LIIKESALAISUUKSIIN KOHDISTUVIEN INSIDER-RISKIEN HALLINTA

Ville Jääskeläinen

Suojelupoliisin julkaisusarja 1/2018

LIIKESALAISUUKSIIN KOHDISTUVIEN INSIDER-RISKIEN HALLINTA

Ville Jääskeläinen

ISBN 978-952-324-230-2 (nid.)
ISBN 978-952-324-231-9 (PDF)

Tutkimus perustuu tekijän opinnäytetyöhön, joka on hyväksytty Laurea-ammattikorkeakoulun turvallisuusjohtamisen koulutusohjelmassa vuonna 2018. Tulkinnoista ja kannanotoista vastaa tekijä, eikä niitä ole tulkittava Suojelupoliisin virallisiksi näkemyksiksi.

Sisällys

1 Johdanto 4
1.1 Keskeiset käsitteet 6
1.2 Tutkimustarve 7
1.3 Tavoite ja tutkimuskysymys 8
1.4 Tutkimuksen rakenne ja teoreettinen viitekehys 10
2 Tutkimusasetelma 12
2.1 Tiedonkeruumenetelmät 13
2.1.1. Integroiva kirjallisuuskatsaus 13
2.1.2 Tilannekuvan koostaminen poliisiasiain tietojärjestelmästä 16
2.1.3 Teemahaastattelut 18
2. 2 Aineiston analyysi ja teemoittelu 19
3 Liikesalaisuudet 22
3.1 Liikesalaisuustiedot 22
3.2 Tiedon oikeudeton hankkiminen ja käyttäminen 24
4 Insider-uhka 26
4.1 Insider-taksonomia ja -uhkan rajaus 26
4.2 Liikesalaisuuksiin kohdistuvat insider-uhkat 29
4.3 Liikesalaisuuksiin kohdistuvien insider-rikosten tilannekuva Suomessa 41
5 Insider-riskien hallinta 54
5.1 Työsuhteen alun insider-riskien hallintakeinot 61
5.1.1 Rekrytointivaihe 61
5.1.2 Henkilöturvallisuusselvitys 64
5.1.3 Salassapitosopimus 67
5.2 Työsuhteen aikaiset sekä yleiset insider-riskien hallintakeinot 70
5.2.1 Turvallisuuspolitiikka 70
5.2.2 Suojattavan tiedon tunnistaminen, luokittelu ja priorisointi 72
5.2.3 Tiedonsaantitarpeen rajaaminen 75
5.2.4 Tehtävien eriyttäminen 76
5.2.5 Vähimpien oikeuksien periaate 79
5.2.6 Henkilöstön koulutus 81
5.2.7 Työhyvinvointi 85
5.3 Teon paljastaminen ja työsuhteen päättymisvaiheen riskien hallintakeinot 88
5.3.1 Teon havaitseminen 88
5.3.2 Havaintojen ilmoittaminen 95
5.3.3 Puuttuminen ja sisäinen tutkinta 99
5.3.4 Työsuhteen päättymisvaihe 105
6 Johtopäätökset 111
6.1 Liikesalaisuuksiin kohdistuvien insider-riskien hallinta Suomessa 111
6.2 Diskussio 113
Lähteet 119

1 Johdanto

From those whom we trust,
comes a great caution

– Arabialainen sananlasku

Tieto on tänä päivänä organisaatioiden arvokkainta omaisuutta ja tietotekniikan jatkuva nopea kehitys mahdollistaa entistä suurempien tietomäärien käsittelyn, siirtämisen ja tallentamisen. Useat yritykset ovat riippuvaisia tiedoistaan ja pyrkivät suojaamaan ei-julkiseksi luokitellut liikesalaisuustiedot oikeudettomalta ilmitulolta ja käyttämiseltä.

Työelämän kehityksen johdosta tietoon kohdistuu kuitenkin uudenlaisia riskejä, jotka ovat aiempaa todennäköisempiä ja vakavampia. Erityisesti innovaatioihin liiketoimintansa perustavat yritykset altistuvat yhä enenevässä määrin tietovarkauksille, tiedon luvattomalle kopioinnille, vakoilulle tai salassapitosopimusten rikkomiselle, joissa tekojen tarkoituksena on liikesalaisuuksien väärinkäyttö (EU/2016/943, 2).

Tutkimusten mukaan yli 78 % pienistä ja keskisuurista suomalaisista yrityksistä ja yli 93 % suurista yrityksistä, jotka tuottavat innovaatioita, hyödyntävät liikesalaisuuksien tai patenttien antamaa suojaa tietojensa turvaamiseksi (Wajsman & Garcia-Valero 2017, 30–33). Liikesalaisuuksien suojaaminen on erityisen tärkeää pienille ja keskisuurille yrityksille, koska innovaatioiden oikeudettomasta ilmitulosta ja käyttämisestä seuraavat vahingot voivat pahimmassa tapauksessa kaataa yrityksen.

Paradoksaalista on, että oma henkilöstö on sekä yrityksen tärkein tekijä että uhka. Tietoturvayhtiö McAfeen tekemän tutkimuksen mukaan 43 %:ssä tiedon oikeudettomista hankkimis- ja käyttämistapauksista vastuussa oli organisaation oma työntekijä (2015, 4). Lisäksi toisessa yhdysvaltalaistutkimuksessa yritykset kertoivat menettäneensä sadoista tuhansista jopa miljooniin dollareihin vuodessa omien työntekijöiden aiheuttamien tietoon kohdistuneiden riskien takia (Ponemon 2016, 9).

Kilpailevat yritykset tai omien kansallisten yritystensä etuja varmistavat tiedustelupalvelut voivat yrittää soluttaa tai värvätä tietolähteitä yrityksestä viemään liikesalaisuustietoja tai yrityksen oma työntekijä voi käyttää hyötymistarkoituksessa hänelle annettuja tietoja. Edellä kuvattu uhka, jota tässä tutkimuksessa kutsutaan englanninkielisellä termillä ”insider” ei ole uusi, mutta siihen liittyvät riskit ja niiden toimintaympäristö muuttavat jatkuvasti muotoaan. Pahimmillaan insider-rikoksina ilmentyvät riskit ovat piilorikollisuutta, joka ei tule kohteena olleen yrityksen eikä viranomaisten tietoon koskaan. Yhdysvaltain keskustiedustelupalvelu CIA:n entinen työntekijä on todennut, että ihmisten lojaalius omaa maatansa kohtaan on asia, johon monet uskovat ja jonka mukaan monet elävät. Lojaalius palkan maksavaa yritystä kohtaan ei kuitenkaan usein saavuta samaa asemaa ihmisten arvoissa. (Earnest & Karinch 2010.)

Tämän työn tutkimustavoitteena on selvittää, miten suomalaiset yritykset voivat parhaiten hallita liikesalaisuuksiin kohdistuvia insider-riskejä ja mitkä ovat riskienhallintakeinojen uhkat ja mahdollisuudet. Käytännössä työn tulosten on tarkoitus auttaa yrityksiä niiden omassa tiedustelun torjuntatyössä. Ilmiötä tutkitaan Suomessa toimivien yritysten näkökulmasta, vaikkakin monet insider-uhkaan, sen ilmenemismuotoihin ja riskien hallintakeinoihin liittyvät tekijät ovat universaaleja paikallisesti noudatettavasta lainsäädännöstä riippumatta.

Tutkimusongelmaa lähestytään laadullisesti ja tiedonkeruumenetelminä on käytetty kirjallisuuskatsausta ja asiantuntijahaastatteluja. Kirjallisuuslähteet perustuvat merkittävältä osin anglosaksiseen tutkimukseen, joten suomalaisten turvallisuusasiantuntijoiden haastatteluilla on pyritty tuomaan suomalaisen elinkeinoelämän ja viranomaisten näkökulma käsiteltävään aiheeseen. Riskienhallintasynteesin lisäksi työssä esitetään Suomessa vuosina 2012–2016 tapahtuneita insider-rikoksia koskeva tilannekuva. Faktatietoon perustuvan tilannekuvan tarkoituksena on tukea yritysten riskinhallintaan kuuluvaa uhkakartoitusprosessia sekä viestintää insider-riskeistä, joita on vaikea hallita ja joista viestiminen yrityksen sisällä on haastavaa.

Tutkimuksen lähestymis- ja kirjoitustavan valinnalla on pyritty tutkimustulosten ja ilmiön yleistajuistamiseen. Aihe on ajankohtainen, koska uusi liikesalaisuuslaki on hyväksytty tutkimuksen julkaisuhetkellä ja keskeisinä referensseinä käytetyt riskienhallintaa ja tietoturvallisuutta käsittelevät standardit on tutkimusprosessin aikana päivitetty. Tutkimukseen perehtymisen jälkeen lukijalla tulisi olla ajantasainen peruskäsitys siitä, mikä on suomalaisiin liikesalaisuustietoihin kohdistuva insider-uhka ja miten insider-riskejä voidaan hallita.

1.1 Keskeiset käsitteet

INSIDER

Tässä tutkimuksessa insiderilla tarkoitetaan yrityksen työntekijää, joka tahallisesti vaarantaa tietoturvallisuuden ja pyrkii käyttämään omaksi tai kolmannen osapuolen hyödyksi yrityksen liikesalaisuustietoja. Määritelmä sisältää lainsäädännön näkökulmasta sekä tiedon oikeudettoman hankkimisen että käyttämisen.

Tekstin luettavuuden parantamiseksi työntekijällä voidaan tarkoittaa samanaikaisesti yrityksen nykyistä tai entistä työntekijää, harjoittelijaa tai sopimuskumppania. (Cappelli ym. 2012, xx; Jackson 2012, 278; Mehan 2016, 11–14; Blackwell 2009, 8; Contos 2006, 51; Cole & Ring 2000, 7.)

Väärinkäsitysten välttämiseksi insider-termiä ei ole suomennettu. Insiderin mahdollinen käännös "sisäpiiriläinen" on finanssialalla käytössä oleva termi, jolla viitataan arvopaperikaupan kannalta merkityksellisen tiedon omistamiseen sekä rikoslaissa (39/1889, 51.luku) ja arvopaperimarkkinalaissa (746/2012, 12. luku) kiellettyyn sisäpiirintiedon väärinkäyttöön, mikä ei täysin vastaa tässä tutkimuksessa käytettyä määritelmää yrityksen sisällä olevasta uhkasta.

LIIKESALAISUUS

Liikesalaisuudella tarkoitetaan tietoa, joka on salaista, jolla on taloudellista arvoa ja jonka haltija on pyrkinyt kohtuullisin toimenpitein pitämään salaisena.

RISKI

Riskillä tarkoitetaan epävarmuuden vaikutusta tavoitteisiin (ISO 31000:2018, 3.1). Tässä tutkimuksessa riski-käsitettä kuvataan ISO 31000 2018-standardin määritelmän lisäksi suojattavan arvon, sitä koskevien haavoittuvuuksien ja uhkien leikkauspisteenä.

RISKIENHALLINTA

Riskienhallinta (risk management) on "koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien osalta (ISO 31000:2018, 3.2)". Se on yrityksen osa, joka vastaa riskienhallinnan menetelmien kehittämisestä ja toteuttamisesta, mutta ei riskeistä (SFS 2018).

RISKIEN HALLINTA

Riskien hallinnalla (managing risk) tarkoitetaan yrityksen tekemiä toimenpiteitä riskien ottamiseksi ja välttämiseksi (SFS 2018).

YRITYSSALAISUUS

Yrityssalaisuus on rikoslaissa (39/1889, 30.luku 11 §) käytössä ollut termi, joka on uuden liikesalaisuuslain (2018) myötä vaihdettu liikesalaisuuden määritelmään.

1.2 Tutkimustarve

Helsingin seudun kauppakamarin lokakuussa 2016 teettämän kyselytutkimuksen mukaan suomalaisyritykset (n = 754) pitävät phishing- ja haittaohjelmahyökkäyksien jälkeen kyberturvallisuuden suurimpana uhkana yhtiön luottamuksellisen tiedon vuotamista ja seuraavaksi suurimpana uhkana yhtiön omia työntekijöitä.

Erityisesti suuriksi luokitellut suomalaisyritykset (yli 200 henkilöä) pitivät kyselyssä omia työntekijöitä yhtenä suurimmista kyberturvallisuuden uhkista (40 % vastaajista). (Helsingin seudun kauppakamari 2016, 8-9.) Havaintoja tukee Yhdysvalloissa 2005 tehty tutkimus, jonka mukaan kiinnostus yritysten sisäisiä uhkia kohtaan kasvaa yrityksen koon kasvaessa (Contos 2005, 34).

Helsingin seudun kauppakamari on lisäksi laatinut Keskuskauppakamarin kanssa selvityksen vuonna 2017, jonka aiheena olivat yritysten rikosturvallisuustilanne ja muun muassa yrityksiin kohdistuneet rikokset ja väärinkäytökset. Selvitys perustuu 762 yritysjohtajan vastauksiin. Selvityksessä 17 % vastaajista ilmoitti, että viimeisen kolmen vuoden aikana yrityksen työntekijä on syyllistynyt tiedon väärinkäyttöön yritystä kohtaan. Huomion arvoista on, että suurista yrityksistä (yli 250 henkilöä) jopa 44 % ilmoitti työntekijän syyllistyneen tiedon väärinkäyttöön yritystä kohtaan. (Saario & Vesterinen 2017, 13 & 17). Myös Yhdysvalloissa vuonna 2016 tehdyn tutkimuksen perusteella tapahtuneiden insider-rikosten todennäköisyys korreloi vahvasti organisaation suuren koon kanssa (Ponemon Institute 2016, 7).

