvan omaavat henkilöt erityisesti tuovat kyberuhka-aiheita keskusteluun erityisen aktiivisesti ja näin jakavat osaamistaan laajemmalle joukolle.

(H2) ”Ei ole vuosittaista kolutusta, mutta aina säännöllisin väliajoin tiimissä puhutaan. Puhutaan myös koko organisaation lävitse, että aina silloin tällöin nostetaan asia esiin. Ja meillä on erikseen esimerkiksi luotonvalvonta porukka niin he monesti saattaa näitä jutella toimistolla kaikkien kuullen. Vähän ehkä haastaakin välillä siinä aiheessa ja sillain, että meillä on aktiivinen keskustelu tän

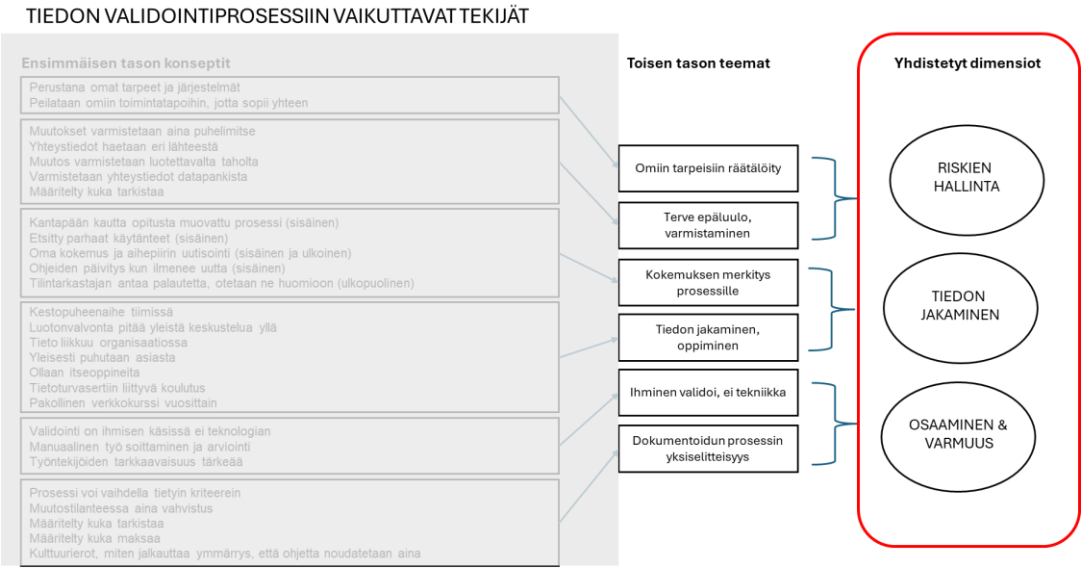
aiheen ympärillä. Varsinkin, jos meille tulee huijaus, niistä melkein aina siinä kohtaa käydään yhteisesti keskustelu. Mistä joku tiesi, että se on huijauskirje ja mitä tässä nyt taas pitikään tehdä ja tavallaan että pidetään semmoisella keskustelulla sitä tietoisuutta yllä vähän koko ajan."

Validointiprosessi on *5) ihmisen käsissä ei teknologialla toteutettavissa*. Se, että validoinnille löytyy selkeä prosessi, ohjeet ja taidot on oleellista, sillä tiedon käyttöönoton validoinnin toteuttaa ihminen. Mitään työkalua tai ohjelmistoa tähän tarkoitukseen ei ole. Kauppakumppaneilta ei edes pääsääntöisesti pyydetä pankin laatimaa todistusta tilinomistajuudesta. Niitä ei pidetä luotettavina, koska ne koetaan helpoiksi väärentää. Tämän kaltaista palvelua, jossa tilinumeron voisi varmistaa pankilta tai vastaavalta toimijalta suoraan, pidettiin tervetulleena apuna tulevaisuudessa. Kriteerinä mahdollisille työkaluille tai palveluille on ehdoton luotettavuus. Pääasiallinen tapa tiedon aitouden varmistamiselle on jo aiemmin mainittu soittaminen. Tilanteesta ja yrityksestä riippuen soittaja on henkilö, joka tuntee toimittajan parhaiten. Tyypillisimmin ostaja tai henkilö talousosastolta.

Viimeisenä toisen tason teemana kuviossa 5. on 6) *dokumentoidun prosessin yksiselitteisyys*. Osoittautui tärkeäksi, että prosessi on olemassa, että se tukee työntekijöitä työssään ja on osa yrityksen toimintaympäristöä. Organisaation jäsenet pitkälti luovat prosessit omien kokemustensa kautta, yhdessä ja toisiltaan oppien, kuitenkin ulkoiset tietosyötteet huomioiden. Näin ollen selkeä prosessin olemassaolo, dokumentoituna ja ohjeistettuna, toimi työkaluna työntekijöille. Yksiselitteisyys loi pohjaa erikoistilanteiden hoitamiseen ja selkeytti roolijakoa, kuka tekee mitäkin. Validointiprosessin jalkauttamisessa oli myös koettu kulttuurieroja. Ulkomaisten tyttärien kanssa toimiessa on pitänyt tehdä erilaisia toimenpiteitä näiden kulttuurierojen takia. Nämä olivat tulleen esiin erityisesti toimitusjohtajahuijauksissa. Vaati sinnikästä opastusta, koulutusta ja keskusteluja, että oli saatu kaikki ymmärtämään, että prosessi ja siinä annetut käytänteet olivat pakollisia. Oli saatava jalkautettua, että sähköpostitse saatu tilitieto tai maksupyyntö varmistetaan aina, tästä säännöstä ei poiketa koskaan. Tämän periaatteen läpivieminen kaikissa toimipisteissä kulttuurista ja aiemmista toimintatavoista poiketen oli osoittautunut erittäin työlääksi projektiksi.

(H3) "Ja sen jälkeen nää prosessit on hiottu kuntoon ja silloin kyllä tuli tappioita. Me tehtiin ne ohjeistukset ja verkkokurssit. Kyselyt, miten yhtiöt toteuttaa niitä. Sen jälkeen me otettiin sisäiset tarkastukset ja me mennään jopa paikan päälle valvomaan, että ne oikeasti toteutuu." (tytäryhtiöt ulkomailla)

Lopuksi kuvioon 14. listatuista tiedon validointiin vaikuttavista ensimmäisen tason konsepteista, päästiin kuuden listatun ja tässä luvussa esitellyt toisen tason teemojen kautta kolmeen dimensioon; riskien hallinta, tiedon jakaminen ja osaaminen ja siitä kumpuava varmuus. Kolme dimensiota eli ulottuvuutta on rajattu kuviossa 14. punaisella.

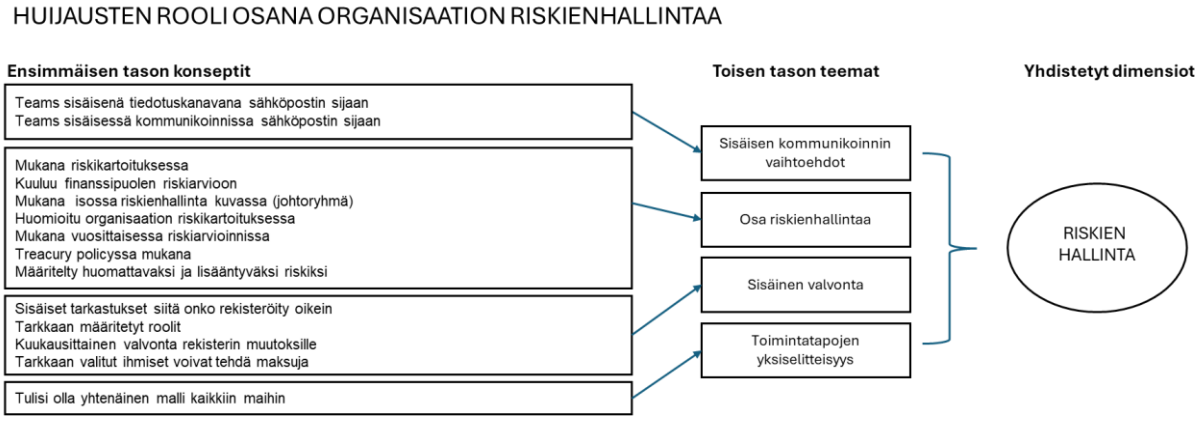


Kuvio 14. Tiedon validointiprosessiin vaikuttavien tekijöiden yhdistetyt dimensiot (mukaillen Corley & Gioia, 2004, 184)

Nuolet osoittavat kuvioissa 13. ja 14. miten ensimmäisentason konseptit ryhmittyvät toisen tason teemoiksi ja siitä edelleen teemat yhdistyvät ulottuvuuksiksi. Tutkielman aloituspisteen mukaisesti tutkimuksella haetaan vastausta tutkimusongelmaan. Samaan aikaan kun empiirinen tutkimusaineisto kertoo haastatteluaineiston kautta tutkittavasta ilmiöstä haastateltujen sanoin niin tutkimusta vie eteenpäin myös tutkimuskysymys, jolle haetaan vastausta. Tässä luvussa käsiteltiin ensimmäinen kolmesta pääaihealueesta; validointiprosessiin vaikuttavat tekijät.

4.2.2 Huijausten rooli osana organisaation riskienhallintaa

Alla oleva kuvio 15. esittelee vuorostaan toisen pääaihealueen huijausten roolin osana organisaation riskienhallintaa. Kuvio osoittaa miten empiirisestä tutkimusaineistosta suodattui Gioian metodia mukaillen ensimmäisen ja toisen kooditason kautta huijausten rooliin osana organisaation riskienhallintaa viittaavat dimensiot. Nuolet kuvioissa 15. osoittavat miten ensimmäisentason konseptit ryhmittyvät toisen tason teemoiksi ja siitä edelleen teemat yhdistyvät ulottuvuuksiksi eli dimensioiksi. Tämä luku vastaa toiseen alatukimuskysymykseen: *”Kuinka suurena riskinä huijaukset nähdään?”*.



Kuvio 15. Huijausten rooli osana organisaation riskienhallintaa (mukaillen Corley & Gioia, 2004, 184)

Pääaihealueen, huijausten rooli osana organisaation riskienhallintaa, ensimmäisen tason konsepteista rakentui neljä toisen tason teemaa: sisäisen kommunikoinnin vaihtoehdot, tiedon validointi osana riskienhallintaa, sisäinen valvonta ja toimintatapojen yksiselitteisyys.

Yhdessä yrityksessä oli siirrytty *1) sisäisessä kommunikoinnissa* ja huijausviestinnässä Temsin käyttöön sähköpostin sijaan. Tämä toimintatapa oli poissulkenut toimitusjohtajahuijaukset sähköpostitse kokonaan pois riskilistalta. Teams:ia käytettiin myös tehokkaasti tiedotuskanavana huijauksiin liittyen, muun muassa lähetettiin kanavaan näytille, minkälainen epäilyttävä viesti oli vastaanotettu. Tämä mahdollisti ajatustenvaihdon heti tuoreeltaan viestiin

liittyen sekä kaikki näkivät millaisia huijausviestejä, oli aina liikkeellä. Organisaatiossa koettiin Teams:in hyödyntäminen hyvin tehokkaana ja tervetulleena muutoksena.

(H6) ”Just mietin tuossa noita sähköposteja, että joskus kauan sitten olihan ne aika paljon tönkömpiä. Taas toisaalta, että nykyään kun meidän viestintä on teamsissa niin sen nyt jo tietää, että jos sähköpostilla tulisi toimitusjohtajalta viestiä, että se ei ole todellinen, koska emme viesti sisäisesti sähköpostilla.”

Keskusteltaessa siitä kuinka suurena riskinä huijausviestejä yrityksessä pidetään riskikartoituksen tai vastaavan riskien kokonaiskuvan kontekstissa, oli kaikilla haastatelluilla yrityksillä huijaukset ja kyberuhat oleellinen *2) osa riskienhallintaa*. Riski on määritelty muun muassa huomattavaksi ja lisääntyväksi ja se huomioidaan riskiravioissa tai -kartoituksissa. Näin ollen huijaukset saivat organisaatioissa huomiota ja painoarvoa osana riskiarviointeja.

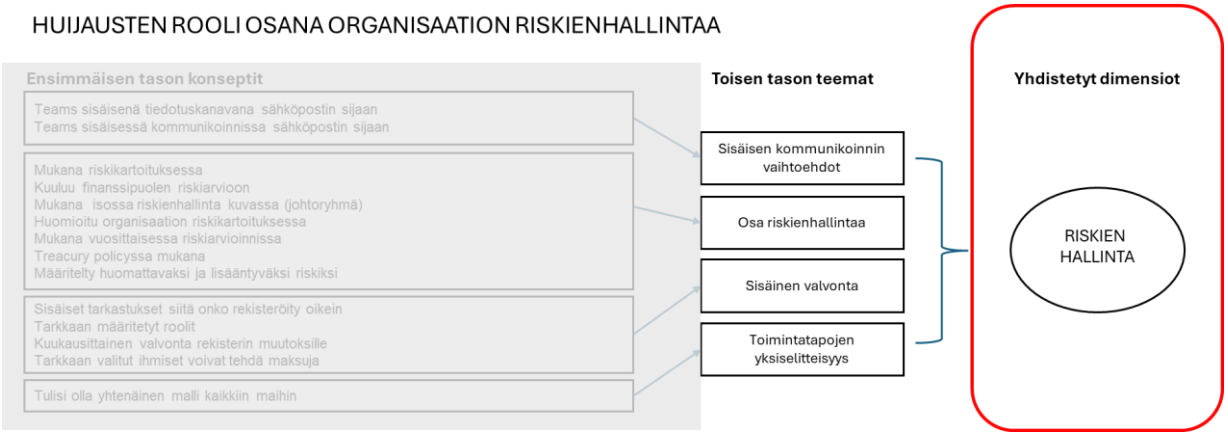
(H5) ”Meillä on konsernitasolla treasury policy, jossa on määritelty konsernissa hyvät talouspraktiikat tai tämmöiset prosessit, että esimerkiksi maksuliikenteeseen ja laskujen ja maksujen hyväksymiseen liittyvät toimintatavat. Ja sitten meillä on kansainvälisen pakoteseurannan ja kaupallisten riskien hallintaprosessi olemassa.”

Kolmanneksi toisen tason teemaksi nostin *3) sisäisen valvonnan*. Sen lisäksi, että tilitiedon validoinnille oli kehitetty toimintatavat, oli ympärille usein kehitetty myös sisäistä valvontaa. Tämä ilmeni erilaisin tarkastuksina kuten maksurekisterin muutosten valvonta, jossa tarkistettiin kuukausittain, että tehdyt muutokset oli toteutettu prosessin mukaan. Oleellista sisäistä valvontaa olivat myös tarkkaan määritellyt roolijaot sille kuka saa tehdä mitäkin.

(H3) ”Verkkokurssi on semmoinen, miten saa väen opetettua ja millä pystyy oikeaa työtapaa välittämään eteenpäin. Mutta me valvotaan myös, eli tehdään vuosittain sisäisiä tarkastuksia meidän yhtiöihin ostoreskontramaksujen kotrollien toteuttamisista.”

Myös riskienhallinnan näkökulmassa nousi esiin *4) toimintatapojen yksiselitteisyys*. Erityisesti korostui, toimintatapojen yhdenmukaistaminen kaikissa konsernin yhtiöissä kuten ulkomaisissa tyttärissä ja myös yritysostojen yhteydessä uuden yrityksen sisäänajo konsernin toimintatapoihin.

(H5) ”Tää on semmoinen asia, mikä tulevallakin tilikaudella on yks tärkeimpiä kehitysasioista. Että me saataisiin sisäisen valvonnan prosessi, jossa voitaisiin varmistaa, että tän tyyppiset asiat on samalla tasolla kaikissa yksiköissä. Mutta on puutteita kyllä, tuolla ulkomailla enemmän kuin Suomessa ja se on paha tilanne kun ei ihan tiedä.”