Kauppakamarien rikosteemaa käsittelevän vuonna 2012 laaditun selvityksen mukaan noin joka kymmenennessä yrityksessä (12 %) poislähtevä työntekijä oli kopioinut luvatta tietoja viimeisen kolmen vuoden aikana. Lähes joka seitsemännessä yrityksessä (15 %)

oli myös kerrottu "kriittisistä yritysasioista" luvatta joko henkilökuntaan kuuluvalle tai ulkopuoliselle viimeisen kolmen vuoden aikana. (Keskuskauppakamari & Helsingin seudun kauppakamari 2012, 26.)

Tämän tutkimuksen tarve perustuu edellä mainittujen tutkimustulosten perusteella insider-uhkatiedon, riskienhallintatiedon ja suomalaisen lainsäädännön yhdistävää tietoa koskevaan tutkimusaukkoon.

Insider-uhkaa ja sen aiheuttamien riskien hallintaa on tutkittu paljon etenkin anglosaksisissa maissa. Tutkimusta ovat tehneet yhdysvaltalaiset ja iso-britannialaiset tietoturvaviranomaiset, yliopistot sekä turvallisuus- ja tiedusteluviranomaiset (muun muassa Software Engineering Institute 2016; NITTF 2016; CPNI 2013; Cappelli ym. 2012; Department of Defence 2011; Colwill 2009; Kowalski ym. 2009). Tutkimuksen suunnitteluvaiheessa ei kuitenkaan havaittu suomalaisten yritysten liikesalaisuuksiin kohdistuvien insider-riskien hallintaa koskevaa tutkimustyötä. Omien työntekijöiden aiheuttamiin tekoihin liittyvää vahinko- ja tietoriskienhallintaa sekä turvallisuusjohtamista koskevaa lainsäädäntöä ja sen soveltamista on tutkittu sekä Suomessa että ulkomailla (mm. Valtiovarainministeriö 2008; Humphreys 2008). Kyseisten tutkimusalueiden tuloksia ei ole kuitenkaan havaintojen perusteella integroitu.

Kansallisen yritysturvallisuusstrategian mukaan "suomalaisten yritysten tärkein pääoma on tieto". Strategiassa kuvataan kuitenkin, miten elinkeinoelämällä on ollut ongelmia liikesalaisuuksien määrittelyssä. (Sisäasiainministeriö 2012, 22.) Tiedon suojaaminen digitalisoituvassa maailmassa on yrityksille elintärkeää ja insider-uhka aiheuttaakin merkittävimpiä yritysten tietopääomaan kohdistuvia riskejä.

Jotta tietopääomaa voidaan tehokkaasti suojata insider-uhkalta, tulee se tunnistaa ja määritellä liikesalaisuudeksi. Liikesalaisuuden antaman juridisen suojan yhtenä kriteerinä on tunnistamisen ja määrittelyn lisäksi myös tosiasiallisesta salassapidosta huolehtiminen (Vapaavuori 2016, 66). Tosiasiallisesta salassapidosta huolehtimiseksi yrityksen tulee omilla turvallisuustoimenpiteillään suojata liikesalaisuustietoa insider-riskeiltä.

1.3 Tavoite ja tutkimuskysymys

Työn tavoitteena on tutkimusaukkoon perustuen selvittää ja koota synteesi siitä, miten suomalaiset yritykset voivat parhaiten hallita liikesalaisuuksiin kohdistuvia insider-riskejä ja mitkä ovat riskienhallintakeinojen uhkat ja mahdollisuudet.

Insider-uhkiin ja -riskienhallintaan liittyvää teoriaa on pyritty käsittelemään monipuolisesti, jotta lukijalla olisi mahdollisuus tehdä omia tulkintoja ja päätelmiä lukemisen ohessa. Viskari (2001, 31) korostaa laadukkaan tutkimuksen perustuvan aiheen suppeaan ja syvälliseen rajaukseen. Tehty rajaus on tärkeä tutkimuksen validiteetin varmistamiseksi, koska insider-uhka- ja riskityyppeihin lukeutuu hyvin erilaisia profiileja, haavoittuvuuksia ja niihin soveltuvia riskien hallintakeinoja, mistä syystä on järkevä syventyä tarkasti rajattuun uhkaprofiiliin ja riskeihin.

Välittömästi samaan aiheeseen keskittyneitä suomalaisia tutkimuksia ei prosessin aikana havaittu, joten tutkimuksen teossa pyrittiin luomaan perusta suomalaista elinkeinoelämää koskevalle insider-tutkimukselle sitomalla ilmiö mahdollisimman paljon osaksi suomalaista elinkeinoelämää lainsäädännön käsittelyllä sekä erityisesti haastatteluilla saadulla empiirisellä näkökulmalla. Joissain kohdin tutkimusta on kuitenkin ollut tarkoituksenmukaista viitata myös sellaisiin insider-tutkimuksiin, joissa on tutkittu julkishallintoon kohdistuvia insider-riskejä.

Tutkimuksen ulkopuolelle on rajattu insider-uhkan ja siihen liittyvän riskienhallinnan keinot, jotka liittyvät tietojärjestelmillä toteutettavaan käyttäytymisen valvontaan ja tietoverkkojen ja -järjestelmien tarkempiin teknisiin kontrolleihin. Rajauksen ulkopuolelle on jätetty myös erilaiset varta vasten insider-uhkien havaitsemiseen kehitetyt tietojärjestelmät (esim. Parker ym. 2004, 148).

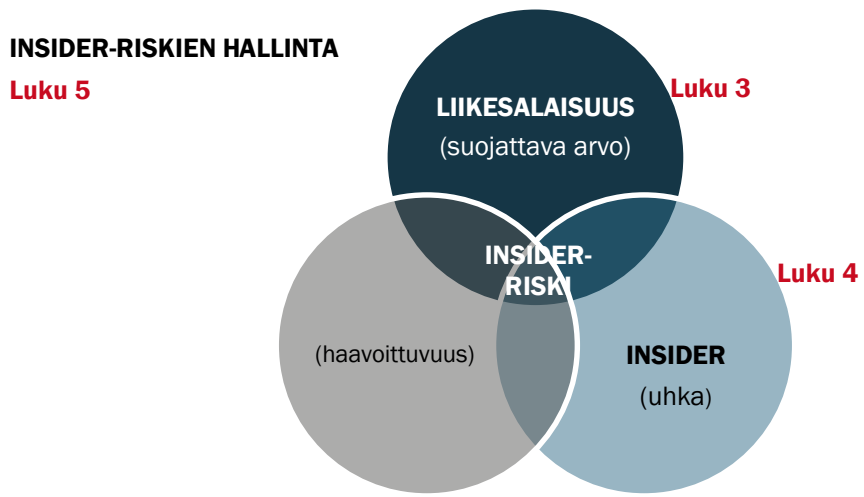
Tutkimus keskittyy hallinnollisin keinoin toteutettaviin yleisiin riskien hallintakeinoihin, joiden merkitys insider-riskien hallinnassa on merkittävämpi kuin teknisten kontrollien (Blankenship 2016). Merkittävin näkökulmaan vaikuttava tekijä on tutkimuksen yhteydessä käsiteltävä lainsäädäntö. Insider-riskejä ja niiden hallintaa on käsitelty rikoslain (39/1889) ja liikesalaisuuslain (2018) näkökulmasta.

Työn rakenteen taustalla oleva tutkimuskysymys ohjaa tutkimuksen tekemistä, joten tutkimusongelma tulisi aina jäsentää tutkimuskysymykseksi (Kananen 2008, 130). Silvermanin (2005, 90) ja Punchin (1998, 49) mukaan hyvän tutkimuskysymyksen merkkejä ovat, että kysymykseen on mahdollista vastata ja kysymys on kiinnostava ja aihe ajankohtainen. Eriksson ja Kovalainen (2008, 41) lisäävät, että hyvin rajattu tutkimuskysymys ilmaisee ainoastaan yhden tai muutaman tutkimuksen pääideoista.

Työn tavoitteiden täyttymiseksi tutkimuskysymys on muotoiltu seuraavasti:
Miten liikesalaisuuksiin kohdistuvia insider-riskejä voidaan hallita Suomessa?

1.4 Tutkimuksen rakenne ja teoreettinen viitekehys

Tutkimuksen teoreettinen viitekehys ja runko muodostuvat liikesalaisuuksista ja insider-uhkasta. Työn empiirinen osuus ja tulokset kuvaavat insider-riskien hallintaa. Viitekehys voidaan kuvata insider-riskin määritelmän avulla (kuvio 1), jossa riski muodostuu suojattavan arvon (liikesalaisuus), uhkan (insider) ja eri haavoittuvuuksien leikkauspisteeseen.



Kuvio 1: Insider-riski ja tutkimuksen viitekehys

ISO 27005 2013-standardin mukaan riskienhallinnan tulisi perustua uhkien tunnistamiseen, jotta riskien arviointi olisi vaikuttavaa (6 & 8.2.3). Standardiin perustuen tutkimuksessa käsitellään ensin viitekehyksenä liikesalaisuudet ja insider-uhka, joiden jälkeen esitellään insider-riskien hallintaa koskevat tulokset ja analyysi.

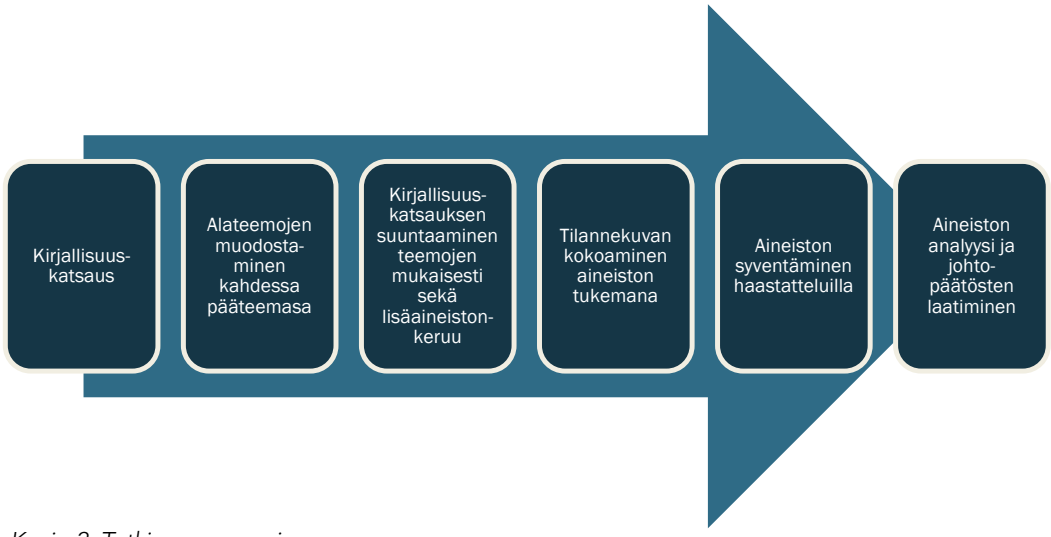
Viitekehys alkaa liikesalaisuuden määritelmän ja luonteen lyhyellä esittelyllä tutkimuksen suojattavaksi arvoksi määritellyn liikesalaisuustiedon tunnistamiseksi. Insider-uhka on käsitelty omana lukunaan, jossa tunnistetaan ja mallinnetaan uhka sekä luodaan ajantasainen tilannekuva elinkeinoelämän havaintojen ja poliisin tietoon tulleiden insider-tapausten perusteella. Suojattavan arvon ja uhkien tunnistamisen jälkeen esitellään tutkimuksen kirjallisuuskatsaukseen ja teemahaastatteluihin perustuvia erilaisia insider-riskien hallintakeinoja.

Insider-riskien hallintaa käsittelevässä luvussa kirjallisuuskatsauksen ja haastattelujen tulokset on yhdistetty. Eri menetelmien tuottamien aineistojen yhdistämisellä pyrittiin analyysissä luomaan tilanne, jossa suomalaisten turvallisuusasiantuntijoiden haastattelut muodostavat anglosaksisten tutkimuslähteiden tulosten kommentaarin ja eri tutkimusmenetelmillä kerättyjen lähteiden välille syntyy keskustelua. Yhdistelmällä parannettiin myös työn luettavuutta, koska haastatteluaineiston teemoittelu perustui kirjallisuuskatsaukseen. Hirsjärvi ym. mukaan (2010, 261–261) onnistuneen laadullisen tutkimuksen yhtenä merkkinä onkin, että tutkijan pohdinta ja tieteellinen kerronta sekoittuvat ja tukevat toisiaan.

2 Tutkimusasetelma

Tässä luvussa kuvataan työn tutkimusasetelma, koska tutkimusta koskevan lähestymistavan, käytettyjen tiedonkeruu- ja analyysimenetelmien ja tutkimusaineiston valinnan sekä työn luotettavuuden ja eettisten näkökulmien kuvaaminen ja perusteleminen on olennainen osa tutkimustyötä (Viskari 2009, 36).

Tutkimustyön lähestymistapa oli laadullinen, jossa lähtökohtana on tutkittavan ilmiön kuvaaminen (Hirsjärvi ym. 2010, 161–163; Tuomi & Sarajärvi 2009, 85.) Laadullinen lähestymistapa soveltui liikesalaisuuksia uhkaavien insider-riskien tutkimiseen, koska tarkoituksena oli kuvata ilmiötä useista eri näkökulmista. Laadulliset työt jaetaan usein neljään luokkaan: kartoittava, selittävä, kuvaileva ja ennustava. Työ voi sisältää piirteitä eri luokista, mutta ensisijainen luokka voidaan määritellä työn tarkoituksen perusteella. (Hirsjärvi 2010, 137–138.) Tämä työ on luokiteltu kartoittavaksi, koska tarkoituksena oli tuottaa tutkimusaiheesta integroiva synteesi ja ideoita suomalaisten yritysten liikesalaisuuksia uhkaavien insider-riskien hallitsemiseen.



Kuvio 2: Tutkimusprosessi

Kuviossa 2 on kuvattu tutkimusprosessi. Prosessi mukaili hermeneuttiseksi kehäksi kutsuttua prosessia, jossa tulkinnan edetessä myös tutkijan esiymmärrys muuttuu, joka vaikuttaa tutkimuksen uuteen suuntaamiseen, joka tuo jälleen uutta ymmärrystä, jolloin tulkintaprosessille ei voida asettaa absoluuttista päätepistettä (Väkevä 1999).

Tutkimus alkoi kirjallisuuskatsauksella, jonka perusteella työlle muodostui viitekehys sekä analyysin pohjana toimiva teemoittelu. Teemoittelun johdosta kirjallisuuskatsausta suunnattiin uudelleen ja teemoja varten kerättiin täydentävää aineistoa. Suuntaamisen perusteella ja aineiston tietojen pohjalta päädyttiin vertailun vuoksi kokoamaan Suomea koskeva insider-rikostilannekuva.

Insider-uhkaa ja –riskienhallintaa koskevan aineiston analyysin perusteella suoritettiin teemoihin liittyvä lainsäädäntöä koskeva tiedonkeruu, jonka aineistoa verrattiin kirjallisuuskatsauksen aineistoon suomalaisen näkökulman saamiseksi tutkimukseen. Lainsäädännöllisen tarkastelun jälkeen suoritettiin asiantuntijahaastattelut, joiden tarkoituksena oli syventää aiempaa aineistoa, kerätä taustatietoa kirjallisen aineiston analyysiä varten sekä kommentoida kirjallisuuskatsauksen tuloksia (Alastalo & Åkerman 2010, 375). Tutkimusprosessin viimeisenä vaiheena oli lopullinen aineiston analyysi ja johtopäätösten laatiminen.

2.1 Tiedonkeruumenetelmät

Tutkimuksen tiedonkeruumenetelminä käytettiin kirjallisuuskatsausta ja sen tuloksia syventäviä haastatteluita. Toteutetulla aineisto- ja menetelmätriangulaatiolla pyrittiin lisäämään työn luotettavuutta (Tuomi & Sarajärvi 2002, 141–142). Kirjallisuuskatsauksen ja haastattelujen lisäksi erillisenä aineistona käytettiin poliisiasiain tietojärjestelmän tietoja, joista koottiin insider-rikosten Suomea koskeva tilannekuva. Tiedonkeruu kohdennettiin tutkimustavoitteen saavuttamiseksi kolmen eri aihepiirin aineistoon:

1. insider-uhka
2. omien työntekijöiden aiheuttamien tahallisten tietoriskien hallinta
3. liikesalaisuuksia ja insider-riskienhallintakeinoja koskeva lainsäädäntö

2.1.1. Integroiva kirjallisuuskatsaus

Tietoperustan luominen ja teemoittelun muodostaminen toteutettiin kirjallisuuskatsauksena. Salmisen mukaan kirjallisuuskatsauksen avulla voidaan tarkastella aiempiin tutkimuksiin liittyvää teoriaa ja luoda sen perusteella uutta tietoa. Ne voidaan jakaa kolmeen perustyyppiin: kuvaileva kirjallisuuskatsaus, systemaattinen kirjallisuuskatsaus ja meta-analyysi.

Kuvailevaa kirjallisuuskatsausta voidaan luonnehtia yleiskatsaukseksi, jossa tutkittavaa aihetta pystytään kuvaamaan laajasti ja tutkimusaiheen ominaisuuksia voidaan luokitella tarvittaessa. Kuvaileva kirjallisuuskatsaus voidaan edelleen jakaa kahteen eri tyyppiin, joita ovat narratiivinen ja tässä tutkimuksessa käytetty integroiva kirjallisuuskatsaus. (Salminen 2011, 3-6)

Integroiva kirjallisuuskatsaus sopii menetelmäksi, kun halutaan kuvata tiettyä ilmiötä mahdollisimman monipuolisesti. Sen avulla voidaan saavuttaa ajantasaista tietoa tutkimusilmiöstä, kehittää teoriaa ja soveltaa tiedon tuloksia käytäntöön (Flinkman & Salanterä 2007, 86). Cooper (1989, 15) jakaa integroivan kirjallisuuskatsauksen vaiheet viiteen osaan: tutkimusongelman asettelu, aineiston hankkiminen, arviointi, analyysi sekä tulkinta ja tulosten esittäminen.

1. Tutkimus-ongelman asettelu	2. Aineiston hankkiminen	3. Arviointi	4. Analysointi	5. Tulkinta ja tulosten esittäminen
”Miten liike-salaisuuksiin kohdistuvia insider-riskejä voidaan hallita Suomessa?” Tutkimus-kysymys sisältää insider-uhkan, riskien-hallinnan ja suomalaisen liikesalaisuuslain säädännön integraation	Aineiston-keruussa käytettiin sekä sähköisiä tietokantoja että kirjallisuus-lähteitä	Aineiston arvioinnissa keskityttiin sisäänotto- ja poissulku-kriteerien perusteella kerätyn aineiston relevanssin arviointiin	Tutkimus-aineisto analysoitiin sisällön-analyysin menetelmällä Analysoinnin tarkoituksena oli tuottaa työn tavoitteiden mukainen laaja-alainen synteesi aineiston tuloksista	Aineiston luokittelua varten tehtiin pääjako uhka- ja riskienhallinta-aineistolle näiden mahdollisimman selvän ja johdon-mukaisen esitystavan varmistamiseksi ja tutkimus-kysymykseen vastaamiseksi

Taulukko 1: Integroivan kirjallisuuskatsauksen viisi vaihetta (Cooper 1989, 15)

Kirjallisuuskatsauksen aineistonkeruu tapahtui 1.1.2016–31.12.2017. Aineiston keruussa hyödynnettiin sekä sähköisiä tietokantoja (EBSCOhost, ProQuest Central, ProQuest Ebook Central, Google Scholar, Google) että kirjallisuuslähteitä, joita hankittiin erityisesti Laurea-ammattikorkeakoulun kirjastosta ja uusimmat julkaisut kirjakaupoista.

Hakusanoina käytettiin insider-uhkaan liittyen käsitteitä: insider threat, insider risk ja insider risk management, jotka ovat kaikki insider-aihetta käsittelevissä tutkimuksissa yleisesti käytettyjä termejä. Testihakujen perusteella suomenkielistä aineistoa ei ollut saatavilla, lukuun ottamatta kauppakamareiden laatimia kyselytutkimuksia.

Riskienhallinnan taustalla olevaksi näkökulmaksi valikoitui useissa insider-uhkaa koskevissa aineistoissa sovellettu syvyyssuuntainen turvallisuusperiaate ja siihen perustuva ISO 27000-tietoturvallisuuden hallintajärjestelmän standardisarja. Tästä syystä riskienhallintaa varten ei tehty erillistä aineistonkeruusuunnitelmaa, vaan perehdyttiin standardisarjaan. Turvallisuusjohtamista ja Suomea koskevaan lainsäädäntöön liittyvää aineiston keruuta varten ei myöskään laadittu erillistä aineistonkeruusuunnitelmaa, vaan lakeihin ja oikeuskirjallisuuteen perehdyttiin insider-uhkaa koskevan aineiston ja syvyyssuuntaisen turvallisuusajattelun perusteella tehdyn jaon suuntaamana.

Aineiston haun jälkeen suoritettiin aineiston valinta. Stolt & Rautasalon mukaan kirjallisuuskatsauksen aineistolle tulee määritellä tutkimuskysymyksiin perustuvat sisään- ja poissulkukriteerit. Hyväksyttyjen ja poissuljettujen aineistojen valinta perustuu kriteereihin, joiden perusteella voidaan tehdä aihealueeseen, menetelmiin ja tuloksiin liittyviä rajauksia. (2007, 59.)

SISÄÄNOTTOKRITEERIT	POISSULKUKRITEERIT
YLEISET KRITEERIT KAIKELLE AINEISTOLLE	
Suomenkielinen tai englanninkielinen aineisto	Muu kuin suomen- tai englanninkielinen aineisto
Vastaa tutkimusongelmaan	Ei vastaa tutkimusongelmaan
KRITEERIT INSIDER-UHKAA KOSKEVALLE AINEISTOLLE	
Tiedon luottamuksellisuuden tahalliseen vaarantamiseen liittyvä aineisto hyötymis-tarkoituksessa (tiedon oikeudeton hankkiminen ja käyttäminen)	Tiedon luottamuksellisuuden tahattomaan (unintentional insider) vaarantamiseen liittyvä aineisto, tiedon käytettävyyden ja eheyden vaarantamiseen liittyvä aineisto, tiedon luottamuksellisuuden tahalliseen vaarantamiseen liittyvä, mutta yrityksen vahingoittamiseen tai väärinkäytösten paljastamiseen liittyvä aineisto, muu insidereita koskeva aineisto, joka ei liity suojattavaan tietoon.
KRITEERIT RISKIEN HALLINTAA KOSKEVALLE AINEISTOLLE	
Vahinkoriskejä koskeva aineisto	Muita kuin vahinkoriskejä koskeva aineisto
Tahallisesti aiheutettujen ihmislähtöisten riskien hallintaan (security) liittyvä aineisto	Ainoastaan tapaturmien, onnettomuuksien ja virheiden riskienhallintaan (safety) liittyvä aineisto
KRITEERIT LIIKESALAISUUKSIA KOSKEVALLE AINEISTOLLE	
Insider-riskienhallintaan liittyvä suomalaista elinkeinoelämää säätelevää lainsäädäntöä koskeva aineisto (Suomen ja EU:n regulaatio)	Muiden maiden elinkeinoelämää säätelevää lainsäädäntöä koskeva aineisto

Taulukko 2: Lähdeaineiston sisäänotto- ja poissulkemiskriteerit

Taulukon 2 kriteerien täyttymistä arvioitiin otsikon, avainsanojen ja tarvittaessa varsinaisen tekstin perusteella. Ensimmäisenä poissulkevana tekijänä käytettiin otsikkoa, jonka perusteella poissuljettiin tutkimuskysymykseen vastaamiseen liittymätön aineisto. Otsikon perusteella soveltuvaa aineistoa arvioitiin tarkemmin mahdollisten avainsanojen ja varsinaisen tekstin perusteella. Tarvittaessa aineistosta poimittiin ainoastaan tietty luku, josta oli hyötyä tutkimuksen toteuttamisessa. Aineiston valinnassa käytettiin hyväksi sanahakutoimintoa, jonka takia alkuperäisiä hakusanoja voitiin etsiä tekstin sisältä. Sisäänottokriteerit suunniteltiin tarkoituksella laveaksi, jotta aineistoa kertyisi paljon. Aineiston suuri määrä mahdollisti saturoituneen aineiston ulkopuolisten yksittäisten havaintojen poimimisen tutkimukseen.

2.1.2 Tilannekuvan koostaminen poliisiasiain tietojärjestelmästä

Kirjallisuuskatsauksen aineiston alustavan analyysin perusteella havaittiin, että useissa maissa on koottu tilastotietoja yrityksiin kohdistuneista insider-rikoksista. Tällaista Suomessa tehtyä rikostilastoa ei tutkimuksen teon yhteydessä havaittu, joten erityisesti suomalaisen näkökulman saamiseksi ja yritysten uhkakartoitusprosessin (ISO 27005 2013) tukemiseksi päädyttiin kokoamaan Suomea koskeva insider-rikostilannekuva.

Rikoslain (39/1889) 30. luvussa on säädetty liikesalaisuuksien rikosoikeudellinen suoja. Näiden lisäksi lain 38 §:ssä määritellyt salassapitoon liittyvät rikokset voivat liittyä liikesalaisuusvelvoitteen rikkomiseen. Tilannekuvan kokoamiseksi rikoslaista poimittiin lainkohdat, joissa teko kohdistuu liikesalaisuuksia sisältävään tietoon ja tekijällä on mahdollista toteuttaa teko yrityksen sisältäpäin ja mahdollisesti legitiimien käyttöoikeuksien avulla.

Koska tässä tutkimuksessa määriteltyihin rikoksiin on mahdollista syyllistyä myös insider-tekijää koskevan rajauksen ulkopuolelle määriteltävä henkilö, piti tilannekuva koostaa käymällä läpi jokainen rikosilmoitus laadullisesti. Tilannekuvan laajuus päätettiin rajata viiden vuoden ajanjaksolle, jotta tutkimus luo ajankohtaisen kuvan liikesalaisuuksiin kohdistuvista insider-rikoksista. Tilannekuvan koostaminen aloitettiin vuoden 2017 aikana, joten tilannekuvan ajanjaksoksi määriteltiin viisi viimeistä täyttä kalenterivuotta.

Tilannekuvassa on esitetty elinkeinoelämään kohdistuvien yrityssalaisuusrikoksina ilmentyvien insider-riskien tilannekuva Suomessa vuosina 2012–2016.