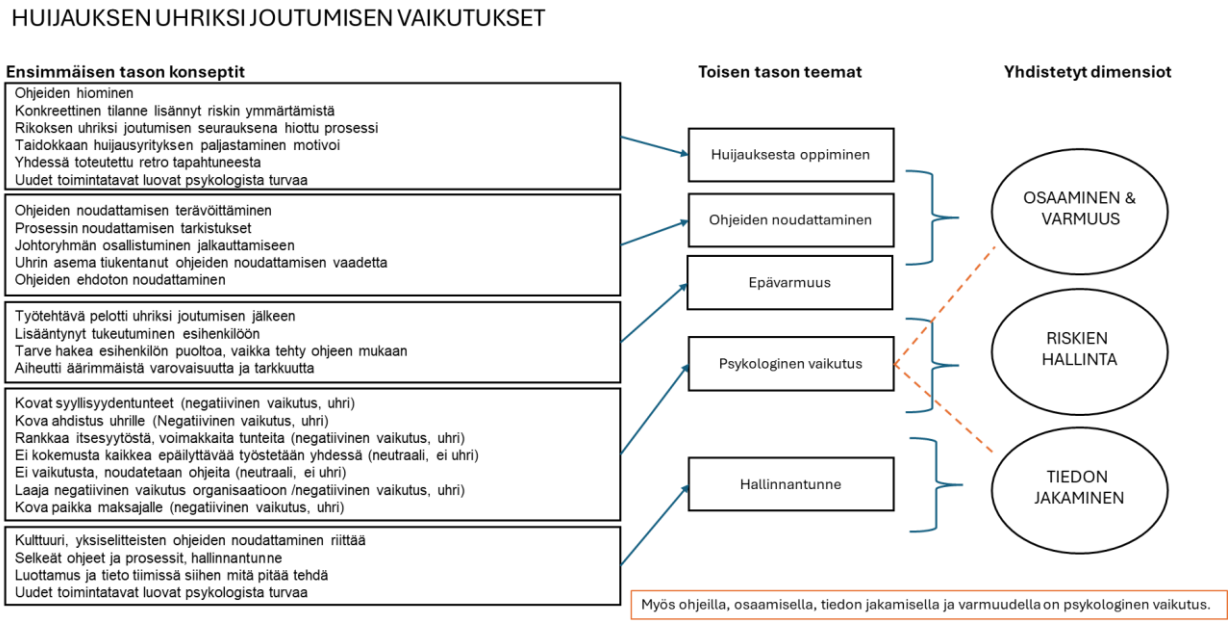


Kuvio 16. Huijausten rooli osana organisaation riskienhallintaa -osion yhdistetyt dimensiot (mukaillen Corley & Gioia, 2004, 184)

Kuvio 16. kuvaa miten luvussa kuvatut toisen tason teemat yhdistyvät kaikki yhden, jo edellisestä luvusta tutun, dimension alle. Toisena käsitelty pääaihealue huijausten rooli osana organisaation riskienhallintaa suodattuu kokonaisuudessa riskien hallinta dimension sisään. Ensimmäisen tason konsepteja tarkemmin katsoessa, löytyy yhteys myös edellisen luvun dimensioihin tiedon jakaminen ja osaaminen. Tiedon jakaminen sisäisiä kommunikoinnin vaihtoehtoja pohdittaessa tai osaaminen osana toimintatapojen yksiselitteisyyttä. Mutta tässä luvussa katsotaan konsepteja ja teemoja rikienhallinnan lasien läpi eli miten ne palvelevat rikien hallintaa.

4.2.3 Huijauksen uhriksi joutumisen vaikutukset

Alla oleva kuvio 17. esittelee kolmannen pääaihealueen, huijauksen uhriksi joutumisen vaikutukset. Kuvio osoittaa, kahden aiemman luvun tapaan, miten tutkimusaineistosta tehdyt aihealueen ensimmäisen ja toisen tason koodaukset kuljettavat analyysia kohti yhdistettyjä dimensioita. Tämä luku vastaa kolmanteen alatutkimuskysymykseen: *”Millaisia vaikutuksia huijauksilla on organisaatiolle ja miten niistä selvitään?”*



Kuvio 17. Huijauksen uhriksi joutumisen vaikutukset (mukaillen Corley & Gioia, 2004, 184)

Viimeisenä käsiteltävän pääaihealueen, huijauksen uhriksi joutumisen vaikutukset, ensimmäisen tason konsepteista suodattui viisi toisen tason teemaa: huijauksesta oppiminen, ohjeiden noudattaminen, epävarmuus, psykologinen vaikutus ja hallinnantunne. Kuudesta haastatellusta yrityksestä puolet olivat tulleet huijatuiksi, ja kaikki olivat kohdanneet erilaisia yrityksiä mukaan lukien BEC-huijausyrityksiä. Huijausyrityksistä yleisin muoto oli toimitusjohtajahuijaukset, mutta vastausten perusteella ne myös tunnistettiin tehokkaasti.

Ensimmäisen tason konsepteista nousi selkeästi esiin *1) huijauksista oppiminen* vaikuttimena validointiprosessien kehittämiseen. Konkreettiset tilanteet olivat myös lisänneet ymmärrystä, joskus aiemmin turhanakin pidettyjä toimintatapoja kohtaan. Huijausten seurauksena oli tukittu prosesseissa mahdollisesti olleita aukkoja, mutta myös taidokkaan huijausyrityksen tunnistaminen oli motivoinut ja suorastaan innostanut työntekijöitä.

(H4) ”Ostajaan meni ihan täydestä. Se oli normi viestien ja muiden ihan oikeiden asioiden mukana ja kaikki sanamuodot, sanavalinnat ja tämmöiset, se tyyli täsmäsi. Ostaja välitti sen maksajalle, että tämmöinen, mutta tässä on uudet tilitiedot tähän laskuun. Maksaja oli sitten heti, että joo mutta että meillä on nyt tämmöinen käytäntö, että nyt täytyy sun sitten vielä soittaa. Tämä oletettu yhteyshenkilö lähetti pankin todistuksen, mikä näytti ihan oikealta, mutta maksaja oli edelleenkin tiukkana. Että oletko sä soittanut sille yhteyshenkilölle, ja sitten ostaja viimeiseksi luovuttiin ja soitti. Yhteyshenkilö kertoi, että ei hän ole mitään viestiä lähettänyt.”

Huijaustilanteet olivat myös tiukentaneet *2) ohjeiden noudattamisen* ehdotonta vaatimusta. Sovittuja toimintatapoja oli uhriksi joutumisen jälkeen sekä hiottu, että niiden painoarvoa ja ehdotonta noudattamista oli tiukennettu. Lisäksi prosessia oli jalkautettu organisaatioon kampanjan omaisesti ja näin varmistettu, että kaikki olivat jatkossa toimintatavoista tietoisia. Samalla oli myös luotu ohjeiden noudattamiseen seurantatapoja. Asian tärkeyden painottamisessa oli muun muassa käytetty johtoryhmää sanomanviejänä toimintatapojen jalkauttamisessa. Tämä oli koettu tarpeelliseksi konsernin ulkomaalaisissa yhtiöissä.

(H1) "Kyllä, meillä oli ohjeistus olemassa aikaisemminkin, joka oli oikeastaan sama ohjeistus. Mutta sitten se oli hukkunut jonnekin arkistoon ja työntekijät oli vaihtunut. Kun oli tämä huijauskeissi niin käytiin sen jälkeen tarkasti läpi, että mitä tapahtui ja teamsissä istuttiin ja käytiin läpi prosessi step by step - näin toimitaan. Meillä on olemassa kirjalliset ohjeistukset ja Teams ohjeistukset ja nyt niitä noudatetaan"

Huijaustilanteet olivat aiheuttaneet työntekijöille erityistä *3) epävarmuutta* työn suorittamisessa huijatuksi tulemisen jälkeen. Työn teko oli muuttunut äärimmäisen varovaiseksi ja esihenkilöön tukeutuminen oli lisääntynyt. Esimerkkitilanteessa validointiprosessi oli selkeä, ohjeet olivat hyvät ja jalkauttamiseen oli käytetty runsaasti aikaa, ja silti työntekijät kokivat tarpeelliseksi hakea vielä hyväksynnän esihenkilöltä, vaikka tämä ei ollut osa prosessia.

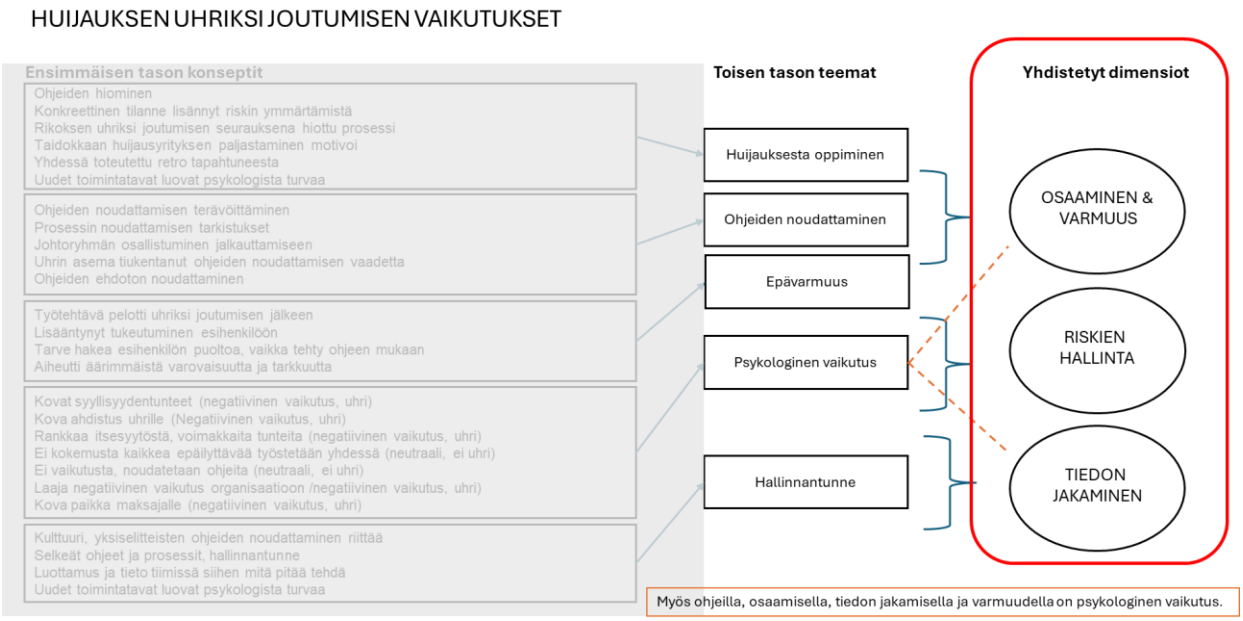
(H4) ”Sitten on puhuttu meidän maksajien kanssa monta kertaa, kun näitä on ollut ja tiedetään että tämmöistä ihan oikeasti tapahtuu niin on tullut vähän pelkoa, että aina kun on jotain vähänkään kummallista niin tulee epävarmuus että voiko tähän luottaa. Ja se ahdistus, varsinkin mitä suuremmista maksuista on kysymys, niin sitä varovaisempi on sen kanssa.”

Huijauksin uhriksi joutumisella oli huomattavia *4) psykologisia vaikutuksia* niitä kokeneissa yrityksissä. Niissä yrityksissä, jotka olivat kokeneet vain huijausyrityksiä, kokemukset eivät olleet vastaavia. Työntekijät, jotka olivat olleet osana huijaustilannetta, tunsivat kovia syyllisyyden tunteita, ahdistusta ja rankaa itsesyytöstä. Yhdessä yrityksessä nämä tunteet olivat jopa aiheuttaneet irtisanoutumisen. Negatiiviset vaikutukset ulottuivat myös laajemmin organisaatiossa, kuin vain suoraan heihin, joille kokemus oli henkilökohtainen. Viimeisen teeman, hallinnantunne, kohdalla ensimmäisen tason konseptina nousi esiin myös uusien, parempien toimintatapojen tuoma psykologinen turva. Näin nähtynä negatiivisista ja vaikeista tilanteista voidaan myös päätyä myös positiiviseen efektiin.

(H3) ”Se kamala syyllisyyden tunne ja paineet. Se veti ihmisiä sairauslomalle ja irtisanoutumaan. Sitten kun me vietiin ensimmäisiä versioita meidän uusista ohjeistuksista, niin se oli iso viesti meiltä. Kun me noudatetaan näitä meidän johtoryhmän ja hallituksen hyväksymiä sääntöjä ja kontrolleja, niin me turvataan se meidän oma työ. Se on se oma selusta, että kun me noudatetaan näitä niin me voidaan mennä tyytyväisin mielin nukkumaan ja olla varmoja, että me ollaan tehty kaikki mahdollinen.”

Viimeisenä teemana, huijauksen uhriksi joutumisen vaikutuksista, nousi *5) hallinnantunne*. Kysyttäessä keinoja, joilla voitiin hallita negatiivisia uhriksi joutumisen vaikutuksia, nousi esiin keinoja kasvattaa hallinnantunnetta eli päästä pelon ja epävarmuuden tunteista eteenpäin. Tärkeää oli, että yrityksen organisaatiokulttuuri osoittaa, että on olemassa sovittu prosessi ja jos sitä noudattaa se riittää. Haastatellut kokivat, että yksiselitteiset ohjeet, prosessit ja toimintatavat luovat psykologista turvaa ja hallinnantunnetta. Hallinnantunteen luojana toimii myös luottamus ja tiimissä selkeä tieto mitä kunkin rooliin kuuluu. Haastatteluissa moni kiinnitti huomiota siihen, että tuuraajien osalta olisi hyvä parantaa heidän osaamistaan ja sitä kautta hallinnantunnetta ja varmuutta.

(H2) ”Aina jos, tulee joku tilinumeromuutos niin kaikilla vähän niinku nousee tuntosarvet aina pystyyn. Tavallaan että melkein ennemmin epäillään huijausta, kuin että annettaisiin mennä vaan. Meillä luottamus siihen, että me tiedetään mitä meidän pitää tehdä, jos tulee just jotain tämmöisiä muutoksia. Meillä on varmaan vähän semmoinen hallinnantunne.”

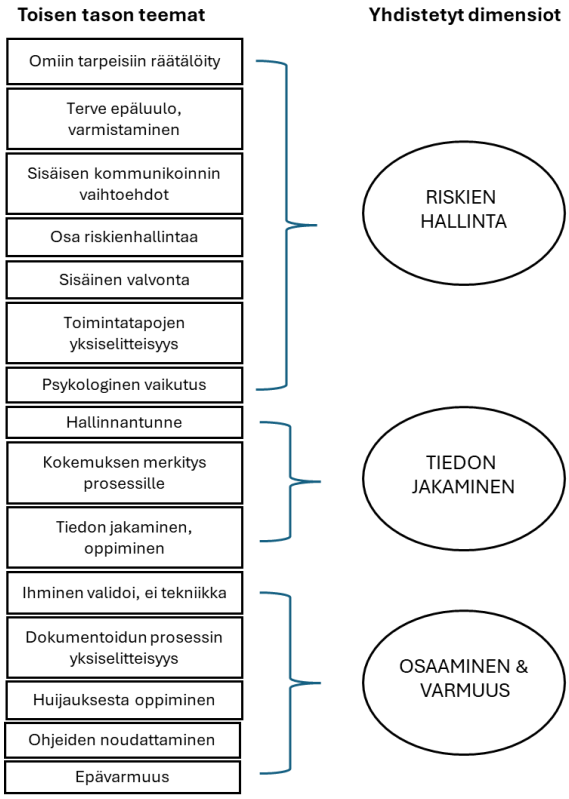


Kuvio 18. Huijauksen uhriksi joutumisen vaikutukset aihealueen yhdistetyt dimensiot (mukaillen Corley & Gioia, 2004, 184)

Kuvio 18. näyttää miten luvussa kuvatut toisen tason viisi teemaa yhdistyvät kolmen, edellisistä luvuista tuttujen dimensioiden alle. Oranssit katkoviivat kuvaavat, miten psykologisiin vaikutuksiin löytyi yhteys kaikkien kolmen dimension kanssa. Näen kuitenkin, että negatiivisten psykologisten vaikutusten ennaltaehkäisyn työkalut kuuluvat riskien hallinnan työkalupakkiin.