Tilannekuva perustuu poliisin tietoon tulleisiin rikosepäilyihin niissä elinkeinoelämään kohdistuvissa rikoksissa, joissa teko voi sisältää yritysten suojattavan tiedon väärinkäyttöä. Tilannekuvan ulkopuolelle rajattiin tutkimuksen tietojärjestelmiä koskevan aiherajauksen perusteella rikoslain (39/1889) 38.luvun 8 § ja 8 a § sekä rikoslain 12. luvun maanpetosrikokset niiden valtionhallintoon viittaavan ja jo pelkän ilmoitustiedon salaisen luonteen vuoksi. Tilannekuvassa on esitetty jokaiseen rikosnimikkeeseen liitettyjen rikosilmoitusten määrä ja insider-tunnusmerkkien täyttävien tekojen määrä kaikista ilmoituksista. Insider-tunnusmerkkien täyttyminen on arvioitu jokaisen rikosilmoituksen sisällön perusteella erikseen seuraavien rajausten mukaisesti:

Poliisiasiain tietojärjestelmään tehdyn haun yleisinä rajauksina olivat seuraavat tekijät:

- rikosten epäilty alkamisaika oli aikavälillä 1.1.2012 – 31.12.2016
- tilannekuvasta on rajattu pois manner-Suomen ulkopuolella tapahtuneeksi ilmoitetut rikokset
- tilannekuvassa ei ole huomioitu poliisin, syyttäjän tai tuomioistuimen ratkaisuja ilmoituksiin liittyen, koska tilannekuvassa on haluttu esittää insider-epäilyjen määrä

Insider-tunnusmerkkien määrittelynä käytettiin seuraavaa rajausta:

- rikosilmoituksessa mainittu epäilty on henkilö, jolla on asemansa puolesta sisäistä tietoa organisaatiosta ja voi olla organisaation nykyinen tai entinen työntekijä, harjoittelija tai sopimuskumppani
- epäillyn insider-rikoksen kohteena ollut tieto on suojattu yrityksen edun vuoksi
- epäillyn insider-rikoksen ilmeisenä tavoitteena on ollut tiedon hyödyntäminen (hyödyntämistarkoitus) omaksi tai kolmannen osapuolen hyödyksi, ei kohteena olevan yrityksen haitaksi (vahingoittamistarkoitus) tai väärinkäytösten ilmiantamiseksi (whistleblowing)

Tilannekuvan tulokset on esitetty rikosnimikkeittäin, minkä jälkeen on koottu tilannekuvan yhteenveto. Ulkomaisiin tilastotietoihin tehtävän vertailun vuoksi tilannekuvatiedoissa on lisäksi vertailtu sukupuolten osuutta määritellyissä insider-tekijöissä sekä teknisissä ja ei-teknisissä rooleissa työskentelevien osuutta tunnusmerkkeihin sopivista epäillyistä insider-tekijöistä. Tilannekuvan lähdeaineisto on julkisuuslain (621/1999, 24§) perusteella salassa pidettävää, mutta järjestelmästä poimittu tieto on sanitoitu ja luokiteltu julkiseksi ennen tutkimuksen julkaisemista.

2.1.3 Teemahaastattelut

Kirjallisuuskatsauksen avulla kerätyn aineiston syventämiseksi tehtiin lisäksi haastatteluita. Haastattelut soveltuivat tutkimuksen syventäväksi tiedonkeruumenetelmäksi parhaiten, koska kirjallisuuskatsauksen johdosta tutkimuksella oli vahva tietoperusta, jota haluttiin pyrkiä syventämään. Esimerkiksi kyselytutkimuksella saatavat vastaukset olisivat oletettavasti tuottaneet lähinnä jo kirjallisuuskatsauksessa havaittuja saturoituneita yleistietoja Suomessa vähän tutkitusta aiheesta.

Haastattelulajiksi valittiin teemahaastattelu, jossa vastaukset eivät ole sidottu ennaltamääritettyihin vastausvaihtoehtoihin. Tällaista haastattelua kutsutaan myös puolistrukturoiduksi haastatteluksi. (Hirsjärvi & Hurme 2000, 47–48.) Teemahaastattelut käydään nimensä mukaisesti eri teemojen alla, joten haastattelulaji soveltui hyvin kirjallisuuskatsauksen perusteella luotujen teemojen alle kootun tiedon syventämiseen.

Alastalon ja Åkermanin mukaan teemahaastatteluina suoritettavien asiantuntijahaastattelujen tarkoituksena on hankkia tietoa, jota asiantuntijalla oletetaan olevan, erotuksena haastatteluista, joiden tarkoituksena on selvittää haastateltavasta itsestään jotakin (2010, 373).

Tutkimushaastateltavien valinta oli kokonaisuus, jossa pyrittiin löytämään asiantuntijoita, joilla on erilainen koulutus- ja työtausta keskenään. Yhteisenä tekijänä oli kuitenkin haastateltavien vahva asiantuntemus aihepiirin teemoista. Haastateltavien koulutusaste vaihteli ylemmästä korkeakoulututkinnosta tohtorin tutkintoon ja haastateltavat olivat poliisi-, sotilas- ja siviilitaustaisia asiantuntijoita sekä elinkeinoelämästä että viranomaisista. Tällä ratkaisulla pyrittiin saamaan sekä yritysasiantuntijoiden konkreettinen ja omakohtainen näkemys että viranomaisten kokoava näkemys elinkeinoelämään kohdistuvista insider-uhkista ja niistä muodostuvien riskien hallinnasta. Haastateltavia henkilöitä oli yhteensä seitsemän.

Koska tutkimuskohteena ja haastattelujen aiheena olivat suojautumiskeinot rikosilmiöltä, jolla on kytkös kaikkein vakavimpiin tiedon luottamuksellisuuteen kohdistuviin uhkiin, päätettiin tasapuolisesti kaikkien haastateltavien henkilöllisyys suojata heidän itsensä ja edustamiensa organisaatioiden suojaamiseksi. Tämän ei todettu vaarantavan työn reliabiliteettia verrattuna muuhun tutkimuskenttään, koska haastateltavien anonymisoiminen on muodostunut normiksi laadullisessa haastattelututkimuksessa (Alastalo & Åkerman 2010, 383).

Haastatteluihin valmistauduttiin huolellisesti laatimalla kirjallisuuskatsausta koskeva alustava analyysi ennen haastatteluja.

Alustavan analyysin perusteella muodostuivat kahteen pääteemaan jaetut alateemat, jotka toimivat samalla haastattelujen teemoina. Usein haastatteluiden analysointiin käytettävä teemoittelu rakentuu vasta haastatteluaineistosta saatavan aineiston perusteella (Saaranen-Kauppinen & Puusniekka 2006a). Tutkimuksen triangulaation takia teemoittelu on kuitenkin johdettu kirjallisuuskatsauksessa muodostuneista teemoista, jotta aineiston analysointi ja tietoperusta voidaan luontevasti yhdistää. Haastattelukysymysten muotoilussa pyrittiin yleisestä yksityiseen pyrkivään rakenteeseen, jossa haastateltaville annettiin aluksi mahdollisuus kertoa aihepiiristä vapaasti (Hirsjärvi & Hurme 2000, 107).

Haastateltavia lähestyttiin ensin puhelimitse, minkä jälkeen heille lähetettiin tutkimusta ja sen aihetta koskevat yleistiedot sekä haastatteluteemat sähköpostilla. Alastalo & Åkermanin mukaan haastattelijan tulisi välttää tilannetta, jossa hänen sanomisensa vaikuttavat haastateltavan vastauksiin (2010, 381). Tästä syystä haastateltaville jaettiin pelkästään haastattelukysymykset etukäteen ja ainoastaan kysyttäessä tarkennettiin aihetta tai kysymyksiä. Tällä pyrittiin välttämään johdattelua, jonka valmiista kirjallisuuskatsauksesta tai insider-tilannekuvasta puhuminen olisivat mahdollisesti aiheuttaneet.

2. 2 Aineiston analyysi ja teemoittelu

Tutkimusaineistoa kerättiin ja analysoitiin osittain samaan aikaan. Tutkimuksen alateemat luotiin impressionistisesti lähdekirjallisuuden perusteella, ja niiden sisällä käsiteltiin sekä katsauksen että haastattelujen avulla kerätyt tiedot. Alateemojen alle pyrittiin analyysissä luomaan synteesi, jota syvennettiin asiantuntijahaastattelujen perusteella.

Tutkimusaineiston analysointiin sovellettiin teemoittelua ja deduktiivista teorialähtöistä analyysiä, jotta eri tavalla ilmiöitä lähestyneistä aineistosta saatiin muodostettua järjestelmällinen synteesi (Saaranen-Kauppinen & Puusniekka 2006). Tähän ratkaisuun päädyttiin tutkimuksen tavoitteiden vuoksi sen perusteella, että aineisto, teoria ja empiria saatiin keskustelemaan keskenään (Anttila 2006, 392). Teemoittelun avulla saatiin nostettua esille eniten käsitellyt teemat tutkimuksen insider-riskien hallinnan viitekehyksessä.

Aineiston alateemojen valinta perustui aineistossa eniten käsiteltyihin aihealueisiin eli saturaatioon, jolla tarkoitetaan aineistossa tapahtuvaa kertautumista. Hirsjärven ym. mukaan saturaatiota voi kuvata siten, että on olemassa tietty määrä aineistoa, jonka perusteella voidaan tehdä yleistyksiä kaikesta olemassa olevasta aineistosta (2010, 182).

Insider-riskien hallintaan liittyviä kokoavia alateemoja tunnistettiin aineiston saturaation perusteella neljätoista:

- rekrytointivaiheen toimenpiteet
- henkilöturvallisuusselvitys
- salassapitosopimus
- turvallisuuspolitiikka
- suojattavan (liikesalaisuus) tiedon luokittelu
- tiedonsaantitarpeen rajaaminen
- tehtävien eriyttäminen
- vähimpien oikeuksien periaate
- henkilöstön koulutus
- työhyvinvointi
- teon havaitseminen
- teosta ilmoittaminen
- tekoon puuttuminen
- työsuhteen päättymiseen liittyvät toimenpiteet

Insider-riskienhallinnan alateemoja voi aineiston analyysin perusteella kutsua myös insider-riskienhallinnan parhaiksi käytänteiksi, koska niitä on sovellettu ja käsitelty eniten eri julkaisuissa.

Kirjallisuuskatsauksen menetelmällisenä tavoitteena oli löytää aiemmissa tutkimuksissa ja julkaisuissa saturoitunutta insider-riskienhallinta-aineistoa täydentävää tietoa. Useissa aineistoissa esitettiin samoja toistuvia havaintoja insider-uhkasta ja -riskienhallinnasta. Lähes jokaisessa läpikäydyssä aineistossa oli kuitenkin jotain uutta tietoa yksityiskohtien muodossa, mitä ei ollut tuotu muissa aineistoissa esille. Nämä saturoituneen aineiston rinnalla esitellyt tiedonmurut ovat koottuna uutta tietoa ja osa työn tuloksista.

Haastattelujen analysoinnin tavoitteena oli syventää kirjallisuuskatsauksessa saatuja tuloksia ja nostaa esiin erilaisia kokemukseen perustuvia tietoja insider-riskien hallinnasta ennalta valituissa teemoissa.

Aineisto on pyritty saamaan keskustelemaan kirjallisuuskatsauksen ja tietoperustan kanssa ja mahdollisesti kyseenalaistamaan tai tukemaan niissä esitettyjä väitteitä. Toisin kuin kirjallisuuskatsauksessa, haastatteluaineiston keruussa ei tavoiteltu saturaatiota, vaan niiden tarkoituksena oli tuoda erilaisia näkökulmia kirjallisuuskatsauksen tuottamaan aineistoon. Haastattelut nauhoitettiin analyysiä varten, mutta materiaalille tehtiin työstämisvaiheessa ainoastaan propositiotason litterointi. Vilkan ja Airaksisen mukaan litterointi ei ole välttämätöntä, mikäli tiedonhankinnan tavoitteet voidaan saavuttaa ilman sitä (2003, 64). Sanatarkka litterointi suoritettiin ainoastaan, kun haluttiin esittää sitaatteja, jotka kommentoivat erityisen osuvasti tietyn alateeman alla käytyä keskustelua kirjallisuusaineiston, tietoperustan ja muiden asiantuntijoiden kesken.

Haastateltaviin viitataan tekstissä lähteenä ”Haastateltava A-G”.

3 Liikesalaisuudet

Tässä luvussa kuvataan tiiviisti, mikä on liikesalaisuus ja mitä on liikesalaisuustiedon oikeudeton hankinta ja käyttäminen lainsäädännön perusteella. Jotta yritys voi suojata tietonsa tehokkaasti tulee sen tuntea liikesalaisuuksia koskeva lainsäädäntö, koska useat liikesalaisuuksia koskevat oikeustapaukset eivät ole menestyneet, kun liikesalaisuuden reunaehtojen täyttymistä ei ole voitu osoittaa. (Vapaavuori 2016, 45–46.)

3.1 Liikesalaisuustiedot

Suomen lainsäädännössä on useita kohtia, joissa viitataan välillisesti tai välittömästi insider-toimintaan. Tässä työssä lainsäädäntöä käsitellään kuitenkin lähinnä uuden liikesalaisuuslain (2018), Rikoslain (39/1889) sekä EU:n liikesalaisuusdirektiivin näkökulmasta, koska liikesalaisuuslain on tarkoitus kumota Sopimattomasta menettelystä elinkeinotoiminnassa annettuun lakiin (1061/1978) kirjatun liikesalaisuuksia koskevan sääntelyn ja Työsopimuslakiin (55/2001) on tarkoitus tehdä lakiuudistuksen myötä viittaus uuteen liikesalaisuuslakiin (HE 49/2018, 1).

Liikesalaisuuslain säätämisen tarkoituksena oli tuoda kansallisesti täytäntöön EU:n liikesalaisuusdirektiivi ja selkeyttää nykyistä pirstaleista sääntelyä (HE 49/2018, 1 & 36). Direktiivin jalkautuksen jälkeen liikesalaisuuksien vähimmäistaso tulisi olla sama kaikissa jäsenmaissa. (Eur-Lex 2016, Vapaavuori 2016, 24).

Liikesalaisuudella tarkoitetaan lain mukaan tietoa:

a) joka ei ole kokonaisuutena tai osiensa täsmällisenä kokoonpanona ja yhdistelmänä tällaisia tietoja tavanomaisesti käsitteleville henkilöille yleisesti tunnettua tai helposti selville saatavissa;
b) jolla a alakohdassa tarkoitetun ominaisuuden vuoksi on taloudellista arvoa elinkeinotoiminnassa;
c) jonka laillinen haltija on ryhtynyt kohtuullisiin toimenpiteisiin sen suojaamiseksi;

Tämä EU:n liikesalaisuusdirektiivistä johdettu liikesalaisuuslaissa esitetty määritelmä perustuu Suomea velvoittavaan TRIPS-sopimukseen (World Trade Organization 1994, 39 artikla).

Liikesalaisuudet voidaan asian jäsentämiseksi jakaa teknisiin ja taloudellisiin yritys-salaisuuksiin.

Teknisiä yrityssalaisuuksia voivat olla esimerkiksi (Vapaavuori 2016, 52–53):

- tuotanto-, valmistus- ja kokoonpanopiirustukset
- testitulokset
- tuotteiden rakenne ja spesifikaatiot
- valmistusohjeet
- käsikirjat
- tuotanto-, käsittely- tai säilöntämenetelmät
- kemiallisten yhdisteiden koostumukset
- konemallit
- prototyypit
- lähdekoodit
- tietokoneohjelmistot
- tuotekehityksen tulokset

Taloudellisia yrityssalaisuuksia voivat olla esimerkiksi:

- tuotekehitys-, yhteistoiminta- ja yrityskauppasopimukset sekä muut liiketoiminta-sopimukset
- yritysten välisiä suhteita koskevat tiedot
- asiakasrekisterit ja -tiedot
- hankintahinnat
- toimittaja- ja alihankkijatiedot
- katetiedot
- alennuspolitiikat
- hinnastot
- strategia-, liiketoiminta- ja markkinointisuunnitelmat
- talousennusteet
- myyntitiedot
- yrityskauppasuunnitelmat
- julkaisematon mainoskampanjamateriaali
- kilpailija-analyysit
- yrityksen organisaatiotiedot
- henkilöstötiedot
- myynti- ja hinnoittelutiedot

Tämän lisäksi myös tieto siitä, että jokin menetelmä, prosessi tai tuote ei toimi voi olla liikesalaisuus (Vapaavuori 2016, 74–75). Liikesalaisuuden voimassaoloajalle ei teoriassa ole rajaa, mikäli suojattava tieto pysyy salaisena ja sitä suojataan asianmukaisesti. Liikesalaisuudella ei myöskään ole maantieteellisiä rajoitteita, vaan se on voimassa ympäri maailman. (Vapaavuori 2016, 33-34.)

3.2 Tiedon oikeudeton hankkiminen ja käyttäminen

Liikesalaisuuslaissa (2018) on määritelty liikesalaisuuden oikeudeton hankkiminen, joka on osa tässä tutkimuksessa käsiteltävä insider-uhkaa. Lain mukaan liikesalaisuutta ei saa hankkia tai yrittää hankkia oikeudettomasti. Tiedon hankkiminen on oikeudetonta, jos se tapahtuu:

1) anastamalla;
2) luvattomasti kopioimalla, jäljentämällä, havainnoimalla tai muutoin käsittelemällä sellaisia liikesalaisuuden haltijan asiakirjoja, esineitä, materiaaleja, aineita tai sähköisiä tiedostoja, jotka sisältävät liikesalaisuuden, tai joista liikesalaisuus voidaan johtaa; tai
3) muulla kuin 1 tai 2 kohdassa tarkoitetulla hyvän liiketavan vastaisella menettelyllä.

Liikesalaisuuden hankkiminen on oikeudetonta myös, jos henkilö on liikesalaisuuden hankkiessaan tiennyt tai tämän olisi pitänyt tietää, että liikesalaisuus on saatu suoraan tai välillisesti siltä, joka on oikeudettomasti käyttänyt liikesalaisuutta tai ilmaissut sen 4 §:ssä tarkoitetulla tavalla.

Poikkeuksen tekee se, että ”liikesalaisuuden hankkiminen, käyttäminen tai ilmaiseminen ei ole oikeudetonta, jos liikesalaisuus on hankittu, sitä on käytetty tai se on ilmaistu yleisen edun suojaamista varten väärinkäytöksen tai laittoman toiminnan paljastamiseksi”. Tällä lainkohdalla viitataan väärinkäytösten ilmiantamiseen, jota kutsutaan englanninkielessä termillä ”whistleblowing”. Tiedon hankkiminen, käyttäminen tai ilmaiseminen ei myöskään ole oikeudetonta, jos sitä voidaan pitää hyväksyttävänä sananvapauden käyttämisenä.

Liikesalaisuuden antaman suojan saamiseksi yrityksen tulee huolehtia salassapitoehdon tai -sopimuksen tekemisestä työntekijöiden kanssa, koska tietoa ei saa käyttää oikeudettomasti tai ilmaista, jos henkilöä sitoo liikesalaisuuden käyttämistä tai ilmaisemista rajoittava sopimus tai velvoite. Liikesalaisuus ei kuitenkaan sopimuksesta huolimatta anna suojaa yrityksen tiedoille seuraavissa tapauksissa (Vapaavuori 2016, 35):

- toinen yritys keksii itsenäisesti liike- tai yrityssalaisuuden (independent discovery)
- toinen yritys selvittää liike- tai yrityssalaisuuden valmista tuotetta tutkimalla (reverse engineering)
- toinen yritys saa sattumalta tiedon liike- tai yrityssalaisuudesta
- jos käytetään työntekijöiden tai työntekijöiden edustajien tiedonsaantia ja heidän kuulemistaan koskevaa oikeutta tai
- sellaisella muulla tavalla, joka on hyvän liiketavan mukaista

4 Insider-uhka

Onkohan yhtäkään työntekijää, joka ei olisi vienyt mitään tietoa mukanaan lähtiessään yrityksestä?

– Haastateltava A

Tässä luvussa kuvataan riskien lähteenä toimiva insider. Uhkasta pyritään luomaan kuva käsittelemällä sen eri ilmenemismuotoja, tyypillisimpiä tekijäprofiileja, motivaatiotekijöitä ja riskitoimialoja.

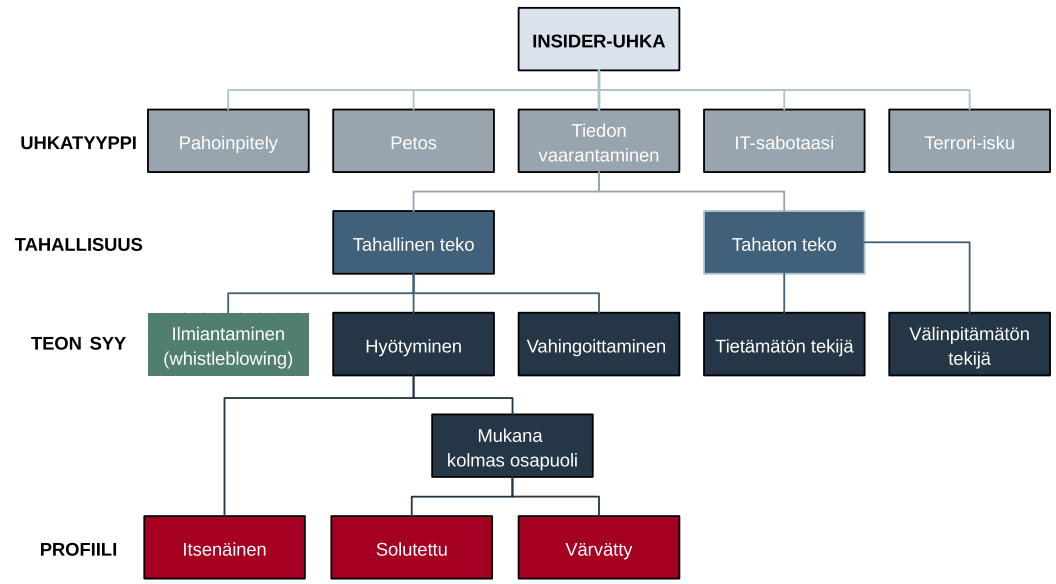
Uhkatyypin, tahallisuuden ja teon syyn rajaus on tärkeää, koska erilaisten insider-uhkatyyppien taustalla olevat motiivit, tekotavat ja ominaisuudet vaihtelevat ja vaikuttavat olennaisesti suunniteltaviin riskienhallintatoimenpiteisiin ja insider-riskien tehokkaaseen arviointiin ja hallintaan (ISO 27005 2013, 8.2.3). Profiilitietojen lisäksi esitellään poliisiasiain tietojärjestelmän tietojen perusteella luotu tilannekuva epäillyistä insider-rikoksista Suomessa.

4.1 Insider-taksonomia ja -uhkan rajaus

Oman henkilöstön aiheuttaman uhkakokonaisuuden moniulotteisuuden takia insider-ilmiötä on luokiteltu eri tavoin kontekstista riippuen. Ainoa kaikkia insider-määritelmiä yhdistävä tekijä on uhkan tuleminen organisaation sisältä. Kuviossa 3 on tätä tutkimusta varten laadittu laaja-alainen insider-uhkien taksonomia, jossa on otettu huomioon tutkimuksissa havaitut eri insider-uhkan ilmenemismuodot, eri tutkijoiden esittämät luokitteluvariaatiot ja tämän tutkimuksen tavoitteet.

Insider-uhkien jako tässä tutkimuksessa mukailee taksonomian ylätasolla uhkatyyppien perusteella Gellesin ym. (2016) ja Cappellin ym. (2012) tekemää insider-uhkien jakoa petoksiin, terroristisiin tekoihin, pahoinpitelyihin, IT-sabotaaseihin ja tiedon vaarantamiseen (2016, 4; 2012, 23-28, 61-62 & 101-104).

Tiedon vaarantamiseen liittyvät uhkat on taksonomian keskitasolla jaettu Cappellin ym. määritelmän mukaisesti tahallisiin (intentional) ja tahattomiin (unintentional) tekoihin.



Kuvio 3: Insider-uhkien taksonomia

Tahattomat teot on edelleen jaettu Gellesin ym. (2016, 4) jaon mukaisesti tietämättömyydestä ja välinpitämättömyydestä johtuviin tekoihin.

Tahalliset teot on jaettu liikesalaisuuslain (2018) mukaisiin ilmiantamiseen liittyviin tekoihin, vahingoittamistarkoituksessa tehtyihin tietovuotoihin sekä hyötymistarkoituksessa tehtyihin Cole & Ringin määrittelemiin itsenäisesti toimiviin ja kolmannen osapuolien ohjaamiin värvättyihin ja solutettuihin insider-uhkiin (2005, 321).

Insider-uhkan yksi ilmenemismuodoista on perinteinen petosrikollisuus. Rikoslain mukaan petoksella tarkoitetaan tekoa, jossa henkilö pyrkii hankkimaan itselleen tai toiselle oikeudetonta taloudellista hyötyä (1889/39, 36.luku 1 §). Weiland ym. (2010) määritelmän mukaan insider-petos voi tarkoittaa esimerkiksi tietojärjestelmään kohdistuvaa tietojen muokkaamista, lisäämistä tai poistamista henkilökohtaisen hyödyn saamiseksi tai tiedon varastamista luottokorttipetosten tai identiteettivarkauksien toteuttamiseksi. Cappellin ym. (2012, 102) tutkimusten mukaan petosrikoksia tekevät insiderit eivät usein toteuta tekoaan yksin, vaan yhteistyössä. Lisäksi useat tutkimuksissa havaituista järjestäytyneeseen rikollisuuteen kytköksissä olevista rikoksista olivat insidereiden toteuttamia petosrikoksia, eivätkä esimerkiksi tietovarkauksia.

Insider-uhka voi ilmetä myös terroritekona. Muun muassa Afganistanin turvallisuusjoukoissa (ANSF) palvelleet poliisit ja sotilaat tekivät vuosina 2011-2012 yhteensä 80 hyökkäystä heidän kanssaan yhteistyössä toimivia monikansallisia kriisinhallintaoperaatiojoukkoja (ISAF) vastaan (Gray & Faiez 2012). Hyökkäysaallon jälkeen ISAF-operaation komentaja totesi, että terroristisessa tarkoituksessa toimivat insiderit ovat yksi Afganistanin operaation merkittävimmistä uhkista (Beaulieu-Hains 2013). Yhdysvaltain puolustusministeriön julkaiseman raportin (Department of Defence 2013, 33) mukaan Afganistanin turvallisuusjoukkojen terroristisessa tarkoituksessa tekemien insider-hyökkäysten merkittävimpänä syynä oli vastapuolella toimivien kapinallisten tai uskonnon vaikutus radikalisoituneihin tekijöihin. Toinen esimerkki terroristisessa tarkoituksessa tehdystä insider-teosta on marraskuussa 2016 uutisoitu tapaus, jossa Saksan turvallisuuspalvelu BfV:n työntekijä oli pidätetty epäiltynä islamistisen terrori-iskun suunnittelusta. Pidätetyn 51-vuotiaan saksalaismiehen tarkoituksena oli järjestää pommi-isku BfV:n päämajassa. (Reuters 2016.)

Työpaikkaväkivaltaa ei tyypillisesti käsitellä insider-uhkana, koska insider-toiminnan on historiallisista syistä usein katsottu liittyvän lähinnä vakoiluun. Työpaikkaväkivalta voidaan kuitenkin nähdä insider-toimintana, joka kohdistuu yrityksen henkilöstöön. Tällöin väkivallantekijänä on yrityksen toinen työntekijä (Gelles ym. 2016, 159). Tilastojen mukaan vuosittain 110 000 – 140 000 henkilöä Suomessa joutuu työssään uhkailun tai fyysisen väkivallan kohteeksi ja työpaikkaväkivallan seurauksena kuolee keskimäärin kaksi henkilö vuodessa (Matson-Mäkelä 2013). Tilastoissa ei kuitenkaan ole eroteltu työpaikalla tapahtuvaa ulkopuolisten tai asiakkaiden tekemää väkivaltaa työntekijöiden kollegoihin kohdistamasta väkivallasta, joten tarkkaa tietoa ilmiön laajuudesta ei ole.