4.3 Tulosten yhteenveto ja pohdinta

Kaiken kaikkiaan empiirisestä tutkimusaineistosta suodattui koodauksen edetessä 15 toisen tason teemaa ja kolme dimensiota; riskien hallinta, tiedon jakaminen sekä osaaminen & varmuus, jotka on listattu alla kuviossa 19. Dimensiot voi nähdä työkalupakkeina, joista löytyy sopiva työkalu niihin linkitettyihin teemoihin.



Kuvio 19. Kaikkien aihealueiden toisen tason teemat ja niistä yhdistetyt dimensiot (mukaillen Corley & Gioia, 2004, 184)

Riskien hallinnan työkalupakissa on organisaation toimintaympäristön ymmärrys. Kokonaiskuva organisaation toiminnoista, joka mahdollistaa yksityiskohtien kuten tiedon validointiprosessin räätälöinnin omiin tarpeisiin sopivaksi. Riskien hallinnan tavoitteet ja painopisteet määrittävät toivotun mittariston varmistamisen tasoille, sisäiselle valvonnalle ja toimintatavoille. Riskien hallinnan tontille kuuluvat myös käytettävät ohjelmistot ja järjestelmät, kuten tässä tutkimuksessa mainitut kommunikointikanavat. Haastatteluissa kävi ilmi, että huijaukset ja erilaiset kyberuhat huomioidaan organisaation riskiarvioinnissa kaikissa tutkituissa yrityksissä. Psykologisten negatiivisten vaikutusten vakavuus ja voimakkuus yllättivät empiirisessä aineistossa eniten. Tämän vaikuttavuuden vuoksi nostin myös psykologiset vaikutukset riskien hallinnan piiriin. Näkisin, että negatiivisten vaikutusten ennaltaehkäisy on tärkeää ja siihen olisi syytä löytyä hyvät työkalut valmiiksi mietittynä. Näin vältyttäisiin tai vähennettäisiin yllätyksen aiheuttamalta lamaannukselta työntekijöiden keskuudessa, sekä taloudellisen menetyksen todennäköisyys pienenisi ennaltaehkäisevien varotoimien ansiosta.

Tiedon jakamisen työkalupakki tarjoaa työkalut uuden tiedon validointiprosessin kehittymiselle. Prosessi muodostuu ja muokkautuu kokemusten kautta. Yritys pystyy hyödyntämään yksilöiden kokemuksia ja tiedon siirtymistä työntekijöiden keskuudessa. Työntekijät oppivat virheistä, onnistumisista sekä omista ja toisten kokemuksista. Validointiprosessi hioutuu ja pysyy ajan tasalla, kun jaettu tieto ja kokemukset vaikuttavat siihen koko ajan. Kehitystyö ei koskaan lopu, koska ulkoiset tietosyötteet kuten huijausyritykset ja aihealueen uutisointi muuttuvat ympäristön muutosten mukana. Tästä oleellisin esimerkki on teknologian kehitys. Tiedon ja kokemusten jakaminen esimerkiksi keskusteluissa lisäävät hallinnantunnetta, kun yksilö ei jää yksin ajatustensa kanssa. Tiedon jakamisen tuoma hallinnantunne edesauttaa omalta osaltaan negatiivisista psykologisista vaikutuksista toipumiseen ja toisten kokemuksista oppiminen myös osoittaa, että muillekin on käynyt vastaavia tilanteita. Huijaukset ovat ajoittain niin taidokkaita, että edes prosessin noudattaminen ei auta. Tällöin psykologista turvallisuuden tunnetta tuo organisaatio kulttuuri, joka hyväksyy tämän jo etukäteen.

Osaaminen ja varmuus kulkevat käsi kädessä, kun osaaminen ruokkii varmuutta. Mahdollinen epävarmuus vähenee, kun validointiprosessi on yksiselitteisesti dokumentoitu ja ohjeiden noudattaminen on ehdotonta. Huijatuksi tulemisen vaikutus hioo prosessia ja erityisesti muokkaa lopullisesti asenteita. Kokemus opettaa, että prosessin olemassaolo on tärkeä ja sen noudattaminen ehdotonta. Aiemmin todettiin, että validoinnin tekee ihminen tehtävään sopivaa ohjelmistoa tai vastaavaa ei ole. Osaaminen antaa tarvittavan varmuuden tehtävän toteuttamiseen. Huijauksen uhrien epävarmuus on inhimillistä, ja esihenkilöön tukeutuminen on ymmärrettävää. Oppimalla huijauksesta ja parantamalla työvälineitä voidaan edes auttaa ja palauttaa työntekijän itseluottamus työn toteuttamista kohtaan.

Haastatelluissa yrityksissä oli myös kokemusta siitä, että asiakasta oli huijattu heidän yrityksensä nimissä. Muita havaintoja olivat erilaiset tietokalastelut kuten asiakkaiden laskutukseen liittyvä tietokalastelut. Kahdella toimialalla oli kohdattu myös toimialaan liittyviä huijausyrityksiä, muilla oli vain rahaliikenteeseen liittyviä kokemuksia. Kaikilla oli paljon kokemuksia huonoista huijausyrityksistä, niin amatöörimäisistä, että ne olivat heti havaittavissa tai jäivät kiinni jo roskapostifilttereihin. Vaikeimmiksi havaita oli koettu huijaukset, joissa käytyyn sähköpostikeskusteluun oli tullut mukaan uudesta tilinumerosta ilmoittaminen viestinvaihtojen edetessä eli keskustelun lomaan tai lopuksi.

Haastattelun lopussa kysyin, miten haastatteluun osallistuneet kokivat huijausten nykytilanteen ja ovatko miettineet mitä seuraavaksi on luvassa tällä rintamalla. Kukaan ei ollut havainnut muutosta uudenlaisiin teknisesti parempiin huijauksiin. Ajatus siitä, että esimerkiksi tekoäly olisi parantanut rikollisten työkaluja ei ollut vielä haastatelluissa yrityksissä käynyt toteen. Huijausviestit koetaan kyllä parempina kuin aikaisemmin eli viestien kanssa tarvitsee olla koko ajan tarkempi, mutta mitään eritysisiä uusi tapoja ei ollut tullut haastatelluilla vastaan. Huijausyritykset olivat haastattelujen mukaan lisääntyneet tasaisesti, mutta joukossa oli edelleen myös todella huonoja yrityksiä, jotka oli helppo tunnistaa huijausyrityksiksi. Näitä oli erityisesti toimitusjohtajahuijausten kategoriassa. Ylipäänsä kaikenlaisten kyberuhkien koettiin lisääntyneen ja useammassa yrityksessä oli suunnitelmissa kehittää työntekijöiden osaamista erilaisten uhkien tunnistamisessa. Yhdessä haastattelussa mainittu esimerkki oli organisaatiossa järjestetty kyberturvakampanja, jossa testattiin henkilökunnan

kykyä tunnistaa haitalliset viestit. Toisessa haastattelussa tuli esiin, että vaikka uudenlaisia huijausyrityksiä ei ollut vielä kohdattu, niihin oli jo varauduttu. Oli muun muassa päätetty, että myös tilanteessa, jossa voi tulla kyseeseen deepfake puhelu tai videopuhelu, toimitaan ohjeiden mukaan. Tässäkin tapauksessa varmistetaan tiedon aitous toisesta tai toisista lähteistä. Deepfake eli syväväärennös on videoväärennös, jossa elävä kuva tai ääni on väärennetty.

5 Pohdinta

Kuten luvussa 3. on kuvattu, tämän laadullisen tutkimuksen haastatteluaineisto analysoitiin Grounded Theory tutkimusmetodologiaan perustuvaa Gioia metodia hyödyntäen. Aineisto koodattiin metodin avulla haastattelujen lainauksista kohti käsitteellistettyä analyysin lopputulosta. Ensimmäisen tason käsitteet jaoteltiin kolmen pääaihepiirin alle;
1) tiedon validointiprosessiin vaikuttavat tekijät
2) huijausten rooli osana organisaation riskien hallintaa ja
3) huijauksen uhriksi joutumisen vaikutukset.

Kolmannessa luvussa osoitettiin, miten aihealueittain edettiin ensimmäisen tason konsepteista toisen tason teemojen kautta kolmeen yhdistettyyn dimensioon. Ensimmäisen aihealueen yhteydessä oli 27 ensimmäisen tason konseptia, joista muodostui kuusi toisen asteen teemaa. Toisen aihealueen alla oli 14 ensimmäisen tason konseptia, joista muodostui neljä toisen tason teemaa. Viimeisen, kolmannen aihealueen, yhteydessä oli 26 ensimmäisen tason konseptia, joista muodostui viisi toisen tason teemaa. Ensimmäisen tason käsitteitä oli yhteensä 67, jotka jakautuivat 15 toisen tason teemaan ja lopulta kolmeen dimensioon.

Tutkielman teoreettisen taustan rakenne hahmottui empiirisen tutkimusaineiston koodauksen aikana. Tutkimuskysymykset tarkentuivat tässä vaiheessa ja aineistosta kuoriutui kolme yhdistynyttä dimensiota. Luvussa 2. kuvattu teoreettinen tausta kietoutui tutkimusongelman ja dimensioiden ympärille. Tutkimuskirjallisuudesta nousseilla havainnoilla pyrittiin rikastuttamaan empiirisen aineiston antamaa sanomaa. Ensimmäinen teorialuku käsitteli tietoa käsitteenä, mitä tieto on. Toisessa luvussa tarkasteltiin erilaisia tietoprosesseja kuten SECI-malli. Kolmanneksi kuvattiin mitä tutkimuskirjallisuus sanoo tiedon suojaamisesta, ja tämän jälkeen tarkastelin riskien hallintaa tietojohtamisen kontekstissa mukaan lukien BEC-huijaukset. Viimeisenä luotiin vielä silmäys tietojohtamiseen yleisesti, ja virallisten tahojen ohjeisiin huijauksilta suojautumiseen. Tässä luvussa esitellään yhteenveto empirian peilaavuudesta tutkimuskirjallisuuteen.

5.1 Riskien hallinnan dimensio

Riskien hallinnan dimensiossa on oleellista organisaation toimintaympäristö ja sen tuomat räätälöidyt tarpeet. Yritykset miettivät omista lähtökohdistaan tason, jolla tiedon validointi tehdään ja tässä myös osa ottaa tietosia riskejä, kun asiaa on analysoitu riskin suuruuden perusteella. Yritykset ottavat maksamisessa hyvin poikkeuksellisesti riskejä, jos kyseessä oleva summa on pieni ja validointi ei ole onnistunut toivotulla tavalla, mutta mitään väärinkäytöksen viittaavaa ei ole tullut vastaan. Oman organisaation ja prosessien syvällinen tunteminen auttaa havaitsemaan haavoittumiselle alttiit kohdat ja mahdolliset puutteet. Toiseksi pitää tunnistaa uhat. Esimerkiksi millaisia uhkia tietopääomaan kohdistuu ja missä kohtaa tietoprosessia uhkia todennäköisimmin ilmenee. On tärkeää myös pyrkiä tunnistamaan niin sanottu vihollinen. Tämä auttaa varautumisessa ja parhaiden suojaustoimenpiteiden kohdistamisessa. Tässä tunnistus- ja varautumisprosessissa hyvä työkalu on riskiarviointi. (Whitman & Mattord 2018; Jennex & Durcikova 2020.)

Myös tietopääoman riskiarviointiprosessi kiinnittää huomion tiedon merkittävyyden tunnistamiselle ja sitä kautta mahdollisten uhkien tunnistamiselle. Tässä tutkimuksessa uutena tietona tutkittu tilitieto on suoraviivainen, eikä vaadi laajaa riskiarviointiprosessia, mutta sitä voi kuitenkin peilata tätä vasten. Tilitieto on ehdottomasti oleellinen tieto yritykselle, koska koko liiketoiminnan pyöritys pohjautuu toimivalle rahaliikenteelle. Myös siihen liittyvät uhat ovat tiedossa kuten tässä tutkimuksessa käsitelty BEC-huijaus sekä muut huijausmuodot. Vaikka uusia huijaustapoja voi ilmetä ja varmasti niitä tulee tulevaisuudessa lisää, kuitenkin uhka on selkeästi tiedostettavissa ja tiedon validointikeinoin kontrolloitavissa. Vaikka tässä tutkimuksessa keskitytään ulkoiseen uhkaan, niin yritykset olivat tunnistaneet myös sisäisiä uhkia ja luoneet toimintatapoja ja seurantaa myös näiden uhkien kontrolloimiseen. Huomasin, etsiessäni tutkimukselleni oleellista materiaalia, että tutkimuskirjallisuus keskittyy sisäisiin uhkiin laajasti. Mielestäni Iivonen et al. (2015, 5, kuvio 17) luoma tietopääoman riskiarviointiprosessi on toimiva malli uuden tiedon arviointiin yleisellä tasolla. Tilinumeron osalta sitä voi käyttää validointiprosessin kehittelyn tukena, yksinkertaistettuna. Riskiarviointiprosessin viimeisenä kohtana on esitelty uhkaympäristön jatkuva seuranta. Tämä on tärkeä elementti maksamisen maailmassa, jossa teknologiat kehittyvät nopeasti kuten johdannossa on kuvattu laajemmin. Toisen tason teemoja riskin hallinnan dimension yhteydessä

olivatkin terve epäluulo ja varmistaminen, turvallisempien kommunikointikanavien kokeilut sähköpostin sijalle, sisäinen valvonta ja toimintatapojen yksiselitteisyys. Nämä ovat kaikki tapoja, joilla haastatellut yritykset pyrkivät tarkkailemaan tiedon validointiprosessin toimivuutta, prosessiin osallistuvien toimintaa, tiedon välittymistä, ohjeiden noudattamista ja toimintaympäristön muutoksia. (Ilvonen et al. 2015.)

Aiempana on useasti todettu, että teknologia ei pysty suojaamaan organisaatiota väärältä tiedolta, vaan edelleen ihminen on avain asemassa. Vaikka tämä teknologia vs. ihminen on sijoitettuna laajemmin toisen dimension alle. On siinä kuitenkin myös riskien hallinnan kannalta oleellisia piirteitä. Kyberrikollisuus mielletään teknisenä asiana, mutta suojautuminen vaatii uhan ymmärtämistä. Työntekijöiden tulee ymmärtää jollain tasolla syyllisiä, erilaisia mahdollisia tekotapojen ja suojautumiskeinoja. Varautumisessa on vahvasti läsnä uhkien tunnistaminen. Myös uhrien kokemukset ovat tärkeää tietoa. Omat kokemukset nousivat myös vahvasti esiin haastatteluissa. Ymmärrys ja kokemus ovat voimakkaita työkaluja validointiprosessin rakentamiselle ja siihen liittyvän tietoprosessin jatkuvalle päivittämiselle kilpajuoksussa huijareiden kanssa käytävässä kilpajuoksussa. (Spicer 2019; Ilvonen et al. 2015.) Haastatteluissa kävi ilmi, että huijaukset ja erilaiset kyberuhat huomioidaan organisaatioiden rikiarvioinnissa kaikissa tutkituissa yrityksissä.

Vaikka ihminen on edelleen yllä kuvatusti avainasemassa, nähdään riskien hallinnassa koneoppimisen ja tekoälyn luovan mahdollisuuksia. Uusilla teknologiolla voidaan parantaa petosyritysten tunnistamista ja niiltä suojautumista. Tekoäly mahdollistaa myös tehokkaan automatiikkaa, jolla voidaan tunnistaa ja poistaa inhimillisiä virheitä sekä epäoleellista ja väärää tietoa. Uudet teknologiat tunnistavat tehokkaammin ihmisten välisiä yhteyksiä ja verkostoja. Näin voidaan huomata väärinkäytökset tehokkaammin. (Palgrave & Nature 2019; Leo, Suneel & Maddulet 2019; Tello 2023.) Haastatelluissa yrityksissä ei ollut käytössä tämän kaltaista teknologiaa vielä, vaan validointiprosessit perustuivat ihmisten tarkkaavaisuudelle ja luoduille prosesseille.

Psykologisten negatiivisten vaikutusten voimakkuus huijauksen uhriksi joutuneissa yrityksissä ja työntekijöissä yllättivät empiirisessä aineistossa eniten. Tämän reaktioiden voimakkuuden vuoksi nostin myös psykologiset vaikutukset riskien hallinnan dimension piiriin. Tilanteeseen varautuminen ja siitä selviämiseen on hyvä löytyä työkalut valmiiksi mietittynä. Riskien hallinnan dimensioon toisen tason teema psykologinen vaikutus sopii, koska se kytkeytyy suoraan siihen, että väärä tieto on päässyt prosessin ja kontrollin läpi, jos huijaus onnistuu. Se viittaa haastattelujen perusteella siihen, että huijaus on ollut erityisen taitava tai se voi tulevaisuudessa viitata siihen, että huijaus on täysin uudenlainen. Jos huijatuksi tuleminen saadaan kytkettyä kokonaan pois, vältytään negatiivisilta psykologisilta vaikutuksilta, taloudellisilta menetyksiltä ja mahdolliselta mainehaitalta. (Bhatt 2000; Intezari, Taskin & Pauleen 2017; Zieba & Durst 2019.)

5.2 Tiedon jakamisen dimensio

Tiedon jakamisen dimensio käsittää tiedon validointiprosessin kehittymisen ja jatkokehityksen. Validointiprosessit ovat empiirisen tutkimusaineiston mukaan kehittyneet työntekijöiden kokemusten kautta. Prosessi on hyvä esimerkki SECI-mallin (kuvio 14.) toteutumisesta käytännössä. Tiedon sosialisaatiossa hiljainen tieto välittyy työntekijöiden keskuudessa pääosin keskusteluissa, mutta myös muunlaisessa vuorovaikutuksessa kuten Teamsin chat. Seuraavaksi ulkoistamisessa hiljainen tieto muuttuu eksplisiittiseksi, kun siitä muokataan tulkittavaa kuten prosessikuvaus, toimintasäännöt tai ohjeet. Tämä vaihe laajentaa tiedon käytettävyyttä isommalle joukolle. Tämä taas vuorostaan mahdollistaa uuden tiedon luomisen. Yhdistämisessä edellisessä vaiheessa eksplisiittiseksi muunnetusta tiedosta voi koota suurempia kokonaisuuksia yhdistämällä uutta tietoa vanhaan tietoon tai muihin tietoihin. Vanhaa tieto voisi olla aiempi validointiprosessi, jota uudistetaan uuden tiedon valossa. Muu tieto taas voisi olla viranomaisten antama ohjeistus kyberuhiltasuojautumiseen tai aihetta käsittelevä uutinen. Tiedon käytettävyys kasvaa prosessin edetessä. Viimeisenä SECI-mallissa tulee sisäistäminen. Eksplisiittinen tieto on nyt saavuttanut tason, jossa se on sisäistetty ja ymmärretty. Tiedosta tulee jälleen henkilökohtaista ymmärrystä ja muuttuu yksilön hiljaiseksi tiedoksi. Tämän jälkeen tieto voi jälleen jatkaa matkaa uudelle kierrokselle, eli SECI-mallin spiraaliin. Tutkimuksen tiedot mukailivat hyvin SECI-mallin kuvausta, kun haastateltavat kuvailivat, miten huijaustapauksista keskustellaan ja tieto liikkuu organisaatiossa. Näin

hiljainen tieto luo organisaatiolle uutta tietoa, joka rikastuu matkan varrella koko ajan eläen siirtyen vuorovaikutuksesta kirjallisten ohjeiden muotoon. Yritykset pystyvät hyödyntämään yksilöiden kokemuksia ja tiedon siirtymistä työntekijöiden keskuudessa. Työntekijät oppivat toisiltaan jakamalla tietoa virheistä, onnistumisista sekä kokemuksista, myös organisaation ulkopuolelta tullutta tietoa kuten uutiset jaetaan työyhteisössä.

Tiedon jakaminen on yksi peruselementeistä tietoprosessien kuvauksissa. Tyypillinen tietoprosessi etenee tiedon luonnista, tiedon säilyttämiseen, jakamiseen ja lopulta käyttöön eli hyödyntämiseen (Heisig 2009; Alavi & Leidner 2001; Bhatt 2001.) Tässä ilmenee mielestäni tutkimusaukko, jonka havaitsin opintojen varrella. Tietoprosessit eivät huomioi mielestäni riittävästi tiedon validointia. Alla olevaan kuvioon 20. olen hahmotellut tietoprosessin, joka kuvaa tietoprosessin uuden tiedon validoinnin ympärille.

Kuvio 20. Uuden tiedon validointiprosessi

Koen, että validoinnilla tulisi olla oma paikkansa tietoprosessissa kuvion 19. kaltaisesti. Kuten jo aiemmin totesin organisaation toiminnan kannalta, on tärkeää, että väärä tieto tunnistetaan hyvissä ajoin ennen sen päätymistä hyödynnettäväksi. Tämä tarve tuli hyvin konkreettisesti esiin haastatteluissa. Jotta organisaatiossa voidaan varmistua tilinumerotietoa tallennettaessa, että muutos on todellinen, validi ja aito, on kyettävä luomaan vastaanotetun datan ja käyttöön otettavan tiedon välille pitävä validointiprosessi. Tiedon validointiin oli kaikissa yrityksissä rakennettu prosessit ja selkeät ohjeet, joita kehitettiin jatkuvasti. Käytännössä empiirisen aineiston mukaan informaation validointi aloitti prosessin, mutta tietoprosessien tutkimuskirjallisuudessa validointia ei korostettu enkä löytänyt yhtään tukimusta, jossa validointi olisi ollut tutkimuksen kohteena. Tietojohtamisen kirjallisuudessa uudempana ilmiönä nähdään organisaation tiedon ja tietoprosessien suojaaminen ja turvaaminen

kasvavaa huomiota. (Goode & Lacey 2022; Murray & Durcikova 2014; Jonnex & Zyngier 2007.)

Yleistäen tietojohtamisen kirjallisuudessa riskinä pidetään tiedon menettämistä esimerkiksi eläköitymisen ja työntekijän menettämisen yhteydessä. Muita kuvattuja tietoriskejä ovat tietoon liittyvien mahdollisuuksia hukkaaminen, puutteellinen tiedon tallentaminen ja epäonnistunut tiedon hyödyntäminen (Ilvonen et al. 2018; Jennex & Zyngier 2007.) Ulkoisina riskeinä pidetään tiedon joutumista vääriin käsiin tai, että tietoa jaetaan liikaa niin, että mahdollinen hyöty menetetään (Manhart &Thalmann (2015). Tietojohtamisen kirjallisuus tunnistaa, että luodut mallit eivät yleensä tunnista virheiden ehkäisemisen tärkeyttä. Ongelmien taustalla on kuitenkin usein tietovirhe, jota ei tunnistettu. (Sveen, Rich & Jager 2007.) Jennex ja Zyngier (2007) kuvaavat, että tietojohtamisen näkökulmasta turvallisuusnäkökulmat nähdään tutkimuksissa välillä eräänlaisina esteinä. Nähdään, että turvallisuuden korostaminen on haitta tai este tiedon jakamiselle. Organisaation tietopääomaa pidetään yleisesti tärkeänä, joten monet tutkijat pitävät tärkeyden ja oleellisuuden kautta selviönä, että tiedon ja tietoprosessien turvallisuus on sisäänrakennettu fakta. Tämä ajatusmalli voi olla syy miksi tutkimukset eivät keskity tiedon validointiin, jota on tässä pro gradu tutkimuksessa pohdittu. (Jennex ja Zyngier 2007.) Tämä oli mielenkiintoinen näkemys, joka selittää validoinnin tärkeyden eräänlaisen puuttumisen kirjallisuudesta. Pidän tätä kuitenkin hivenen outona, koska niin perusteellisesti ja monenlaisia tutkimuksia toteutetaan, että tätä aihepiiriä vain sivutaan harvakseltaan.

Kuten tämän pro gradu tutkimuksen aineisto osoittaa, käytännössä uuden tiedon arviointia maksamisen kontekstissa pidetään erittäin tärkeänä. Prosessin kehitystyö ei koskaan pysähdy, koska ulkoiset tietosyötteet kuten uudet huijausyritykset ja kyberuhkien uutisointi pitävät asiaa esillä päivittäin. Tiedon ja kokemusten jakaminen sekä toisilta oppiminen työyhteisön vuorovaikutustilanteissa lisäävät hallinnantunnetta. Yhteisöllisyydentunne ja organisaatio kulttuuri, jossa hyväksytään myös inhimilliset virheet, auttaa negatiivisista psykologisista vaikutuksista toipumisessa. Rikolliset osaavat ajoittain olla niin taitavia, että edes ohjeet ja prosessin noudattaminen ei pelasta tilanteessa. Organisaatio kulttuuri, jossa on juurrutettuna psykologinen turvallisuuden tunne, auttaa työntekijää ja työyhteisöä toipumisessa.

Haastatelluissa yrityksissä tiedon validointiprosessien ja ohjeiden kehityksessä huijauksilta suojautumisessa työyhteisön vuorovaikutus toimi promoottorina kehitykselle. Tiedon jakamista kannattaakin organisaatioissa stimuloida antamalla sille aikaa ja tapoja toteutua. Hyvä tavoite on juurruttaa tiedonjakaminen tavanomaiseksi osaksi jokapäiväistä toimintaa. Psykologisesti turvalliseen ja inspiroivaan organisaatiokulttuurin panostaminen johdon toimesta luo hyvän maaperän tiedonjakamiselle. (Akhavan & Zahedi 2014.)

Tietojohtamisen kirjallisuudessa kuvattu organisaation on kyky luoda uusia ideoita ja ratkaisuja, tuli esiin haastatteluissa kokemuksen, tiedon jakamisen ja niiden kautta oppimisen tuomana hallinnantunteena. Aina ei ole tarvetta luoda uutta, vaan kyseessä voi olla vanhan uudelleen soveltamista tai painopisteen vaihtamista. Empiirisestä aineistosta löytyi myös käytännön tilanteista tarpeen ja keinot arvioida käytössä olevaa tietoa ja osaamista. Sekä validointiprosesseista käytänteet uuden tiedon hyväksymiselle hyödynnettäväksi. Tietoa myös muunneltiin esittävämpään muotoon kuten ohjeiksi ja säännöiksi. Jonka jälkeen sen jakaminen helpottui esimerkiksi konsernin eri yhtiöihin. Huijauskokemusten ja validointiprosessin ympärille kietoutuva tietotaito ja kokemukset päätyivät hyödynnettäväksi yritysten prosesseihin. Yhtymä kohta oli havaittavissa käytännön ja teorian välillä, kun tietojohtamisen kiertokulku pitää yllä ydinosaamista oppimalla, reflektoimalla, poisoppimalla ja uudelleen oppimalla. (Bhatt 2001.)

5.3 Osaamisen tuoman varmuuden dimensio

Osaamisen tuoman varmuuden dimensio on kolmas ja viimeinen empiirisen aineiston pohjalta koodauksen kautta analyysistä yhdistynyt dimensio. Osaaminen ja varmuus kulkevat käsi kädessä sekä yksilöissä, että työyhteisössä. Osaaminen ruokkii varmuutta. Varmuus poistaa epävarmuutta. Varmuus myös poistaa tai lieventää negatiivisten psykologisten tunteiden vaikutuksia huijauksen uhreiksi joutuneilta. Empiirinen aineisto osoitti, että hyvin dokumentoitu ja ohjeistettu yksiselitteinen validointiprosessi tukee ja poistaa epävarmuutta. Huijauksen uhriksi joutuminen on osoittautunut yrityksille tehokkaaksi oppikouluksi. Huijatuksi joutumisen vaikutus on hionut prosessia ja erityishuomiona muokannut lopullisesti asenteita ja ymmärrystä.

Hyvä keino välttyä huijauksen uhriksi joutumiselta on kouluttaminen, ajantasainen tiedottaminen ja prosessien kontrollointi. Tietolähteen luotettavuuden arviointi on taitona avainasemassa huijauksilta suojautumisessa. Perusteellisesti suunnitellut prosessit, koulutus ja kokemus mahdollistavat parhaat työkalut epäilyttävien tilanteiden tunnistamiseen. Tiedon jakaminen, joka käsiteltiin edellisessä luvussa, on myös tärkeässä roolissa. Tiedon jakaminen edesauttaa myös koko organisaatiotason oppimista. (Bhatt 2000; Daghfous, Belkhodja & Angell 2013; Jennex et al. 2022.) (Wittman & Mattord 2018.) Varsinaista säännönmukaista koulutusta huijaamisiin liittyen tuli vastaan vain kahdessa haastattelussa, mutta toisilta oppiminen oli yhteistä kaikille. Myös ulkopuolisten tahojen ohjeita huomioitiin jonkun verran, vaikka selkeästi päärooliss olivat omat kokemukset peilattuna organisaation toimintatapoihin ja riskiarvioon. Viranomaisten ja vastaavien tahojen ohjeita huijauksilta suojautumisen ei aktiivisesti seurannut kukaan haastatelluista. Huijaamiseen ja kyberuhkiin liittyvää uutisointia kyllä seurattiin. Yksi haastateltu seurasi lisäksi Traficomin cybersecurity forecastiä. Lähtökohtana omiin toimintatapoihin pidettiin omaa toimintaa, sen luonteenpiirteitä, prosesseja ja tarpeita. Yksi haastateltu toi myös esiin tilintarkastajalta tulevan palautteen maksamisen riskeihin liittyen. Näitä on kyseisessä yrityksessä huomioitu ja tehty muutoksia palautteen mukaan.

Aiemmin todettiin, että validoinnin tekee ihminen tehtävään sopivaa ohjelmistoa tai vastaavaa ei ole. Osaaminen antaa tarvittavan varmuuden tehtävän toteuttamiseen. Huijauksen uhrien epävarmuus on hyvin inhimillistä, ja esihenkilöön tukeutuminen on lisääntynyt tilanteiden jälkeen huomattavasti. Oppimalla huijauksista voidaan edesauttaa ja palauttaa työntekijän itseluottamus työtehtävää kohtaan. Tutkimuskirjallisuudesta nousi esiin huomion arvoinen seikka. Koska tämä pro gradu tutkimus kiinnittää erityisitä huomiota riskeihin ja suojautumiseen on käytännössä kuitenkin pakko löytää tasapaino käytettävyyden ja kontrollin välillä. Tähän ajatukseen peilaten on mitoitettava tiedon oikeellisuuden validointi ja prosessin tehokkuus yhteen sopiviksi. Balanssi tule löytää riskiarvioinnin kautta huomioiden mahdolliset negatiiviset kokemukset työyhteisössä. Kokonaisuutta tarkasteltaessa tarkka analyysi uuden tiedon hyväksymisvaiheessa poistaa riskejä sekä viattomien virheiden että tahallisten huijausten aiheuttamalta haitalta ja taloudellisilta menetyksiltä pitkällä aikavälillä. Balanssi nimissä validointiprosessi ei saa kuitenkaan olla liian raskas. (Jennex & Durcikova 2014.)

Osaamisen tuoma varmuus dimensio voidaan myös liittää mahdollistaja näkemyksen (kuvio 6.). Se kuvaa miten toimivaan tietojohtamiseen vaikuttavat organisaation mahdollistajat. Mahdollistajia ovat organisaation kulttuuri, organisaatio ja sen sisäiset roolit, yrityksen johtajuus ja strategiat, työntekijöiden taidot ja motivaatio, organisaation kontrolliympäristö, toimintojen ja suorituksen mittarit sekä millaista teknologiaa on käytössä. Onnistumisen nähdään olevan kiinni kaikista näistä mahdollistajaosa-alueista. (Heisig 2009.) Mahdollistajat, oikein painotettuna, tarjoavat organisaation kulttuurin ja johtajuuden, joka tukee oppimista ja taitojen kehittymistä. Tuo varmuutta epävarmuuden tilalle sekä oikein mitoitettua kontrollia, olematta kyttäämistä, joka tukee validointiprosessin yksiselitteisyyttä ja ohjeiden noudattamisen asenteita. Kuten on jo monesti todettu, kokemukset opettavat, mutta myös mittarit tuottavat myös kehittymistä ja oppimista tukevaa tietoa ja konkretisoivat edistystä ja näyttävät parannuskohteet. Vaikka ihmisellä on edelleen validoinnissa päärooli, nähdään jo nyt paljon koneoppimisen ja tekoälyn luomia mahdollisuuksilla. Niiden avulla voidaan parantaa petosyritysten havaitsemista ja suojautumista. Tekoäly mahdollistaa tehokkaampaa automatiikkaa, joka tunnistaa ja poistaa inhimillisiä virheitä ja väärää tietoa. Uudet teknologiat tunnistavat tehokkaasti ihmisten välisiä yhteyksiä. Tämä auttaa tunnistamaan rikollista toimintaa aivan uudella tavalla. (Palgrave & Nature 2019.)