Tiedon käytettävyyteen ja eheyteen liittyvällä **insider-IT-sabotaasilla** tarkoitetaan tekoa, jossa insider käyttää tietotekniikkaa aiheuttaakseen vahinkoa yrityksille tai ihmisille. IT-sabotaaseja on Yhdysvalloissa tehdyissä tutkimuksissa havaittu kaikilla toimialoilla ja niiden aiheuttamat vahingot ovat olleet erittäin merkittäviä yrityksille. Teot ovat usein järjestelmäasiantuntijoiden toteuttamia ja ne on tehty teknisesti vaativilla tavoilla. Yhdessä esimerkkitapauksessa järjestelmäasiantuntijan tehtävissä työskennellyt insider tuhosi 18 kuukauden ajan kerätyn syöpätutkimusaineiston, jota ei ollut varmuuskopioitu. (Cappelli 2012, 23-31.)

4.2 Liikesalaisuuksiin kohdistuvat insider-uhkat

Tietoon kohdistuva insider-uhka on samankaltaisesta määritelmästään huolimatta luokiteltu eri tavalla. Esimerkiksi Kansainvälinen atomienergiajärjestö IAEA luokittelee insider-uhat ainoastaan pääjakona aktiivisiin ja passiivisiin insider-uhkiin (IAEA 2008, 4-5), Blackwell luokittelee insiderit kolmeen kategoriaan ja Cole & Ring viiteen eri kategoriaan (Blackwell 2009, 9-10; Cole & Ring 2005). Naton kyberturvallisuuskeskuksen julkaisemassa tutkimuksessa insider-uhkat on jaettu viiteen eri kategoriaan ja tahalliset tietoon kohdistuvat insider-uhkat tiedon varastamiseen ja vakoiluun liittyviin uhkiin (Kont, Pihelgas, Wojtkowiak, Trinberg, Osula 2015, 3). Blankenship taas käsittelee insider-uhkia kolmesta eri näkökulmasta: tahaton väärinkäyttö, vaarantunut käyttäjätili ja tahallisesti toimiva insider (2016, 2).

Tietoon kohdistuvat insider-uhkat on useissa tutkimuksissa eroteltu teon tahattoman (unintentional) ja tahallisen (malicious) luonteen perusteella (Collins ym. 2016, 3; Gelles 2016, 4-9; Cappelli ym. 2012, xxi).

Cappelli ym. luokittelevat tahattomiin insider-uhkiin tapaukset, joissa insider tarkoittamattaan vaarantaa työnantajansa tiedon luottamuksellisuuden, eheyden tai käytettävyyden. Cappelli ym. mukaan tahattoman insiderin teko voi myös olla seurausta esimerkiksi ulkopuolisen uhkan toteuttamasta sosiaalisesta vaikuttamisesta (social engineering) (2012, xxi). Gelles ym. jakavat tahattoman insider-motiivin vielä kahtia tietämättömiin ja välinpitämättömiin insidereihin. Insiderit, jotka ovat tietämättömiä työnantajansa turvallisuuspolitiikasta ja –ohjeista vaarantavat yrityksen tiedot ulkoisille uhkille, jolloin he ovat uhkana tahattomia, tietämättömiä insidereita.

Insiderit, jotka tuntevat työnantajansa turvallisuuspolitiikan ja –ohjeet, mutta eivät noudata niitä, vaarantavat yrityksen tiedot ulkoisille uhkille, jolloin he ovat uhkana tahattomia, välinpitämättömiä insidereita. (2016, 3-5.) Tutkimusten mukaan huolimattoman toiminnan taustalla voi edellä mainitun mukaisesti olla alhainen tietoturvatietoisuus, asenteelliset ongelmat sekä työtehtävistä johtuvat paineet (Nykänen 2011, 22).

Tahallinen insider-teko voi ilmentyä tässä tutkimuksessa tehdyn rajauksen lisäksi myös yrityksen liiketoiminnan vahingoittamiseen pyrkivänä tietovuotona tai väärinkäytösten ilmiantamiseen pyrkivänä whistleblowingina.

Liiketoiminnan vahingoittamiseen pyrkivä tietovuoto voi olla esimerkiksi yrityksen liikesalaisuudeksi määrittelemien tietojen julkaisemista ilman yrityksen lupaa sen vahingoittamiseksi. Tällaisista teoista on muutama havainto myös poliisiasiain tietojärjestelmiin tehdyissä rekisterihauissa, jotka on esitelty myöhemmin tässä tutkimuksessa. Whistleblowingilla taas tarkoitetaan toimintaa, jossa tekijä paljastaa tietoja työnantajansa väärinkäytöksistä yleiseen tietoon tai viranomaisille, tarkoituksenaan suojata yleistä etua (HE 49/2018, 23; Council of Europe 2014). Teon laillisen luonteen takia whistleblowing on merkitty eri värillä kuvioon 3 erottamaan sen muista insider-uhkista, koska lainsäädännön ja moraalin näkökulmasta kyseessä ei ole insider-uhka.

Tässä tutkimuksessa keskitytään kuvaamaan ja hallitsemaan riskejä, jotka muodostuvat tahallisesta insider-uhkasta, tekojen syynä on tiedon väärinkäytöstä tai vakoilusta hyötyminen ja teot kohdistuvat yritysten liikesalaisuuksiin. Määritelty uhka on lainsäädännön näkökulmasta sekä tiedon oikeudeton hankkiminen että käyttäminen. Nämä insider-profiilit on kuvattu kuviossa 3 punaisella värillä. Insiderilla tarkoitetaan tässä tutkimuksessa organisaation nykyistä tai entistä työntekijää tai harjoittelijaa. (Cappelli ym. 2012, xx; Jackson 2012, 278; Mehan 2016, 11-14; Blackwell 2009, 8; Contos 2006, 51; Cole & Ring 2005, 7.)

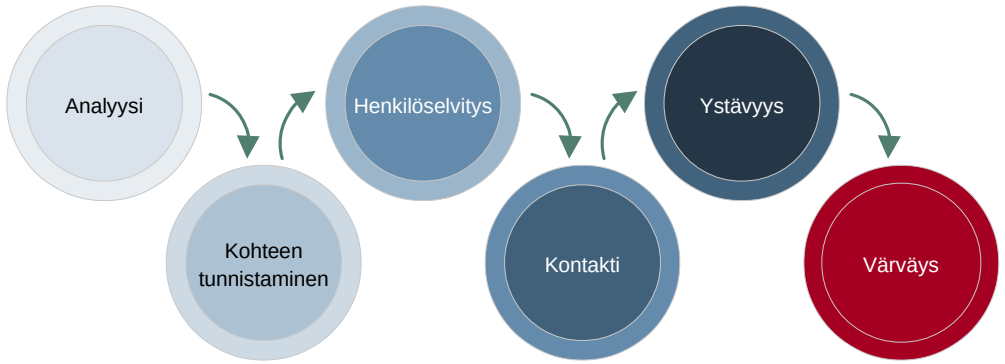
On kuitenkin muistettava, että omien työntekijöiden lisäksi sopimuskumppaneilla saattaa olla samat käyttö- ja pääsyoikeudet tiettyihin tietoihin, kuin omilla työntekijöillä, jolloin myös sopimuskumppanit muodostavat potentiaalisen uhkan (Blankenship 2016, 9). Vaikka tutkimuksessa käytettävä insiderin määritelmä sisältää sopimuskumppanit ja yrityksen entiset työntekijät, kutsutaan insider-tekijöitä yhteisesti työntekijä-käsitteellä, jotta tutkimusteksti pysyy luettavampana ja vältytään toistolta.

CPNI:n tutkimuksessa (2013, 9) 76 % ja Verizonin tutkimuksessa lähes 90 % insidereista toimi itsenäisesti ilman ulkopuolista ohjausta tai tukea. Tämä tutkimus keskittyykin pääosin itsenäisesti toimivien insiderien käsittelyyn.

Itsenäisesti toimivien insidereiden lisäksi tutkimus kohdistuu kahden muun tahallisen insider-profiilin tarkasteluun ja riskien hallintaan, joihin molempiin liittyy kolmas osapuoli ja joita voi olla erityisen vaikea estää ja havaita (Contos 2006, 32). Toinen on työsuhteen aikana yrityksen sisältä värvätty insider, minkä seurauksena luotetusta työntekijästä tulee insider-uhka työnantajalleen. Toinen on yritykseen solutettu insider, jonka tehtävänä on työllistyä kohdeyritykseen ja kerätä tietoa toimeksiantajalleen. Tällaisista kolmannen osapuolen henkilölähteisiin perustuvasta tiedonhankinnasta käytetään tiedustelumaailmassa käsitettä "Human Intelligence", HUMINT (Nato 2017, 57).

Henkilölähteisiin perustuvat operaatiot ovat yleensä pitkäkestoisia ja vaativat usein merkittäviä resursseja tuekseen, joten niiden taustalla on tyypillisesti ulkomainen tiedustelupalvelu tai kilpaileva kansainvälinen suuryritys (Contos 2006, 51). Myös ulkomaisten tiedustelupalvelujen Suomeen kohdistaman toiminnan on havaittu olevan luonteeltaan pitkäkestoista (HaVM 5/2017, 38). Kolmanelle osapuolelle toimivien insider-tekojen aiheuttama vahinko yritykselle on keskimäärin merkittävästi suurempi kuin itsenäisten toimijoiden aiheuttama vahinko. (Cappelli ym.2012, 78.)

CPNI:n tutkimusten (2013) mukaan kolmas osapuoli oli värvännyt 15 % insidereista. Verizonin tutkimuksessa (2017, 48) kolmannelle osapuolelle työskenteleviä värvättyjä ja solutettuja insidereita ei ole eroteltu, mutta niiden yhteinen osuus kaikista havaituista tapauksista oli 7,2 %. Collinsin ym. tutkimuksessa yksilöidyt insiderien rekrytoijat toimivat muun muassa osana järjestäytynyttä rikollisuutta tai ulkomaisissa tiedustelupalveluissa (Collins ym. 2016, 3.) Tiedustelupalvelujen yritysten työntekijöihin kohdistama värväysprosessi voidaan hahmottaa kuvion 4 kautta.



Kuvio 4: Tiedustelupalvelun suorittama insiderin värväysprosessi (mukaillen Suojelupoliisi 2017, 14-15)

Klassinen värväysprosessi (mm. Burkett 2013; Suvorov 1984) on Suojelupoliisin julkaisussa kuvattu kuuden vaiheen kautta, minkä päätteeksi kolmatta osapuolta edustava tiedusteluasiamies pyrkii värväämään kohdehenkilön tiedon välittämisen aloittamiseksi.

1. Prosessin ensimmäisessä vaiheessa tiedustelupalvelu analysoi, minkälaista tietoa se tarvitsee.
2. Analyysin perusteella valitaan kohdeyritys ja tunnistetaan värväyksen kohteeksi valikoituva työntekijä, jolla on hallussa tarvittavat tiedot tai on keino päästä tarvittavaan tietoon käsiksi.

3. Kolmatta vaihetta kutsutaan henkilöselvitykseksi, jossa selvitetään kohdehenkilön vahvuuksia, heikkouksia ja taloudellinen tilanne sekä yksityiselämään liittyviä tietoja, minkä perusteella tiedustelupalvelu arvioi värväyksen onnistumismahdollisuutta ja henkilöön liittyviä haavoittuvuuksia.
4. Selvityksen ja värväyspäätöksen jälkeen tiedustelupalvelu ottaa ensimmäisen kontaktin kohdehenkilöön. Kontaktitilanne suunnitellaan etukäteen ja se voidaan järjestää näyttämään värvättävästä täysin spontaanilta kohtaamiselta.
5. Ensikohtaamisen jälkeen tiedusteluasiamies alkaa rakentaa kohdehenkilöön ystävyyssuhdetta, jonka varjolla kohdehenkilöä totutetaan erilaisten huomiota herättämättömien palvelusten tekemiseen, kuten julkisen tiedon hankkimiseen tiedusteluasiamiehelle. Värväyksen motiivi verhotaan ja kohdehenkilölle uskotellaan, että tiedusteluasiamies pyrkii löytämään esimerkiksi ystävän, asiantuntijan tai auttajan henkilöstä. Ystävyyden kehittäminen ja syventäminen saattaa kestää vuosia ja sen aikana kohdehenkilöä usein palkitaan harmittomista palveluksistaan. Hän saattaa toimia jo tässä vaiheessa insiderina ymmärtämättä sitä itse.
6. Viimeisessä vaiheessa tapahtuu varsinainen värväys. Tiedusteluasiamies pyytää kohdehenkilöä toimittamaan sensitiivisiä tietoja yrityksestään. Tietojen toimittamisen jälkeen kohdehenkilö on värvätty tiedustelupalvelun käyttöön ja häntä voidaan alkaa hyödyntää liikesalaisuustietojen järjestelmälliseksi hankkimiseksi kohdeyrityksestä. (Suojelupoliisi 2017, 14-15.)

On kuitenkin huomioitava, että poikkeuksena normaaliin tiedustelutoimintaan ja värväysprosessiin on se, että insider lähestyy tyypillisesti itse tiedustelupalveluja, jotka ovat kiinnostuneita insiderin toimittamista tiedoista. Insideria ei useissa havaituissa tapauksissa ole tarvinnut värvätä, vaan tekijä on tarjonnut itseään tietolähteeksi (Charney 2010, 50.) Yhdysvaltalaisiin vakoilutapauksiin perustuvan tutkimuksen mukaan ainoastaan 7 % värvätyistä henkilöistä jäi kiinni ennen vahingollisen teon toteuttamista, kun taas oma-aloitteisesti tietoa kolmannelle osapuolelle tarjonneista lähes 40 % jäi kiinni kesken operaation (Fischer 1998). Merkittävä ero voi viitata muun muassa tiedustelupalvelujen värvätyille antamaan koulutukseen, jonka perusteella insiderit ovat pystyneet peittämään jälkensä paremmin.

Kolmannelle osapuolelle toimivien värvättyjen lisäksi CPNI:n tutkimista insidereista 6 % oli solutettu kohdeorganisaatioon suunnitelmallisesti (2013, 9). Kuten aiemmin todettiin, Verizonin tutkimuksessa (2017, 48) kolmannelle osapuolelle toimivia värvättyjä ja solutettuja insidereita ei ole eroteltu, mutta niiden yhteinen osuus kaikista havaituista tapauksista oli 7,2 %.

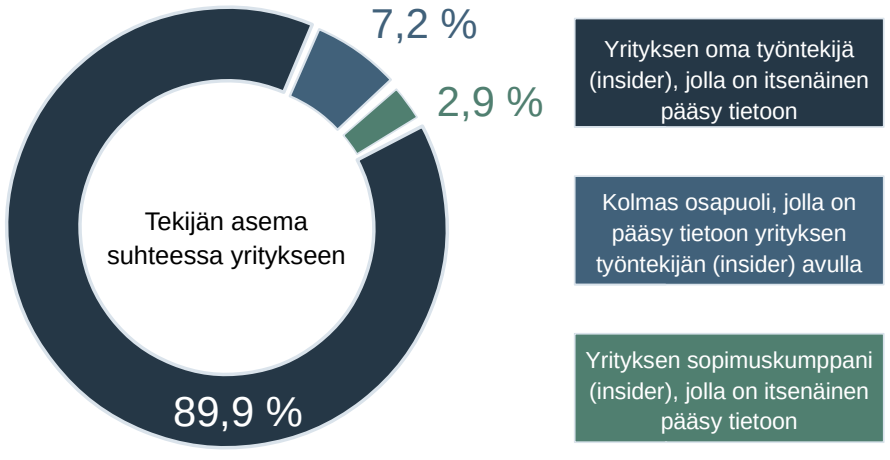
Colwillin mukaan ulkopuoliselle tiedon kerääjälle on huomattavasti kustannustehokkaampaa ja nopeampaa soluttaa insider kohdeyritykseen, kuin käyttää aikaa ja resursseja tiedon hankkimiseen organisaation ulkopuolelta (Colwill 2009, 187). Cole & Ring puhuvat myös kustannustehokkuudesta ja arvioivat, että organisaatioon istutettu kolmesta viiteen vuoteen hiljaiseloa ennen tekoa pitävä insider on sijoituksensa arvoinen ja parempi vaihtoehto, kuin tekijän värvääminen.

Solutettu insider hankkii yrityksen ja ihmisten luottamuksen ja käyttää sitä hyväkseen (Cole & Ring 2005, 324). Hän on usein työnantajan silmin ahkera tekemään työtä, koska ahkera työ edistää yrityksessä etenemistä ja uusien tiedonsaantioikeuksien saamista. Ylennysten johdosta seuraavien uusien tiedonsaanti- ja pääsyoikeuksien lisäksi insider saattaa saada lisää valtaa. Mitä enemmän insiderilla on valtaa, sitä parempi mahdollisuus hänellä on vaikuttaa asioihin omien ja kolmannen osapuolen tavoitteiden palvelemiseksi. (Cole & Ring 2005, 319-320.)

Joissakin havaituissa insider-tapauksissa on myös huomattu, että insider on rekrytoinut yrityksen sisältä muita henkilöitä avustamaan teossa. Tätä tukee myös Cappellin ym. määrittelemä insider-profiili nimeltä ”kunnianhimoinen johtaja (ambitious leader)”, joka toteuttaa tekonsa Colen & Ringin esittämällä tavalla hyödyntämällä muita. ”Kunnianhimoinen johtaja”-profiiliin sopivien kiinnijääneiden insiderien tavoitteena on usein ollut hyödyttää joko oman kilpailevan liiketoiminnan aloittamista tai ulkomaisia tiedustelupalveluja (Cappelli 2012, 78).

Ulkomaisten tiedustelupalvelujen lisäksi juuri kilpailevat yritykset voivat yrittää solutaa omia insider-toimijoitaan kohdeyritykseen (Blackwell 2009, 58-59). Yritysten ja ulkomaisten tiedustelupalveluiden suorittama insider-toiminta eroaa kuitenkin usein merkittävästi toimintatavoiltaan ja taloudellisilta resursseiltaan. Myös riskit ovat erilaiset, koska yritysvakoilua toteuttava yksityinen yritys riskeeraa vähintään maineensa, mutta ulkomaiselle tiedustelupalvelulle insider-toiminnasta kiinnijäämisellä ei välttämättä ole suurempaa merkitystä. (Cole & Ring 2005, 324.)

Kuviossa 5 on esitetty tilasto, jossa vuonna 2017 havaittujen 227:n tiedon väärinkäyttötapauksen tekijän asema suhteessa kohdeyritykseen on määritelty. Suurimmassa osassa tapauksia (89,9 %) tekijä on ollut yrityksen oma työntekijä. Tähän kategoriaan sisältyy tässä tutkimuksessa määritelty itsenäinen toimija. 7,2 % havaituista ja määritellyistä tekijöistä sai tiedon kohdeyrityksessä työskentelevän työntekijän avulla. Tähän kategoriaan sisältyy tässä tutkimuksessa määritellyt värvätty ja solutettu insider. 2,9 % havaituista ja määritellyistä tekijöistä oli yrityksen sopimuskumppaneita, joilla oli itsenäinen pääsy kohdeyrityksen tietoon. (Verizon 2017, 48).



Kuvio 5: Tiedon väärinkäyttäjän asema suhteessa kohdeyritykseen (n=277) (mukaillen Verizon 2017, 48)

Työntekijän aseman lisäksi Taulukossa 3 on kuvattu itsenäisen tekijän ja kolmannelle osapuolelle toimivan värvätyn insiderin profiili, tekijän ammatin, teon aikaikkunan, teon motivaatiotekijöiden, teon toteutustavan ja teon kohteen kautta.

	ITSENÄINEN TOIMIJA	VÄRVÄTTY
TEKIJÄ	Useimmiten tutkija, insinööri, ohjelmoija tai myyjä	Sekä tekniset että ei-tekniset työntekijät
TEON AIKAIKKUNA	Yleensä 60 päivää ennen tai jälkeen työpaikassa lopettamisen	Tapahtuu pitkän ajan kuluessa
		Ensimmäisen teon jälkeen voi kulua pitkä aika ennen seuraavaa tekoa
MOTIVAATIO-TEKIJÄ	Oman kilpailevan toiminnan aloittaminen	Taloudelliset ongelmat tai ahneus
	Uuden työpaikan saaminen	Tyytymättömyys nykyiseen asemaan
		Kolmas osapuoli: Ulkomainen tiedustelupalvelu tai ulkomainen organisaatio (yritys tai rikollisjärjestö)
TEON TOTEUTUS-TAPA	Tiedon siirtäminen pois työpaikalta sähköpostitse, usb-muistivälineellä, paperisina asiakirjoina, jne	Kattaa kaikki toteutustavat
TEON KOHDE	Vie yrityksestä tietoa, jonka kanssa ovat työskennelleet	Vie pyydettyä tietoa yrityksestä, pyrkii peittämään teon jäljet

Taulukko 3: Insider-uhkaprofiilit (mukaillen Kont ym. 2015, 15)

Hyvin harva itsenäisesti toimiva insider vie tietoa organisaatiostaan myydäkseen sen. Sen sijaan insiderit käyttävät tietoa taloudellisen hyödyn saamiseksi sen antaman kilpailuedun turvin. Joko insider vie tiedon mukanaan uuteen työpaikkaan tai perustaa samalla alalla toimivan kilpailevan yrityksen. Useimmiten kilpaileva yritys on perustettu tai uusi työpaikka vastaanotettu jo ennen edelliseltä työnantajalta lähtöä. 40 %:ssä tapauksista tieto päätyy myös ulkomaille (Cappelli ym. 2012, 88).

Toinen Cappellin ym. esiin nostama yleinen väärinymmärrys on, että tietojärjestelmien järjestelmänvalvojat olisivat todennäköisimmin syyllisiä tietovarkauteen. Tosiasiassa tietopääomaan kohdistuvaan oikeudettomaan tiedon hankintaan ja käyttämiseen syyllistyvät useimmiten organisaation nykyiset työntekijät, jotka ovat tutkijoita, insinöörejä, ohjelmoijia tai myyjiä (taulukko 3). (2012, 62-63).

Useimmiten tekijä on mies ja erään tutkimuksen mukaan jopa 96 % insidereista olisi miehiä (Contos 2006, 54). Myös tämän tutkimuksen yhteydessä laaditun tilannekuvan mukaan 91 %:ssa insider-teon merkit täyttävässä yrityssalaisuuden rikkomiseen liittyvässä ilmoituksessa oli yhtenä tai ainoana epäiltynä mies. Cappelli ym. mielestä naisia ei tulisi kuitenkaan täysin sivuuttaa potentiaalisina uhkina (2012, 63). Muun muassa CPNI:n Iso-Britanniassa tilastoimista insidereista (n=120) naistekijöiden osuus oli 18 % (2013, 8).

Insiderin todennäköisin profiili pitää sisällään erilaiset asiantuntija-, tutkija ja myyntitehtävät, mutta ei ole poissuljettua, etteikö myös organisaation johtoon kuuluva henkilö voisi olla potentiaalinen insider (Blankenship 2016, 9).

CPNI:n myös muita insider-riskityyppejä kattavan tutkimusaineiston perusteella 45 % tekijöistä oli johto- tai esimiestason tehtävissä (2013, 8). Toisaalta Verizonin (2016, 36) mukaan tekijän korkea hierarkinen asema yrityksessä korreloi vähemmän teon toteuttamisen kanssa, kuin eri pääsy- ja käyttöoikeuksien laajuus (n=277). Cappellin ym. tutkimuksen perusteella lähes 75 %:lla kiinnijääneistä insidereista (n=496) oli tai oli ollut vakituinen työsuhde organisaatioon, johon tietopääomavarkaus kohdistui (2012, 314). Tämä saattaa ainakin osittain johtua insider-rikosten pitkällä aikajänteellä ja itsenäisesti toimivien insiderien pitkän ajan kuluessa syntyvällä epälojaalisuudella työnantajaa kohtaan.

Erilaisista insider-profiilia haarukoivista tutkimustuloksista huolimatta Cole & Ring esittävät kritiikkiä insider-tekijöiden luokittelusta. Heidän mukaan ei ole olemassa yksiselitteistä insider-profiilia ja tästä syystä tulisi pidättäytyä tekemästä pitkälle vietyjä

johtopäätöksiä ja mahdollisia toimenpiteitä työntekijöiden profiloimisen perusteella (2005, 40) Heidän mukaan insider-uhka tulisi nähdä ainoastaan yhtenä vaihtoehtona, vaikka työntekijään sopisivat useat eri insider-profiiliin viittaavat tekijät (2005, 309).

Cappellin ym. (2012, 61) tutkimustulosten perusteella **tietopääomaan kohdistuva insider-teko** tarkoittaa yleensä seuraavien tietojen viemistä:

- ohjelmat tai lähdekoodit
- liiketoimintasuunnitelmat, tarjoukset ja strategiset suunnitelmat
- asiakastiedot
- tuotetiedot (suunnittelutiedot, kaavat, kaaviot)

Insiderin toteuttamaan tekoon vaikuttaa merkittävästi insiderin edellä käsitelty asema ja toimintamahdollisuudet, koska tekijät kohdistavat yleensä tekonsa helppoihin ja tuttuihin kohteisiin käyttäen hyväkseen heidän nykyisiä tietoja ja taitoja (Blackwell 2009, 22).

Cappelli ym. ovat kuitenkin omassa tutkimuksessaan havainneet, että tahallisesti toimivat tiedon oikeudettomaan hankintaan ja käyttämiseen pyrkivät insiderit voivat valita myös vaikeampia varkauden kohteita, kun taas erityisesti petoksia tekevät insiderit toteuttavat tyypillisemmin taidollisesti ja teknisesti vaatimattomampia tekoja. Tiedon hankintaan pyrkivät insiderit voivat muun muassa käyttää sosiaalisen vaikuttamisen (social engineering) keinoja saadakseen lisää pääsy- ja käyttöoikeuksia tekonsa toteuttamiseksi, koska he tuntevat valmiiksi onnistuneeseen vaikuttamiseen tarvittavat tiedot esimerkiksi työympäristöstä, henkilöstöstä tai sisäisistä termeistä (Contos 2006, 53).

Tietoon kohdistuvia insider-tekoja voi olla erittäin vaikea havaita, koska insiderit vievät yleensä tietoa, johon heillä on olemassa oleva myönnetty käsittelyoikeus ja teko toteutetaan normaalina työaikana. Tästä syystä voi olla vaikeaa erottaa työntekijän perusteltu ja oikeudeton tiedon käsittely. Tutkimustilastojen perusteella useimmat insiderit vievät tietoa työsuhteen lopettamisen yhteydessä. Tämän takia etenkin työntekijöiden siirrettäviin muistivälineisiin, sähköpostiin ja muihin tiedon siirtämiseen soveltuviin keinoihin tulisi kiinnittää tarkempi huomio irtisanomisaikana. (Cappelli ym. 2012, 63-66.)

Cappelli ym. mukaan kolme yleisintä tapaa toteuttaa varkaus on

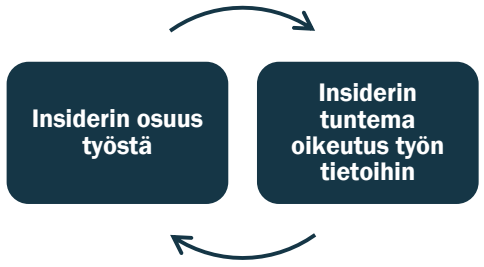
- lähettää tiedot työsähköpostilla ulos yrityksestä
- siirtää tiedot ulos siirrettävällä muistivälineellä
- ottaa etäyhteys yrityksen verkkoon ja toimia fyysisesti yrityksen ulkopuolelta

Amatöörimäisesti toimivat insiderit saattavat lähettää tiedostoja yksityissähköpostiinsa salaamattomana tai salattuna, mutta kolmannen osapuolen kouluttama tai muusta syystä ovelampi insider saattaa esimerkiksi piilottaa tiedostot steganografian keinoin tai kuljettaa ne yrityksestä ulos siirrettävällä muistivälineellä (Jackson 2012, 287-288) tai kamerakännykän muistissa, kuten poliisiasiain tietojärjestelmän perusteella laaditun tilannekuvan yhteydessä havaittiin. On tärkeä huomata, että tiedon fyysinen siirtäminen paperilla oli tekotapana ainoastaan 6 %:ssa (Cappelli ym. 2012, 89-90). Yhdysvalloissa havaituista tekotavoista voikin päätellä, että myös insider-teot ovat siirtyneet vahvasti digiaikaan.