Kun organisaatio puhaltaa yhteen hiileen epävarmuuden tunne hälvenee. Kun tietosyötteet organisaation ulkopuolelta ovat epämääräisiä tai uhkaavia, organisaation yhteinen merkityksellisyyden tunne ja päämäärät vähentävät epävarmuuden tunnetta. Merkityksellisyyden ilmapiiri ei ole muuttumaton. Se muuttuu ympäristön muutosten mukaan. Tämä muutosliike on tärkeä mittari organisaation tavoitteiden uudistumiselle. Liikkeessä mukana pysyminen varmistaa, että tavoitteet ovat oikean suuntaisia ja saavutetaan muuttuvassakin ympäristössä. Muutosliikkeessä organisaatio hioo kyvykkyyksiään sekä kehittää niitä ja luo uutta osaamista. Prosessin paljastaa myös puutteet osaamisessa ja saatavilla olevassa tiedossa. Kun nämä puutteet tunnistetaan herätteenä ulkoiseen impulssiin organisaation jäsenet lähtevät korjaamaan näitä tunnistettuja puutteita. (Choo 2001; Laihonen et al.2013.) Tästä liikkeestä voi käyttää esimerkkinä uusia huijausyrityksiä ja kyberuhkien muuttuvaa maailmaa. Sen asettamiin haasteihin vastaamalla haastatellut yritykset ovat onnistuneet rakentamaan riittävät ja oikein mitoitetut suojakertoimet ulkoisia uhkia vastaan.

5.4 Pohdintoja julkisista ohjeista huijauksien ennaltaehkäisyyn

Virallisten tahojen ohjeiden vähäinen hyödyntäminen kiinnitti huomiota. Kuitenkin validointiprosesseissa oli paljon samoja elementtejä kuin ohjeissa, joita on kuvattu luvussa 2.6. Oli myös mielenkiintoista huomata, että validointiprosessit olivat eri alojen yrityksissä muotoutuneet hyvin keskenään samankaltaisiksi. Suurin ero ulkopuolisten tahojen ohjeiden ja käytännössä toteutettavien toimenpiteiden välillä oli suhtautuminen sosiaalisen median käytön riskitekijöihin. Virallisten tahojen ohjeissa, kiinnitettiin paljon huomiota näihin seikkoihin. Näkökulmana oli, että organisaation ei itse kannata asettaa itseään haavoittuvaan asemaan liiallisella tiedonjakamisella sosiaalisenmedian kanavissa. Näissä ohjeissa ohjattiin erityisesti huomioimaan mitä organisaatio kertoo itsestään nettisivuilla, sosiaalisenmedian kanavissa tai miten työntekijöitä ohjeistetaan kertomaan roolistaan ja työstään omilla sosiaalisenmedian kanavillaan. Ohjeissa ei ollut keskiössä liikesalaisuudet, vaan ennemminkin kuinka uskottavan tarinan ulkopuolinen pystyy keräämillään tiedoilla rakentamaan huijatakseen kohdeorganisaatiota. Esimerkkejä mietittävistä seikoista voisivat olla, kuinka laajasti kuvataan työntekijöiden välistä hierarkiaa, kuinka laajasti kuvataan toimenkuvia ja kerrotaanko siitä, että kyseessä on uusi työpaikka tai vastaavasti siitä, että on palkattu uusi työntekijä.

Tätä luvussa 2.6. kuvatuissa ohjeissa esiin noussutta varovaisuutta siitä, kuinka paljon jaetaan tietoa rooleista, hierarkiasta ja ylipäänsä yksityiskohtia, joista pystyy rakentamaan todentuntuisen huijauksen, ei huomioitu haastateltujen organisaatioiden ohjeissa. Tutkimuksen kohdeyrityksiltä löytyi tietoturvasertifikaatteja tai vastaavan kaltaisia ohjeita, jotka usein allekirjoitetaan työhöntulotilanteessa. Näissä määritellään liikesalaistentietojen käyttö ja käsittely. Joissakin yrityksissä oli lisäksi sosiaalisen median käyttöön annettuja erillisiä ohjeita tai ne li sisällytetty employee code of conduct ohjeisiin (työntekijöiden eettiset käytännesäännöt). Näissä kaikissa ohjeissa pääpaino on liiketoiminnan kannalta salassa pidettäviksi luokiteltujen tietojen käsittely, kuvien käyttö ja sisäiset väärinkäytökset. Tästä aiheesta nousi useissa haastatteluissa sivujuoni varovaisuuden ja toivotun näkyvyyden välillä. Sosiaalisessa mediassa ylpeänä työtään ja työnantajaansa esittelevä henkilö, kun on mitä mainiointa mainosta yritykselle. Yhdessä haastatelluista yrityksistä oli kokemusta siitä, että uusi työntekijä oli heti alkumetreillä joutunut huijausyrityksen kohteeksi. Tämä tilanne oli

opettanut, että aihe on hyvä nostaa perehdytyksessä heti esiin. Yritysten nettisivuilla oli pääasiassa vain yleistietoa. Sosiaalisen median käytön osalta pohdin myös ristiriitaa ohjeiden ja sen välillä, että työnantajat ennemminkin rohkaisevat kertomaan työstä esimerkiksi Linkedin:ssa näkyvyyden, mielikuvan ja mainonnan näkökulmasta. Mielenkiintoista miettiä mihin raja tulisi vetää näkyvyyden ja riskin näkökulmista. Jälleen yksi aihe, jota voi pohtia riskiarvioinnin kautta, kuinka isosta rikistä voi pahimmillaan olla tai kuinka suuri näkyvyys saavutetaan ja miten sitä voi hyödyntää.

Uhkaympäristössä, jossa uhattuna ovat organisaatio, työntekijöitä ja asiakkaat, korostuu tietojohtamisen prosessien turvallisuus ja prosessia pyörittävien osaaminen. Rikollisille ei kannata tehdä elämää helpoksi edesauttamalla rikollista toimintaa. Puutteet työntekijöiden osaamisessa ja riskien ymmärtämisessä, heikkoudet tietoprosesseissa, tiedonkulussa tai päätöksenteossa, ovat kaikki korjattavissa olevia elementtejä. Tätä on kuolleiden kulmien paikkaaminen. Sekä kirjallisuus, että empiria osoittavat, että rikollisille ei voi jättää tilaa. Tämä on asiantila, jota muiden muassa BEC-huijarit osaavat käyttää hyväkseen. Mikäli sähköpostiin luotetaan varauksetta ja validointiprosessia ei toteuteta huolella, on yritys täysin huijareiden armoilla. (Leo ey al. 2019; Goode & Lacey 2022.)

5.5 Pohdintoja tulevaisuudesta

Maksamisen tulevaisuutta miettiessä korostuvat kolme seikkaa. Kulloinkin vaikuttavalla geopoliittisella tilanneella on mittavia maailman laajuisia vaikutuksia. Viime vuosikymmeninä trendinä on ollut globalisaatioon, joka on tuonut myös maksamiseen globaaleja uudistuksia. Kiristyneissä geopoliittisissa tilanteissa yhteistyö saattaa toki lisääntyä joidenkin tahojen välillä, mutta epävakaus lisää kansallista huoltovalmiusajattelua myös rahaliikenteen näkökulmasta. Erikoistilanteisiin globaalissa maksuliikkeessä kannatta varautua, miettimällä vaihtoehtoisia keinoja rahaliikenteen toteuttamiselle. Varajärjestelmiä kannattaa testata säännöllisesti ja miettiä turvalliset toimintatavat erikoistilanteisiin esimerkiksi järjestelmien käyttöoikeuksien ja päätöksenteon näkökulmista. Ennakointia voi toteuttaa laajemminkin esimerkiksi miettimällä geopolitiikan rikistekijöitä ja analysoimalla missä päin maailmaa erikoistilanteet tulevat todennäköisimmin vastaan ja millaisia ne voivat olla. (Botta & Nadeau 2022.)

Toisena vauhdilla kehittyvät teknologiat kuten koneoppiminen ja tekoäly eivät syrjäytä ihmistä kokonaan, mutta ne tulevat muuttamaan työskentelytapoja. Vaikka tämän pro gradu tutkimuksen yrityksissä ei vielä validoida tietoa teknologian avulla, tämä tulee muuttumaan tulevaisuudessa. Uudet työkalut tulevat auttamaan petosyritysten havaitsemisessa ja suojautumisessa. Uudistuvat työkalut tulevat kattamaan suojautumiskeinoja järjestelmille, tietopääomalle ja asiakkaiden tiedoille. Uusien teknologioiden tehokkuus mahdollistaa nopean operoinnin valtavalle määrälle dataa. Tällöin ihmisten ja organisaatioiden välisiä yhteyksiä ja verkostoja on helpompi tunnistaa. Tämä auttaa tunnistamaan rikollista toimintaa esimerkiksi entistä tehokkaammin. Teknologian kehitys vaikuttaa maksamisen tulevaisuuteen. Finanssialan toimijat modernisoivat ydinjärjestelmiään mahdollistamaan reaaliaikaisuuden, open-banking vaateet ja pilviteknologian hyödyntämisen. (Palgrave & Nature 2019; Botta & Nadeau 2022.)

Viimeisenä mainitsen vastuullisuuden tulevaisuuden muokkaajana. ESG eli vastuu ympäristöstä (environmental), ihmisistä (social) kuten työntekijöistä ja asiakkaista sekä hallinnosta (governance) kuten lain noudattamisesta ovat tärkeässä roolissa myös maksamisessa. Rahalaitoksilla on tärkeä ja vastuullinen rooli osana maksujärjestelmää. Toimijat mahdollistavat maksamisen ja pyrkivät suojaamaan omalta osaltaan rahaliikennettä rahanpesulta ja petoksilta asiakkaiden hyväksi. (Botta & Nadeau 2022.)

Nämä kaikki yllä mainitut elementit löytyvät myös tietojohtamisen taustatrendeistä. Tietojohtamisen taustatrendejä ovat muun muassa informaation määrän lisääntyminen, teknologian kehitys, globaalit markkinat, työn digitalisaatio, kestävyys ja muutostahdin kiihtyminen (Kianto 2021).

6 Johtopäätökset

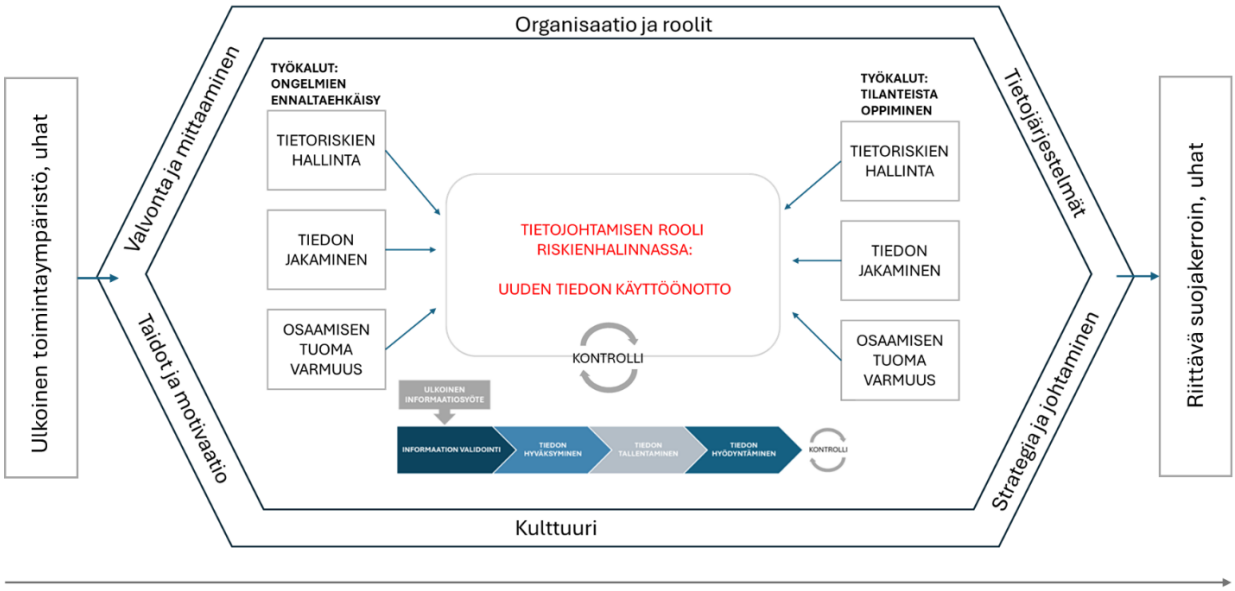
Maailma muuttuu nopeasti ja tiedosta on tullut tärkein resurssi muutoksen hallinnassa. Tiedon avulla voidaan sekä parantaa että pahentaa maailmantilaa. Virheellinen tieto korruptoi, kun taas aito ja hyödynnettävissä oleva tieto on mahdollistaja. Tiedon monimuotoisuus on myös tietoprosesseja rikastuttava tekijä tiedon luomisen, jakamisen ja hyödyntämisen näkökulmasta. Tiedon oikeellisuus ja totuudenmukaisuus luovat vakaan pohjan tietoprosseille ja päätöksenteolle. Luvussa 1.1.1 asetin pro gradu -tutkimukselle päätutkimuskysymyksen ja kolme alatutkimuskysymystä. Kolmeen alatutkimuskysymykseen, *”Miten uuden tiedon validoimiseen luotuun tietoprosessiin on organisaatiossa päädytty?”, ”Kuinka suurena riskinä huijaukset nähdään?” ja ”Millaisia vaikutuksia huijauksilla on organisaatiolle ja miten niistä selvitään?”*, vastattiin luvussa neljä. Tässä luvussa vastataan päätutkimuskysymykseen:

”Millainen on tietojohtamisen rooli riskienhallinnassa, kun organisaatiossa pyritään suojautumaan uuden tiedon käyttämiseen liittyviltä riskeiltä?”

6.1 Tietojohtamisen rooli uuden tiedon hyödyntämisessä riskienhallinnan näkökulmasta

Empiirinen tutkimusaineisto analysoitiin mukaillen Grounded Theoryn pohjalta syntynyttä, Gioian metodia. Näin varmistettiin analyysin kurinalaisuus suhteessa aineistoon, vaikka tässä laadullisessa tutkimuksessa oli mukana myös luovuutta, teoreettista herkkyyttä ja omaa kokemusta rahaliikenteestä. Tutkimuksessa onnistuttiin luomaan viitekehys, joka vastaa tutkimuskysymykseen ja jota voi hyödyntää uuden tiedon käyttöönotossa. Gioian metodille nimensä antanut tutkija Gioia koki, että tarvittiin tutkimustapa, jossa lähdetään liikkeelle tutkittavien kokemuksista. Tätä ajatusta seuraamalla valitsin haastateltaviksi henkilöt, joilla oli pitkä kokemus alaltaan, työstään maksamisenprosessien parissa ja niihin liittyvässä päätöksenteossa. Halusin tutkia asiantuntijoiden kokemuksia tutkittavasta ilmiöstä. Itse, tutkijana, raportoin aineiston analyysin ja etsin siitä ulottuvuuksia ja niiden kautta ilmiötä selittäviä dimensioita ja tarkastelin näitä löydöksiä teoreettisessa taustassa esitettyihin tietojohtamisen teorioihin peilaten. Seuraavassa kuviossa 21. on koottuna tutkimuksen lopputuloksena

syntynyt viitekehys tietojohtamisen roolista uuden tiedon hyödyntämisessä riskienhallinnan näkökulmasta.



Kuvio 21. Tietojohtamisen rooli uuden tiedon hyödyntämisessä riskienhallinnan näkökulmasta

Viitekehys rakentuu tietojohtamiseen vaikuttavien mahdollistajien raamin sisään (Heisig 2009, 15). Mahdollistajina toimivat organisaation kulttuuri, organisaatio ja sen sisäiset roolit, yrityksen strategiat ja johtajuus, työntekijöiden taidot ja motivaatio, organisaation kontrolliympäristö, toimintojen ja suorituksen mittarit ja valvonta sekä käytössä olevat tietojärjestelmät. Nimensä mukaan mahdollistajat mahdollistavat asioita. Niissä piilee epäonnistumisen ja onnistumisen avaimet. Onnistuessaan organisaation mahdollistajat luovat organisaatioon kulttuurin ja johtajuuden, jotka tukevat oppimista ja tietotaidon kehittymistä. Johtajuus, taidot ja motivaatio ruokkivat varmuutta epävarmuuden sijaan. Oikein mitoitettua kontrolliympäristöä, joka ei tarkoita kyttäämisen kaltaista epäluottamusta, tukee validointiprosessin yksiselitteisyyttä ja ohjeiden noudattamisen asenteita. Ohjeita ja dokumentoitua prosessia ei nähdä epäluottamuksena, vaan ne tuovat hallinnantunnetta stressaaviin ja yllättäviin tilanteisiin. Mittarit ja tavoitteet tukevat omalta osaltaan kehitystä, konkretisoivat edistystä ja paljastavat heikot kohdat. Kuten aiemmin on todettu heikkojen kohtien tunnistaminen kuten myös uhkien tunnistaminen ovat tärkeitä elementtejä riskien arvioinnissa.

Organisaation mahdollistajien raamin ulkopuolella on organisaation ulkopuolinen ympäristö, josta ulkoiset tietosyötteet tulevat (kuviossa vasemmassa reunassa). Tässä viitekehyksessä ulkoinen tietosyöte on potentiaalinen uhka, kunnes toisin todistetaan. Maksamisen ympäristössä toisen tason teemoista esiin nousseet terve epäluulo ja varmistamisen tarve, ovat tarpeellisia suojakeinoja. Tässä tutkimuksessa ulkoisia uhkia edustivat BEC-huijaukset. Organisaation mahdollistajien raamin ulkopuolella oikealla, kuvataan organisaatioon kokemuksen ja oppimisen kautta syntynyttä suojakerrointa. Tarvittavan suojakertoimen lisäksi viitekehys ottaa huomioon, että kerroksen on oltava riittävä, mutta se ei saa olla joustamaton kivimuuri. Mitoittamalla validointiprosessin räätälöidysti omiin tarpeisiin sopivaksi ja huomioimalla riskianalyysin (kuvio 8, s 23) avulla riittävän tason, onnistuu organisaatio suojautumaan riittävällä tasolla rikeihin nähden. Tärkein kriteeri on tiedon merkityksellisyys organisaatiolle, sekä mahdollisten riskien suuruus. BEC-huijauksen kohdalla merkittävimmät riskitekijät ovat taloudellinen menetys, negatiivinen psykologinen vaikutus yksilöön sekä laajemmin työyhteisöön sekä mahdollinen mainehaitta. Riittävä suojakerroin uhkia vastaan on viitekehyksessä oikealla kuvaamassa miten mahdollistajien raamin sisällä tapahtuvat prosessit riskien hallinta, tiedon jakaminen ja osaamisen tuoma varmuus varmistavat suojakertoimen muodostumisen. Toisin sanoen tiedonvalidointiprosessi estää lähtevän maksun toteutuksen huijaustilanteessa.

Pro gradu tutkimuksen empiirisen aineiston analyysin koodauksen tuloksena yhdistyi kolme dimensiota: riskien hallinta, tiedon jakaminen ja osaamisen tuoma varmuus. Dimensioiden rakentumineen on kuvattu yksityiskohtaisemmin luvussa 3. Tutkimustulokset on kuvattu luvussa 4. Viitekehyksessä dimensiot ovat työkaluja, joilla vasemmalla ennalta ehkäistään ongelmia ja oikealla niiden avulla opitaan kokemuksista ja virheistä. *Tietoriskien hallinta dimension* työkaluilla ennaltaehkäistään ongelmia esimerkiksi tunnistamalla uhkia, missä kohtaa tietoprosessia ne luultavimmin ilmenevät ja varautumalla. Tilanteesta oppimisen työkaluja ovat esimerkiksi käytännönkokemukset, joiden kautta ymmärrys kasvaa. Ymmärrys ja psykologiset vaikutukset luovat pohjan riskienhallinnan kehittämiselle. *Tiedon jakamisen dimension* työkaluilla ennalta ehkäistään ongelmia jakaen tietoa vuorovaikutuksessa toisten kanssa SECI-mallin (kuvio 5.) mukaisesti. Tämä hiljaisentiedon muuttuminen eksplisiittiseksi tiedoksi, joka siten jakautuu laajemmalle joukolle ja muuntautuu uudeksi tiedoksi,

joka mahdollistaa validointiprosessin kehittymisen. Tilanteista oppimista tiedon jakamisen dimensio tukee luoden jatkokehityksen aihioita validointiprosessille. Kokemukset ovat tärkeitä rakennuspalikoita prosessin kehittämiselle, ja niitä ei pääse hyödyntämään ilman tiedon jakamisesta. *Osaamisen tuoman varmuuden* työkaluilla ongelmia ennaltaehkäistään kouluttautumalla, seuraamalla ajankohtaista uutisointia tai viranomaisten kuten Traficom tiedotuksia, kontrolloimalla prosesseja ja noudattamalla ohjeita. Tilanteista oppimiseen osaamisen tuoma varmuus tuo huijauksista oppimisen. Tutkimus osoitti, että huijatuksi tuleminen on erityinen oppikoulu, niin hyvässä kuin pahassa. Se hioo prosessin yksityiskohdat ja vaikuttaa validointiprosessia vähätteleviin asenteisiin muuttaen niitä asian tärkeyden ja oleellisuuden ymmärtämiskesi. Tämä taas ohjaa noudattamaan ohjeita paremmin.

Alimmaisena mahdollistaja kehyksen sisällä kuviossa 21. on kuvattuna uuden tiedon validointiprosessi, joka on alla kuviossa 22. suurennettuna.

Kuvio 22. Uuden tiedon validointiprosessin, suurennos

Uuden tiedon validointiprosessissa tieto valitaan käytettäväksi osana organisaation tietoprosesseja ja siitä tulee osa organisaation tietopääomaa tai se hylätään. Validointiprosessin tarve tuli hyvin konkreettisesti esiin haastatteluissa. Validointiprosessi sijaitsee viitekehyksen keskiössä. Sen syntyyn, kehitykseen ja sen mahdollistamaan riskien minimointiin vaikuttavat kaikki muut viitekehyksen elementit edellä kuvatuilla tavoilla. Jotta organisaatiossa voidaan varmistua uutta tilinumeroa tallennettaessa, että muutos on validi ja aito, on luotava vastaanotetun datan ja käyttöön otettavan tiedon välille mahdollisimman aukoton validointiprosessi. Tiedon validointiin oli kaikissa haastatelluissa yrityksissä rakennettu prosessit ja laadittu

selkeät toimintaohjeet. Käytännössä empiirisen aineiston mukaan uuden tiedon validointi aloitti prosessin, mutta tietoprosessien tutkimuskirjallisuudessa validoinnin korostaminen puuttui.

Pitkin tutkimuksen etenemistä minulla vahvistui näkemys selkeästä tutkimusaukosta. Uuden tiedon validoinnista oli vaikea löytää aineistoa. Minua kiinnostivat teemat kuten miten tiedon oikeellisuus ja todenperäisyys varmistetaan tai ylipäänsä huomioidaan riskitekijänä. En löytänyt yhtäkään tutkimusta, jossa tämä olisi ollut tutkittavana ilmiönä. Tarkastellessani BEC-huijausta ja sen vaikutuksia, juuri tiedon oikeellisuuden tunnistaminen oli oleellisinta. Yritysten arjessa tämä oli selviö ja validointiprosessit olivat käytössä ja niitä kehitettiin koko ajan. Tutkimusaukko oli mielestäni yllättävä, koska päätökset ja toiminnot pohjautuvat tietoon. Tiedon oikeellisuuden ja todenperäisyyden olettaisi siis olevan tärkeää, ellei tärkeintä. Löysin yhden selityksen havainnolleni. Koska tietopääomaa pidetään erityisen tärkeänä resurssina monet tutkijat pitävät oletusarvona, että tiedon ja tietoprosessien oikeellisuus on sisään leivottuna. Tämän takia tutkimuksissa katsotaan, että turvallisuutta ei tarvitse erikseen alleviivata. (Jennex ja Zyngier 2007.)

Tutkimuksen edetessä hahmottunut viitekehys on vastaus tutkimuskysymykseen:

”Millainen on tietojohtamisen rooli riskienhallinnassa, kun organisaatiossa pyritään suojautumaan uuden tiedon käyttämiseen liittyviltä riskeiltä?”

Kuvio 21. visualisoi viitekehyksen ja sanallinen kuvaus avaa sen toimintamallia ja siihen vaikuttavia tekijöitä. Myös luvut 2., 4. ja 5. avaavat viitekehyksen elementtejä laajemmin. Yksinkertaisesti todettuna tietojohtamisen elementtejä löytyy paljon uuden tiedon validointiprosessista, siihen vaikuttavista dimensioista ja organisaation mahdollistajien muodostamasta raamista. Uusi tieto, kuten tilinumero, on potentiaalinen uhka. Näin ollen uuden tiedon riskiarviointi ja sen validointiin rakennetun prosessin toimivuus kuuluvat osaksi organisaation riskiarviointia. Maksamiseen liittyvät huijaukset ja kyberuhat olivat kaikissa haastatelluissa yrityksissä osa riskiarviointia. Tietojohtamisen elementtien rooli on suuri ja

monisyinen riskienhallinnassa, kun organisaatiossa luodaan suojakerroin uuden tiedon käyttämiseen liittyviltä riskeiltä suojautumiseen ja haittojen minimoimiseen.

Viitekehys on yksinkertaistettu kuvaus yritysten toimintaympäristön negatiivisista syötteistä ja niiden hallitsemisesta tietojohtamisen työkaluin. Turvallisuus tulisi sisällyttää paremmin ja selkeämmin tietojohtamisen tutkimuskenttään. Asian tarkastelu teknisten ratkaisujen kautta ei riitä, vaan sitä tulee tutkia osana tietojohtamista ja tietoprosesseja. Tietojohtamisen on hyvä sisältää riskien analysointi ja riskienhallinnan on hyvä olla osa organisaation tietojohtamisen strategiaa. Riskienhallinnan tulisi olla jatkuva prosessi ja onnistuakseen se tarvitsee johdon tuen. (Jennex ja Zyngier 2007.) Tämän pro gradu tutkimuksen empiirinen aineisto tukee tätä näkemystä. Jo pelkästään tutkitussa BEC-huijaus ilmiössä haitat ovat paljon suoremmat kuin vain taloudellinen menetys.

Tutkimallani ilmiöllä ei ole suoraa vaikutusta perinteiseen tietojohtamisen tavoitteeseen eli kilpailukyvyn parantamiseen. Vaikutus kohdistuu suorituksen ja suoriutumisen parantamiseen sekä tätä kautta arvonluomiseen organisaatiolle.

6.2 Tutkimuksen jatkohyödyntäminen ja kritiikki

Tässä Pro Gradu tutkielmassa tutkin yritysten tapoja hallita riskejä niiden validoidessa organisaation ulkopuolelta tulevan tiedon todenperäisyyttä. Tutkielmassa toteutettua empiirisen aineiston analyysiä ja tietojohtamisen teorioiden peilausta sekä lopputuloksena muodostettua viitekehystä voi hyödyntää kehittäessään vastaavia maksamiseen liittyviä validointiprosesseja. Tutkimus tarjoaa pro gradu tutkimuksen laajuudessa mitattuna kattavan kuvan tietojohtamisen elementtien hyödyntämisestä riskienhallinnassa, kun organisaatiossa halutaan suojautua uuden tiedon käyttämiseen liittyviltä riskeiltä ja minimoida haitat. Tutkimus ei ole toistettavissa, vaan se on sidottu tähän ajanhetkeen, haastateltujen kokemuksiin ja rooliin sekä tutkijan tutkimusotteeseen tässä hetkessä.

Kuten luvussa 3.4 kuvasin, mitataan laadullisen tutkimuksen luotettavuutta ennemmin uskottavuuden kautta. Mittarina ei ole mittauksen luotettavuus kuten kvalitatiivisessa tutkimuksessa, vaan uskottavuus tutkimuksen toteutusta ja analyysiä kohtaan. Olen pyrkinyt kuvaamaan tarkasti käytetyn tutkimustavan, Gioia metodin käytön askel askeleelta, empiirisen aineiston ja teorian peilauksen ja johtopäätökset. Olen pyrkinyt tulkitsemaan aineistoa tarkasti ja oikein sekä muodostamaan dimensiot ja viitekehyksen tutkimusdataan eli tukittavien käsityksiin perustuen. Otin myös huomioon, että olen itse tutkijana osa tutkimusmenetelmää, Johdannossa ja puhuttaessa yleisesti maksamisesta ammensin paljon omasta ammattiosaamisestani ja kokemuksesta, mutta pyrin myös näihin teksteihin etsimään lähteitä tukemaan sanomaani. Muuten ilmaisin aina selkeästi, jos kyseessä oli omaa pohdintaani. Koen onnistuneeni uskottavan laadullisen tutkimuksen toteutuksessa. (Saunders et al. 2016; Eskola & Suoranta 1998.)

Tutkimusta olisi syventänyt mahdollisuus toistaa haastattelut koodauksen jälkeen. Tai haastattelut olisi voinut toistaa pidemmällä aikajänteellä. Näin olisi voinut analysoida ilmiön pysyvyyttä, mutta pro gradu työn laajuudessa tämä nyt tehty tilanneanalyysi ilmiöstä on riittävä. Aineiston määrä ja analyysi on mitoitettu pro gradun laajuudelle sopivaksi. Tutkimuksessa toteutettiin kuusi puolistrukturoitua haastattelua, joista saatiin riittävä tutkimusaineisto analysoitavaksi. Aineiston määrällä saavutettiin saturaation periaate eli tutkimusongelman kannalta ei tarvittu enempää tietoa. Tarkkaan harkitut ja valitut haastateltavat ja heidän edustamansa yritykset tarjosivat sopivan pienen, mutta tutkimukseen hyvin osuvan korkealaatuisen näytteen. Laadulla varmistin perusteellisen analyysin toteuttamisen. (Eskola & Suoranta 1998; Saunders et al. 2016.)

6.3 Jatkotutkimusten aihioita

Tutkimuksen aineiston analysoinnissa mukailtiin Grounded Theory tutkimusmetodologiaan perustuvaa Gioia metodia. Analyysiprosessi täsmentyy edeten askel askelelta ensimmäisen tason konsepteista, suodattuen toisen tason teemoihin ja lopulta viimeiseksi muodostuvat yhdistetyt dimensiot. aineistoa analysoidaan kokoa ajan ja metodiin kuuluu muistiinpanojen kirjoittamista ja laajaa pohdintaa. Tätä taustaa vasten minulle kertyi iso määrä jatkotutkimusideoita.

Eri tietoprosesseihin tutustuessani havainnoin, että tyypillinen tietoprosessi etenee tiedon luonnista, tiedon säilyttämiseen, jakamiseen ja lopulta käyttöön eli hyödyntämiseen (Heisig 2009; Alavi & Leidner 2001; Bhatt 2001.) Kun peilaan tätä tähän pro gradu tutkimukseen, koen että tietoprosessit eivät huomioi riittävästi tiedon validointia. Tästä havaitsemastani puutteesta olen maininnut jo aiemmin eri kohdissa ja tässä tutkimuksessa asia on saanut arvoisensa huomion, mutta tämä olisi minusta merkittävä tutkimus aihe jatkossa. Lähtökohtana voisi olla monenlainen väärä tietoa tarkoituksellinen kuten huijauksissa, disinformaatio, misinformaatio tai virheellinen tieto.

Artikkeleita etsiessä ja lukiessa tuli mieleen useampi teoreettinen lähtökohta, joista voisi uuden tiedon riskien ja validoinnin dimensioiden teemasta löytää mielenkiintoista tutkittavaa. Aiheetta olisi mielenkiintoista tutkia löydettyjen toisen tason teemojen kautta: organisaation oppimisen näkökulmasta, organisaatiokulttuurin näkökulmasta, psykologisen turvallisuuden näkökulmasta ja tulevaisuudessa myös ajatuksella tekoäly ja koneoppiminen mahdollistajina.

Pohtiessani haastateltuja yrityksiä kumpusi myös jatkotutkimusaiheita. Olisi mielenkiintoista haastatella vastaavasti nyt haastateltujen yritysten tyttäriä ja vertailla tuloksia. Tämä jatkotutkimus pitäisi toteuttaa tänä vuonna, jotta sen voisi katsoa vertautuvat tähän hetkeen tutkittavana ilmiönä. Toinen vastaavan kaltainen mielenkiintoien jatkotutkimusvaihtoehto olisi haastatella eri yrityksiä, mutta muualla kuin Suomessa. Tässä olisi mielenkiintoista, että haastateltavat olisivat hyvinkin erilaisista kulttuureista. Vastaavasti voisi olla mielenkiintoista tehdä vertaileva tutkimus joko eri kokoisissa yrityksissä tai julkinen vs. yksityinen organisaatio.

Luodessani tutkimuksen viitekehystä siihen tuli automaattisesti aspekti ulkoinen toimintaympäristö ja uhat, koska tutkimuksessa käytettiin BEC-huijausta ulkoisena tietosyötteenä. Mutta jäin pohtimaan, millainen viitekehys olisi, jos tietosyöte olisi mahdollisuus. Tämä tutkimus kietoutuu sen ympärille, että uusi tieto on luultavimmin pahasta ja siltä tulee

suojautua. Tieto nähdään kutenkin yritysten tärkeimpänä resurssina eli pääajatus tietojohtamisessa on, että tieto on hyvästä ja sillä saavutetaan etulyöntiasema, kilpailuetua tai kuten tässä tutkimuksessa parempi suorituskyky. Jatkotutkimuksessa voisi kääntää katseen tiedon mahdollisuuksiin ei uhkiin. Vaikka tieto ensin tuleekin aina validoida, jotta jyvät saadaan eroteltua akanoista.

LÄHDELUETTELO

Agazzi, A. (2020) Business Email Compromise (BEC) and Cyberpsychology. Ecclesie, arXiv.org [verkkodokumentti]. [Viitattu 3.8.2023]. Saatuvilla https://arxiv.org/abs/2007.02415

Akhavan, P. & Zahedi, M. R. (2014) Critical Success Factors in Knowledge Management Among Project-Based Organizations: A Multi-Case Analysis. *The ICFAI University journal of knowledge management* 12.1 (2014): 20–20. Print.

Alavi, M. & Leidner, E. (2001) Review: Knowledge Management and knowledge Management Systems: Conceptual Foundations And Research Issues. MIS Quarterly 25(1), pp. 107-136.

Andreeva, T. & Kianto, A. (2012) Does Knowledge Management Really Matter? Linking Knowledge Management Practices, Competitiveness and Economic Performance. Journal of knowledge management 16.4 (2012): 617–636.

Anttila, P. (1998) Tutkimisen taito ja tiedonhankinta. [verkkodokumentti]. [Viitattu 3.1.2024]. Saatuvilla https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/

Archie, J. C., Turner, S. & Wybitul, T. (2020) The Pervasive Threat of Business Email Compromise Fraud – and How to Prevent It. Intellectual Property & Technology Law Journal; Clif-ton Vol. 32, Iss. 7, (Jul/Aug 2020): 13-15

Atlam, H. F. & Oluwatimilehin, O. (2023) Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. Electronics (Basel) ,Vol.12 (1), p.4

Belsis, P., Spyros K. & Evangelos K. (2005) Information Systems Security from a Knowledge Management Perspective. Information management & computer security 13.2/3 (2005): 189–202 [verkkodokumentti]. [Viitattu 30.9.2023]. Saatavilla https://www.researchgate.net/profile/Petros-Belsis/publication/220207883_Information_systems_security_from_a_knowledge_management_perspective/links/5ce088fa299bf14d95a67992/Information-systems-security-from-a-knowledge-management-perspective.pdf

Bhatt, G. (2001) Knowledge management in organizations: examining the interaction between technologies, techniques, and people. Journal of knowledge management, Vol.5 (1), p.68-75

Bhatt, G.D. (2000) Organizing knowledge in the knowledge development cycle. *Journal of Knowledge Management*. Vol. 4 No. 1, pp. 15-26.

Birks, M. and Mills, J. (2015) Grounded theory: A practical guide. Sage. [verkkodokumentti]. [Viitattu 2.12.2023]. Saatavilla https://researchonline.jcu.edu.au/37746/1/37746%20Birks%20and%20Mills%202015%20Front%20Pages.pdf

Botta, A. & Nadeau, M-C. (2022) Global Payments Report, October 2022. McKinsey & Company, Global Banking Practice, The 2022 McKinsey [verkkodokumentti]. [Viitattu 20.12.2023]. Saatavilla https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/the%202022%20mckinsey%20global%20payments%20report/the-2022-mckinsey-global-payments-report.pdf

Choo, C, W. (2001) The knowing organization as learning organization. Education & training (London), Vol.43 (4/5), p.197-205

Chun T., Birks, M. & Francis, K. (2019) Grounded Theory Research: A Design Framework for Novice Researchers. SAGE open medicine 7. [verkkodokumentti]. [Viitattu 10.12.2023]. Saatavilla https://journals-sagepub-com.ezproxy.cc.lut.fi/doi/10.1177/2050312118822927 (verkko)

Corbin, J. M. & Strauss, A. L. (2008) Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory. 3rd edition. Los Angeles, [Calif.]; SAGE, 2008. Print

Corley, K. G. & Gioia, D. A. (2004) Identity Ambiguity and Change in the Wake of a Corporate Spin-Off. *Administrative science quarterly 49.2 (2004): 173–208.*

Cross, C. & Gillett, R. (2020) Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud. Journal of Financial Crime; London Vol. 27, Iss. 3: 871-884. DOI:10.1108/JFC-02-2020-0026

Daghfous, A., Belkhodja, O. and C. Angell, L. (2013) Understanding and managing knowledge loss. *Journal of Knowledge Management,* Vol. 17 No. 5, pp. 639-660.

Davenport, T. H. & Völpel, S. C. (2001) The Rise of Knowledge Towards Attention Management. *Journal of knowledge management* 5.3 (2001): 212–222.

Durst, S., Hinteregger, C. & Zieba, M. (2019) The Linkage between Knowledge Risk Management and Organizational Performance. *Journal of business research 105 (2019): 1–10.*

Durst, S. & Zieba, M. (2019) Mapping knowledge risks: towards a better understanding of knowledge management. Knowledge management research & practice, 2019, Vol.17 (1), p.1-13

Eskola, J. & Suoranta, J. (1998) Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino, 1998. Print.

Eslamkhah, M. & Seno, S. A. H. (2019) Identifying and Ranking Knowledge Management Tools and Techniques Affecting Organizational Information Security Improvement. *Knowledge management research & practice* 17.3 (2019): 276–305. Web.

European Central Bank (2018) The revised Payment Services Directive (PSD2) and the transition to stronger payments security. [verkkodokumentti]. [Viitattu 13.12.2023]. Saatavilla https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html

European Central Bank (2023) The Eurosystem's retail payments strategy – priorities for 2024 and beyond. [verkkodokumentti]. [Viitattu 13.12.2023]. Saatavilla https://www.ecb.europa.eu/pub/pdf/other/ecb.eurosystemretailpaymentsstrategy~5a74eb9ac1.en.pdf?aa5529d7d4b3d566690a338272d64261

Europol (2022) Take control of your digital life. Don't be a victim of cyber scams! [verkkodokumentti]. [Viitattu 13.12.2023]. Saatavilla https://www.europol.europa.eu/sites/default/files/documents/fi_0.pdf

FBI (2022) 2022 INTERNET CRIME REPORT [verkkodokumentti]. [Viitattu 3.8.2023]. Saatavilla https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

FBI (2023) Business Email Compromise. [verkkodokumentti]. [Viitattu 3.8.2023]. Saatavilla https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise

Finanssilala RY (2023) Varo, varmista, varoita -kampanja: Digihuijausten määrä kasvoi selvästi vuoden 2022 jälkipuoliskolla [verkkodokumentti]. [Viitattu 3.8.2023]. Saatavilla https://www.finanssiala.fi/uutiset/varo-varmista-varoita-kampanja-digihuijausten-maara-kasvoi-selvasti-vuoden-2022-jalkipuoliskolla/

F-Secure (2023) [verkkodokumentti]. [Viitattu 24.9.2023]. Saatuvilla https://www.f-secure.com/fi/articles/dark-web /lainattu 24092023

Gehman, J., Glaser, V. L., Eisenhardt, K. M., Gioia, D., Langley, A. & Corley, K. G. (2018) Finding Theory–Method Fit: A Comparison of Three Qualitative Approaches to Theory Building.” Journal of management inquiry 27.3 (2018): 284–300. Web.

Glaser B. G. & Strauss A. L. (1967) The discovery of grounded theory: strategies for qualitative research. New York: Aldine de Gruyter, 1967.

Goode, S. & Lacey, D. (2022) Exploiting Organisational Vulnerabilities as Dark Knowledge: Conceptual Development from Organisational Fraud Cases. Journal of knowledge management 26.6 (2022): 1492–1515.

Heisig, P. (2009) Harmonisation of knowledge management - comparing 160 KM frameworks around the globe. Journal of knowledge management, Vol.13 (4), p.4-31

Hinde, S. (2003) The Law, Cybercrime, Risk Assessment and Cyber Protection. *Computers & security* 22.2 (2003): 90–95. [verkkodokumentti]. [Viitattu 15.10.2023]. Saatuvilla http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/Hinde2003_C&S22_2_LawCybercrimeRiskAssessment.pdf

Hitesh N. S., Aniruddh S. S. & Aniruddh V., Shubha P. (2022) A Comprehensive Review of Fraudulent Email Detection Models teoksessa Giri, Debasis et al. (2022) A Comprehensive Review of Fraudulent Email Detection Models. Proceedings of the Seventh International Conference on Mathematics and Computing. Vol. 1412. Singapore: Springer Singapore Pte. Limited, 2022. 109–127.

Hirsjärvi, S. & Hurme, H. (2022) Tutkimushaastattelu : teemahaastattelun teoria ja käytäntö. [2. painos]. Helsinki: Gaudeamus, 2022. [verkkodokumentti]. [Viitattu 8.1.2024]. Saatuvilla https://www.ellibslibrary.com/reader/9789523458123

Hussinki, H., Kianto, A., Vanhala, M. & Ritala, P. (2017) Assessing the universality of knowledge management practices. Journal of knowledge management, 2017-10, Vol.21 (6), p.1596-1621

Ilvonen, I., Jussila, J.J. & Kärkkäinen, H., (2015). Towards a business-driven process model for knowledge security risk management: Making sense of knowledge risks. *International Journal of Knowledge Management* (IJKM), 11(4), pp.1-18. [verkkodokumentti]. [Viitattu 10.10.2023]. Saatuvilla https://trepo.tuni.fi/bitstream/handle/10024/125768/jussila_IJKM_11_4_article.pdf?sequence=1 10.10.2023

Ilvonen, I., Thalmann S., Manhart, M. & Sillaber, C. (2018) Reconciling digital transformation and knowledge protection: a research agenda. *Knowledge Management Research & Practice,* 16:2 (2018):235-244

Interpol (2023) #BECareful - don't let scammers trick you into making payments to their accounts [verkkodokumentti]. [Viitattu 10.10.2023]. Saatuvilla https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud

Intezari, A., Taskin, N. & Pauleen, D. J. (2017) Looking Beyond Knowledge Sharing: An Integrative Approach to Knowledge Management Culture. *Journal of knowledge management* 21.2 (2017): 492–515. Web.

Jennex, M. & Durcikova, A. (2020) Creating Sustainable Knowledge Systems: Towards a Risk and Threat Assessment Framework. *Journal of Strategic Innovation and Sustainability* 15.4 (2020): 138–152.

Jennex, M. & Durcikova, A. (2014) Integrating IS Security with Knowledge Management: Are We Doing Enough to Thwart the Persistent Threat? 2014 47th Hawaii International Conference on System Sciences. IEEE, 2014. 3452–3459. [verkkodokumentti]. [Viitattu 15.10.2023]. Saatavilla https://ieeexplore-ieee-org.ezproxy.cc.lut.fi/document/6759031

Jennex, M., Durcikova, A. & Ilvonen, I. (2022) Modifying Knowledge Risk Strategy Using Threat Lessons Learned from COVID-19 in 2020-21 in the United States. *Electronic journal of knowledge management.* EJKM 20.3 (2022): 138–151. [verkkodokumentti]. [Viitattu 15.10.2023]. Saatavilla https://academic-publishing.org/index.php/ejkm/article/view/2606/2103

Jennex, M. & Zyngier, S. (2007) Security as a Contributor to Knowledge Management Success. *Information systems frontiers: a journal of research and innovation.* 9.5 (2007): 493–504.

Kallinen, T. & Kinnunen, T. Etnografia. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. [verkkodokumentti]. [Viitattu 6.8.2023]. Saatavilla https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/

Kianto, A. (2011) Tietojohtaminen -mitä, miksi ja miten? Teoksessa Ståhle, P. (toim.) Johtamisen käsikirja, Kauppalehti [kurssimateriaali].

Kianto A. (2021) Johdatus tietojohtamiseen, luento[kurssimateriaali].

Laihonen, H., Hannula M., Helander, N, Ilvonen, I., Jussila, J., Kukko, M., Kärkkäinen, H., Lönnqvist, A., Myllärniemi, J., Pekkola, S., Virtanen, P., Vuori, V. & Yliniemi T. (2013), Tietojohtaminen. Tampere. Tampereen Teknillinen Yliopisto. [verkkodokumentti]. [Viitattu 4.8.2023]. Saatavilla https://trepo.tuni.fi/bitstream/handle/10024/116695/tietojohtaminen.pdf?sequence=2&isAllowed=y

Leo, M., Suneel S. & Maddulety, K. (2019) Machine Learning in Banking Risk Management: A Literature Review. Risks (Basel) 7.1 (2019): 1–22. [verkkodokumentti]. [Viitattu 30.9.2023]. Saatavilla https://www.mdpi.com/2227-9091/7/1/29

Limnell, A. (2023) Ajankohtainen katsaus kyberrikollisuuteen. KRP Kyberrikollisuudentorjunta [verkkodokumentti]. [Viitattu 22.10.2023]. Saatavilla https://poliisi.fi/blogi/-/blogs/ajankohtainen-katsaus-kyberrikollisuuteen-

Louisot, J. & Ketcham, CH. (2014) ERM - Enterprise Risk Management: Issues and Cases, John Wiley & Sons, Incorporated, Somerset. Available from: ProQuest Ebook Central. [9 April 2019].

Magnani, G. & Gioia, D. (2023) Using the Gioia Methodology in International Business and Entrepreneurship Research. *International business review 32.2 (2023)*: 102097

Manhart, M. & Thalmann, S. (2015) Protecting Organizational Knowledge: a Structured Literature Review. *Journal of knowledge management* 19.2 (2015): 190–211.

Martelo-Landroguez, S., Navarro, J.G.C. and Cepeda-Carrion, G. (2019) Uncontrolled counter-knowledge: Its effects on knowledge management corridors. Knowledge Management Research & Practice. 17.2 (2019): 203–212.

Mansfield-Devine, S. (2016) The Imitation Game: How Business Email Compromise Scams Are Robbing Organisations. *Computer fraud & security* 2016.11 (2016): 5–10.

Milton, N., Shadbolt, N., Cottam H. & Hammersley, M. (1999) Towards a Knowledge Technology for Knowledge Management. *International Journal of Human-computer Studies* 51.3 (1999): 615–641.

Nisha, T.N., Bakari, D. & Shukla, C. (2021) Business E-mail Compromise. Techniques and Countermeasures International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), p.217-222

Nonaka, I. (1994) A Dynamic Theory of Organizational Knowledge Creation. *Organization science (Providence, R.I.)* 5.1 (1994): 14–37.

Nonaka, I. Toyama, R. & Konno, N. (2000) SECI, Ba and Leadership: a Unified Model of Dy-namic Knowledge Creation. Long range planning, Vol.33 (1), p.5-34

Leppänen, A. (2021) Kyberrikos on poliisiasia, Opas yrityksille kyberrikostutkinnan kulusta. CYBERDI – Cybercrime prevention, awareness raising and capacity building by RDI on modern cyber attacks (JAMKin ja Polamkin yhteisprojekti) [verkkodokumentti]. [Viitattu 3.10.2023]. Saatavilla https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212/Opas_Kyberrikos+on+poliisiasia.pdf?t=1616740405258

Locke, K. (2003). Bringing grounded theory to studies of management and organizations. In Grounded Theory in Management Research (pp. 94-114). SAGE Publications, Ltd., https://doi.org/10.4135/9780857024428

Palmgren, J. (2024) Huijareilla oli aktiivinen vuosi 2023 – Pankit saivat estettyä digihuijauksia lähes 33 miljoonan euron edestä [verkkodokumentti]. [Viitattu 25.2.2024]. Saatavilla https://www.finanssiala.fi/uutiset/huijareilla-oli-aktiivinen-vuosi-2023-pankit-saivat-estettya-digihuijauksia-lahes-33-miljoonan-euron-edesta/

Palgrave, M. & Nature, S. (2019) Machine Learning and AI for Risk Management. (s. 33-50). Teoksessa Disrupting Finance FinTech and Strategy in the 21st Century. Ed. Lynn, T., Aziz, S. & Dowling, M.1st ed. 2019. Cham: Springer Nature, 2019.

Palva, M. (2015) Suomen Pankin rooli maksuliikkeen kehityksessä: kansallisista järjestelmistä yhteiseurooppalaisiin järjestelmiin. Suomen Pankki, Eurojärjestelmä, yleistajuiset

selvitykset A:116, 2015 [verkkodokumentti]. [Viitattu 23.12.2023]. Saatavilla https://publications.bof.fi/bitstream/handle/10024/43623/A116.pdf?sequence=1&isAllowed=y

Perrott, B. E. (2007) A Strategic Risk Approach to Knowledge Management. *Business horizons 50.6 (2007): 523–533.*

Pienta, D., Thatcher, J. B. & Johnston, A. (2020) Protecting a whale in a sea of phish.

Journal of information technology, Vol.35 (3), p.214-231

Poliisi (2023) Rahanpesun selvittelykeskuksen vuosikertomus 2022 [verkkodokumentti]. [Viitattu 5.10.2023]. Saatavilla https://poliisi.fi/documents/25235045/67733116/Rahanpesun-selvittelykeskuksen-vuosikertomus-2022.pdf/d4d07605-68b5-ee84-ffd7-ec09541dc9d7/Rahanpesun-selvittelykeskuksen-vuosikertomus-2022.pdf?t=1679478208148

Prislan, K., Mihelic, A. & Bernik, I. (2020) A Real-World Information Security Performance Assessment Using a Multidimensional Socio-Technical Approach. *PloS one* 15.9 (2020): e0238739–e0238739.

Rowley, J. (2007) The wisdom hierarchy: representations of the DIKW hierarchy. Journal of information science, Vol.33 (2), p.163-180

Saud Al-Musib, N., Mohammad Al-Serhani. F., Humayun, M. & Jhanjhi, N.Z., (2021) Business email compromise (BEC) attacks. Materials today: proceedings

Saunders, M., Lewis, P. & Thornhill, A. (2016) Research Methods for Business Students: 7. Ed. Seventh edition. Harlow u.a: Pearson, 2016.

Dey I. (2007) Grounded theory (Chapter 5. Teoksessa Seale, C. Qualitative Research Practice. Concise pbk. ed. London: SAGE, 2007. Print.

Spicer, J. (2019) CYBERCRIMINAL PROFILING. EDPACS 60.3 (2019): 1–17. Web

Sveen, F. O, Rich, E. & Jager, M. (2007) Overcoming Organizational Challenges to Secure Knowledge Management. *Information systems frontiers* 9.5 (2007): 481–492. Web.

SWIFT (2023) Swift GPI – the new standard in global payments. [verkkodokumentti]. [Viitattu 5.10.2023]. Saatavilla https://www.swift.com/our-solutions/swift-gpi

Takala, K. (2022) Digitalisaatio muuttaa maksamistapoja Suomessa. [verkkodokumentti]. [Viitattu 13.12.2023]. Saatavilla https://www.eurojatalous.fi/fi/2022/artikkelit/digitalisaatio-muuttaa-maksamistapoja-suomessa/

Tello, J. S. (2023) The impact of AI on the world of finance, a glimpse of the future *CE Noticias Financieras, English ed.;* Miami. 24 May 2023.

The ACCC (2020) Business email compromise scams cost Australians $132 million [verkkodokumentti]. [Viitattu 3.8.2023]. Saatavilla https://www.accc.gov.au/media-release/business-email-compromise-scams-cost-australians-132-million

TIEKE, Tietoyhteiskunnan Kehittämiskeskus r.y. (2023) Mikä on verkkolasku? [verkkodokumentti]. [Viitattu 25.1.2024]. Saatavilla https://tieke.fi/palvelut/liiketoimintapalvelut/verkkolaskuosoitteisto/mika-on-verkkolasku/

Traficom (2022) Laskutushuijaukset lisääntyvät kesäisin - näin suojaudut huijauksilta. [verkkodokumentti]. [Viitattu 3.10.2023]. Saatavilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/laskutushuijaukset-lisaantyvat-kesaisin-nain-suojaudut-huijauksilta?toggle=Ohjeita%20organisaatioille

Ulkoministeriö (2023) Kansainväliset pakotteet. [verkkodokumentti]. [Viitattu 20.12.2023]. Saatavilla https://um.fi/pakotteet

Wagner, S. M., Lukassen, P. & Mahlendorf, M. (2010) Misused and Missed Use — Grounded Theory and Objective Hermeneutics as Methods for Research in Industrial Marketing. *Industrial marketing management 39.1 (2010): 5–15.*

Whitman, M. & Mattord, H. (2018) Management of Information Security. 6th ed. Mason OH: Cengage, 2018. Print

LIITE 1

	HAASTATTELUKYSYMYKSET
	OLEMASSA OLEVAT KAUPPAKUMPPANIT
K1	**Millainen prosessi yrityksessänne on käytössä, kun saatte sähköpostitse tiedon uudesta maksatuksen tilinumerosta?**
K2	**Jos prosessia ei ole käytössä, miksi tähän ratkaisuun on päädytty?**
K3	**Jos prosessi on olemassa, millainen se on ja miten siihen on päädytty?**
3.1	Millaisia päätöksiä prosessin aikana tehdään ja kenen toimesta?
3.2	Onko käytössä teknologiaa avustamassa?
3.3	Koulutatteko työntekijöitä tämän aihepiirin osalta? Miten ja kuinka usein?
3.4	Kuinka usein ja miten prosessin toimivuutta / ajantasaisuutta arvioidaan?
3.5	Otetaanko prosessi (huijausuhka) huomioon riskienhallinnan isossa kuvassa?
K4	**Miten täysin uuden toimittajan kanssa avattava prosessi eroaa aiemmin kuvatusta?**
	VIRANOMAISET
K5	**Miten prosessissa on huomioitu olemassa olevia virallisia ohjeistuksia?**
5.1	ON: miten?
5.2	EI: miksi ei?
	SOME ja NETTISIVUT, oletteko miettineet huijauksia tältä kannalta?
K6	Liittyykö ohjeistuksiinne työntekijöiden työhön liittyvien asioiden avaaminen somessa kuten linkedin)?
	BEC huijaukset
K7	**Onko yrityksenne kohdannut BEC-huijauksia?**
7.1	ON: millaisia ja missä kohtaan paljastuneet?
7.2	Onko ne aina huomattu?
7.3	Meitä on huijattu: miten?
7.4	Jos huijauksia ei ole havaittu, millaisia tappioita olette kärsineet?
7.5	Mitä olette oppineet näistä tilanteista >>ovatko ne aiheuttaneet muutoksia toimintatapoihin?
	Tutkimuskirjallisuudessa puhutaan huijauksen uhrien kokemista
K8	**psykologisista vaikutuksista, kuten pelko ja ahdistus.**
8.1	Miten kokemuksesi mukaan huijaus on vaikuttanut työntekijöihin?
8.2	Miten koet, että tätä vaikutuksiin voi vaikuttaa?
K9	**Ovatko mielestäsi huijaukset muuttuneet viime aikoina?**
K10	**Tuleeko vielä mieleen jotakin, mitä haluaisit lisätä?**

SAATESANAT (tutkimushaastattelut)

Hei xxx,

Tässä vielä sovitusti tietosuojailmoitus ja lisätietoja gradun tutkimusosioon liittyen.

Ensinnäkin kiitos, kun suostuit osallistumaan pro gradu -tutkielmaan liittyvään haastatteluun. Saan näin mahdollisuuden ammentaa LUT-yliopistolle tekeillä olevaan tutkielmaani ammattitaitoosi ja kokemukseesi perustuvasta tiedosta.

Pääaineeni on tietojohtaminen ja johtajuus. Gradussani tutkin millaisia tietojohtamisen tietoprosesseja liittyy tiedon validointiin. Rajauksena tilitiedon aitouden validointi, silloin kun tieto on toimitettu yritykseen sähköpostitse. Aihe kumpuaa alati lisääntyvistä BEC (business e-mail compromise) huijauksista; niiden vaikutuksesta ja haitoilta suojautumisen vaikutuksista yrityksen tietojohtamisen prosesseihin.

Tutkiakseni näitä vaikutuksia haastattelen kansainvälisesti toimivien yritysten talousosastolla työskenteleviä henkilöitä. Vertaan haastatteluissa saamiani tuloksia aiheen tutkimuskirjallisuudesta muodostettuun viitekehykseen sekä viranomaisten antamiin ohjeistuksiin.

Haastattelun kesto on noin yksi tunti ja siihen ei ole tarvetta valmistautua etukäteen. Haastattelu toteutetaan Teamsin välityksellä ja se tallennetaan. Haastattelun jälkeen aukikirjoitan tallenteen tutkimuskäyttöä varten. Aineisto käsitellään anonymisoituna eikä organisaatiota ja haastateltavan henkilöllisyyttä ilmaista tutkielmassa. Tallenne säilytetään tutkimuksen teon ajan ja se on vain allekirjoittaneen käytössä yllä kuvatussa tarkoituksessa.

Liitteenä on vielä henkilötietojen käsittelyyn liittyvä tietosuojailmoitus. Mikäli kysyttävää ilmenee vastaan mielelläni

Kuulemisiin sovittuna haastatteluaikana.

Ystävällisin terveisin,

OPINNÄYTETYÖTÄ KOSKEVA

TIETOSUOJAILMOITUS

EU:n yleinen tietosuoja-asetus (2016/679)

artiklat 13 ja 14

Laatimispäivämäärä:1.11.2023

Mitä tarkoitusta varten henkilötietoja kerätään?

Teen pro gradu -tutkielmaa LUT-yliopistolle (Lappeenrannan-Lahden teknillinen yliopisto). Gradussani tutkin millaisia tietojohtamisen tietoprosesseja liittyy tiedon validointiin. Rajauksena tilitiedon aitouden validointi, silloin kun tieto on toimitettu yritykseen sähköpostitse. Aiheen pohjana toimii alati lisääntyvät BEC-huijaukset (business e-mail compromise). Haastatteluiden avulla pyritään selvittämään, millaisia prosesseja on käytössä tiedon aitouden varmistamisessa. Haastatteluissa kerätään yksilöiden näkemyksiä ja kokemuksia aiheeseen liittyen. Tämä tietosuojailmoitus liittyy näiden tietojen käsittelyyn.

Mitä tietoja kerään?

Haastateltavilta ei kysytä mitään taustatietoja, mutta haastateltavien vastuualueet ovat rekisterinpitäjän tiedossa. Tietoisesti haastatteluissa ei kerätä haastateltavaa yksilöiviä tietoja, mutta keskustelun aikana saattaa tulla esiin joitakin tämän kaltaisia tietoja, jotka tallentuvat tallenteelle ja siitä tehtävään aukikirjoitukseen (litterointi). Tällaisia mahdollisesti yksilöiviä tietoja ei ilmaista tutkielmassa.

Millä perusteella tietoja kerätään?

Tähän tutkielmaan liittyvien henkilötietojen keräämisperuste on haastateltavan suostumus osallistua haastatteluun.

Mistä kaikkialta henkilötietoja kerään

Tutkielman haastatteluiden yhteydessä henkilötietoja kerätään ainoastaan rekisteröidyltä itseltään.

Kenelle tietoja siirretään?

Pro gradu -tutkielmaa liittyvä aineisto luovutetaan anonymisoituna valmiina tutkielmana laatijan lisäksi työnohjaajalle, tarkastajalle ja LUT-yliopiston haltuun.

Minne tietoja siirretään?

Tutkielmassa kerättyjä henkilötietoja saatetaan säilyttää ulkoisten palveluntarjoajien alustoilla. Ulkoisten palveluntarjoajien palvelimien serverit saattavat sijaita Euroopan talousalueen ulkopuolella, näin ollen henkilötietoja saattaa joissain tapauksissa siirtyä EU:n ja ETA-alueen ulkopuolelle säilytykseen.

Kerättyjen tietojen turvallinen säilyttäminen

Haastattelun tallenne säilytetään LUT:n tietoturvallisilla palvelimilla ja tietoihin pääsy on mahdollista ainoastaan rekisterinpitäjälle. Tallenteella olevat yksilöivät tiedot ovat vain rekisterinpitäjän tiedossa, ja tallenteet tuhotaan tutkielman valmistuttua. Aineisto anonymisoidaan litterointi vaiheessa.

Kuinka kauan kerättyä aineistoa säilytetään?

Tallennetta säilytetään pro gradu -tutkielman tekemisen ajan, maksimissaan 12 kuukautta tallennusajankohdasta. Myös litteroitu aineisto säilytetään maksimissaan 12 kuukautta litterointiajankohdasta. Anonymisoitua tietoa ei katsota henkilötiedoiksi eikä niihin sovelleta tietosuojalainsäädäntöä.

Millaista päätöksentekoa aineiston pohjalta tehdään?

Aineistoa käsiteltäessä ei tapahdu henkilörekisteriin liittyvää automaattista päätöksentekoa.

Rekisteröidyn oikeudet

Rekisteröidyllä on oikeus peruuttaa antamansa suostumus, milloin henkilötietojen käsittely perustuu suostumukseen. Tutkimuksen keskeyttämiseen ja suostumuksen peruuttamiseen mennessä kerättyjä tietoja voidaan käyttää osana tutkimusaineistoja.

Rekisteröidyllä on oikeus tehdä valitus Tietosuojavaltuutetun toimistoon, mikäli rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä on rikottu voimassa olevaa tietolainsäädäntöä.

Rekisteröidyllä on seuraavat EU:n yleisen tietosuoja-asetuksen mukaiset oikeudet:
a) Rekisteröidyn oikeus tarkistaa itseään koskevat tiedot.
b) Rekisteröidyn oikeus tietojensa oikaisemiseen.
c) Rekisteröidyn oikeus tietojensa poistamiseen. Oikeutta henkilötietojen poistamiseen ei sovelleta, jos tietojen käsittely on tarpeen yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, jos oikeus tietojen poistamiseen estää tai suuresti vaikeuttaa henkilötietojen käsittelyä
d) Rekisteröidyn oikeus tietojen rajoittamiseen.
e) Rekisteröidyn oikeus siirtää tiedot toiselle rekisterinpitäjälle.

Tutkimusrekisterin tiedot
Rekisterin nimi: Johanna Kiviranta-Mounier, pro gradu -tutkielman aineisto
Kyseessä on kertatutkimus, jonka kestoaika on 1.8.2023 – 31.7.2024
Henkilötietoja säilytetään maksimissaan kaksitoista kuukautta keräysajankohdasta
Rekisterinpitäjän ja yhteyshenkilön tiedot
Nimi: Johanna Kiviranta-Mounier
Puh: xxx xxx xxxx
Sähköposti: johanna.kiviranta-mounier@student.lut.fi
Tutkimuksen suorittaja**:** Tutkimuksen suorittaja ja tietojen käsittelijä on sama kuin rekisterinpitäjä.