Rikosilmiön digitalisoitumistrendistä huolimatta poliisi tiedotti huhtikuussa 2018 esitutkinnasta, jossa myyntitehtävissä työskennellyttä yrityksen entistä työntekijää epäiltiin yrityssalaisuudeksi luokiteltujen tietojen lähettämisestä postilähetyksenä kilpailevalle yritykselle (Poliisi 2018). Perinteisin menetelmin suoritettavaa tekoa ei siis voi täysin poissulkea insider-riskien arvioinnista.

Kuten aiemmin todettiin, itsenäisesti toimivan insiderin yleisin motiivi on kilpailevan yrityksen perustaminen tai kilpailevaan yritykseen siirtyminen. Tällaisessa tapauksessa tekijä ajattelee varkauden yhteydessä toimivansa kohtuullisesti erityisesti silloin, jos hän on vaikuttanut merkittävästi varastamansa tiedon luomiseen yrityksessä. Cappelli ym. tekemien tapaustutkimusten ja niihin liittyvien haastattelujen perusteella useimmat insiderit kokivat olevansa oikeutettuja viemään tiedon, jonka oikeudettomasta hankkimisesta ja käytöstä heitä epäiltiin. Useimmilla insidereilla oli myös pääsyoikeus tietoon, jonka he varastivat.

Mitä pidempään insiderit olivat työskennelleet tietyn projektin parissa, sitä oikeutetummaksi he kokivat tekonsa ja sitä sitoutuneemmin he työskentelivät projektin parissa. (Cappelli ym. 2012, 70.) Oikeutuksen tunne oli lisäksi erityisen vahva, mikäli insiderin rooli projektin kehitystyössä oli ollut suuri. Tällöin henkilö tunsi omistavansa tiedon tai sen seurauksena syntyneen tuotteen.



Kuvio 6: Insiderin tuntema oikeutus varastamaansa tietoon (mukaillen Cappelli ym. 2012, 70)

Cappelli ym. kuvaa oikeutuksen kasvua yksinkertaisella kuviolla (Kuvio 6), jossa insiderin tuntema oikeutus tietoon kasvaa samalla, kun insiderin osuus tietoon liittyvästä työstä kasvaa.

Työntekijän työssä luoma tieto kuuluu kuitenkin työnantajalle. Joskus yrityksen voi olla vaikea osoittaa, että pois lähteneen työntekijän uuteen työpaikkaan mukanaan viemä tieto on kehitetty edellisellä työnantajalla. Tämä on kuitenkin parhaiten osoitettavissa tarkalla toiminnan dokumentoinnilla. (Vapaavuori 2016, 55-56.)

Myös Moore ym. tutkimusten mukaan 60 % insidereista varasti tietoa, jota he olivat ainakin osittain olleet mukana luomassa (2011, 6). McGuiness esittääkin yhtenä insider-riskien hallintakeinona työkiertoa, jonka seurauksena insider ei tuntisi yhtä suurta omistajuuden tunnetta eri projektien tietoja kohtaan (2001, 6). Yhdysvalloissa on myös havaittu äärimmäisiä tapauksia, joissa työntekijät ovat vilpittömästi luulleet omistavansa tiedon, jonka he ovat työssään luoneet, kuten esimerkiksi asiakastietokannan tai ohjelmiston (Collins ym. 2016, 64).

Insider-tekojen taustalla on usein tarve selvittää tai lievittää henkilökohtaisia tai työhön liittyviä ongelmia. Henkilökohtaiset ongelmat voivat liittyä esimerkiksi avioeroon, päihteiden väärinkäyttöön, taloudellisiin vaikeuksiin tai tunne-elämän häiriöihin. Työhön liittyvät ongelmat voivat taas johtua muun muassa työtyytymättömyydestä, riidoista ja kurinpidollisista sanktioista. Useat havaitut teot ovat olleet seurausta pitkään jatkuneesta tilanteesta ja lopullisen päätöksen tekoon ryhtymisestä on voinut lopulta laukaista hyvinkin merkityksetön tapahtuma. (Blackwell 2009, 22-23.)

Taulukkoon 4 on koottu Blankenshipin (2016) ja Yhdysvaltain kansallisen insider-työryhmän määrittelemiä yleisimpiä motivaatiotekijöitä, jonka vuoksi insider toteuttaa tekonsa.

Tietopääomaan kohdistuvan oikeudettoman hankkimisen motivaationa on yleensä ahneus ja raha riippumatta siitä, toimiiko insider itsenäisesti vai kolmannen osapuolen kanssa. (Herbig 2008; Taylor & Snow 1997, 101-125; Cappelli ym. 2012). Useiden insider-tekojen taustalla ovat olleet taloudelliset ongelmat (Cole & Ring 2005, 11). Toisaalta taloudellinen motiivi on usein ainoastaan välillinen, jolloin ensisijaisena motiivina on aloittaa oma kilpaileva toiminta tiedon avulla. CPNI:n ja Cappellin ym. tutkimustuloksissa myös työtyytymättömyyden on havaittu olevan joko päämotivaation lähde tai tekijä, joka vähentää työntekijän sitoutumista kohdeorganisaatioon ja voi edes auttaa insideriksi ryhtymistä.

MOTIVAATIOTEKIJÄ	SELITE
Taloudelliset vaikeudet	Työntekijä saattaa etsiä nopeita rahanansaitsemiskeinoja helpottaakseen taloudellista ahdinkoaan
Oikeutus	Työntekijä saattaa tuntea luomansa tiedon omakseen
Lomautusilmoitus tai –pelko	Työntekijä saattaa kokea lomautusilmoituksen oikeutuksena teolleen viedä tietoa tai aiheuttaa vahinkoa organisaatiolle
Tyytymättömyys tai kosto	Työntekijä voi tuntea tulleensa esimiehen tai työnantajan puolelta väärin kohdelluksi ja toivoo voivansa kostaa vääryyden. Hän haluaa kostaa organisaatiolle tosiasiallisiin tai oletettuihin tapahtumiin liittyvät teot, kuten tunnustuksen puutteen, tapahtumattomat ylennykset, ristiriidat johdon tai työtovereiden kanssa tai vireillä olevat lomautukset
Työpaikkakonfliktit	Erimielisyydet muiden työntekijöiden kanssa voivat johtaa vahingolliseen toimintaan
Riippuvuudet	Erilaiset riippuvuudet voivat johtaa muun muassa taloudellisiin vaikeuksiin
Ideologia	Poliittinen tai uskonnollinen vakaumus voi motivoida työntekijää vahingolliseen toimintaan
Ego	Kokee olevansa sääntöjen yläpuolella ja on alttiimpi itsetuntoa kohottaville toimille ja vaikuttamiselle
Perheongelmat	Avio-ongelmat tai muut stressitekijät kotona saattavat altistaa työntekijän ulkopuoliselle vaikuttamiselle tai muille ongelmille
Ulkopuolinen vaikuttaminen	Ulkomaiset tiedustelupalvelut tai järjestäytynyt rikollisuus saattavat värvätä työntekijän kiristämällä tai palkitsemisella

Taulukko 4: Insiderin yleiset motivaatiotekijät (mukaillen Blankenship 2016, 4; NITTF 2016, 7)

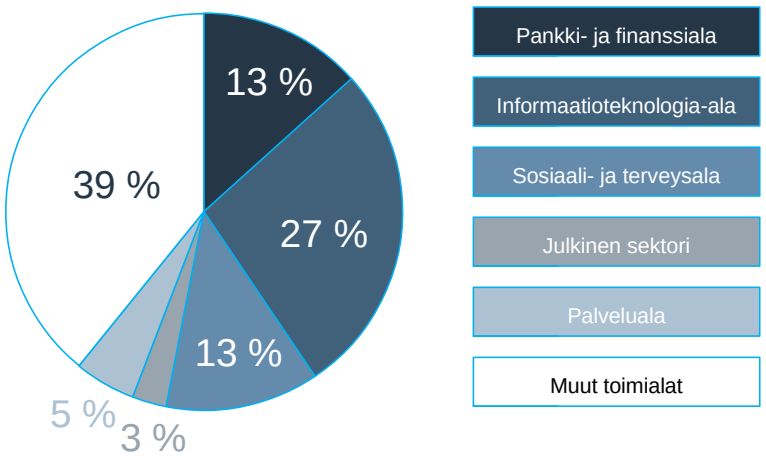
Taloudellisten ja henkilökohtaisten ongelmien aiheuttama inhimillinen haavoittuvuus on realistinen myös Suomessa, sillä maksuhäiriömerkintöjen määrän lisääntyminen on kasvava trendi. Alkuvuodesta 2018 yli 376 000:lla henkilöllä oli luottojen maksuongelmista kertova maksuhäiriömerkintä. Määrän kasvusta kertoo lisäksi trenditieto, jonka mukaan vuosina 2012-2015 maksuhäiriömerkinnän omaavien henkilöiden määrä kasvoi yli 40 000:llä henkilöllä. (Ikävalko 2018; Kauppi 2017, 20.)

Yhtenä merkittävänä motivaatiotekijänä havaittu tyytymättömyys oli myös useissa havaituissa tapauksissa syy hakeutua toiseen organisaatioon töihin. Uuden työpaikan varmistuminen taas nosti halua varastaa tietoa oman työuran ja uuden työnantajan hyväksi. CPNI:n tutkimissa insider-tapauksissa kolmanneksella tekijöistä olikin useampi, kuin yksi motivaation lähde teolle (2013, 4 & 10). Myös useammassa, kuin joka kolmannessa tapauksessa insider vei tietoa varmuuden vuoksi, jos tiedolla olisi myöhemmin merkitystä tekijälle (Cappelli ym. 2012, 72-73.)

Ideologiset syyt olivat päämotivaation lähteenä 40 %:ssa havaituista insider-riskeistä, kuten myös lojaalisuus ystäviä, perhettä tai isänmaata kohtaan. Usein tekojen perusteella lojaalisuus isänmaata kohtaan ylittää lojaaliuden työnantajaa kohtaan. Tätä tukee muun muassa tilastotiedot Yhdysvaltalaisista insider-rikoksista, joiden tekijöillä lähes puolella oli ulkomaan kansalaisuus (Cappelli ym. 2012, 84.) Egoon liittyvä arvostuksen halu oli 22 %:ssa motivaationa lähteenä tekoon.

Herbig (2008) sekä Taylor & Snow (1997) ovat Yhdysvaltain vakoilutapauksia tutkiessaan päätyneet johtopäätökseen, että kiristäminen on vakoiluun syyllistyneiden harvinaisimmista taustasyistä, vaikkakin sillä oli vaikutusta joissakin havaituissa insider-teoissa. Yritykselle erityisen lojaalitkin työntekijät voivat taipua kiristykseen, jos henkilön oma tai läheisten elämä on vaarassa (Cole & Ring 2005, 323). Kiristyksellä saatavien tietojen luotettavuus voidaan kuitenkin usein kyseenalaistaa (Burkett 2013, 11).

Jacksonin mukaan erityisesti motivaatio luo pohjan insider-teoille, joihin jokaiseen liittyy aina harhauttaminen ja petos (2012, 283-290). Toisaalta Cappelli ym. ovat havainneet, että kaikki insiderit eivät ole erityisen huolissaan kiinnijäännistä, eivätkä pyri järjestelmällisesti peittämään jälkiään (2012, 75). Tällaisissa tapauksissa tekijät ovat useimmin toimineet itsenäisesti ilman kolmatta osapuolta.



Kuvio 7: Tietopääomaan kohdistuneiden insider-tekojen jakautuminen eri toimialoille Yhdysvalloissa (mukaillen Software Engineering Institute 2016, 7)

Kuviossa 7 on Yhdysvaltalaisen Carnegie Mellon-yliopiston Software Engineering-instituutin insider-tietokantaan perustuva diagrammi insider-tekojen jakautumisesta eri toimialoille Yhdysvalloissa. Kuviossa on esitetty viisi merkittävintä toimialaa sekä muut toimialat, joissa on havaittu tietopääomaan kohdistunut insider-teko.

Yliopiston keräämän tutkimustiedon perusteella yli neljännes tapauksista tapahtuu IT-sektorilla. Tämän jälkeen eniten havaintoja on pankki- ja finanssialalta sekä sosiaali- ja terveysalalta, molemmista 13 % kaikista havainnoista. Valtion- ja kunnanhallinnossa sekä palvelualoilla oli muutama prosentti havaituista tapauksista ja loput havainnot (39 %) ovat jakautuneet eri toimialoille. Sosiaali- ja terveysala sekä julkishallinto on erotettu omiksi sektoreikseen yhdysvaltalaisen alkuperäisjaottelun perusteella. Toimialajakauma on hyvin samankaltainen Cappellin ym. vuonna 2012 julkaiseman tutkimustiedon kanssa (2012, 311).

Suomen poliisiasiain tietojärjestelmään tehtyjen hakujen perusteella vuosien 2012-2016 aikana havaitut insider-tapaukset jakautuvat hyvin eri toimialoille, eivätkä tapaukset painottuneet tietyille toimialoille, kuten Carnegie Mellon-yliopiston aineistossa.

4.3 Liikesalaisuuksiin kohdistuvien insider-rikosten tilannekuva Suomessa

Taulukossa 5 on esitetty liikesalaisuuksiin (yrityssalaisuuksiin) kohdistuvien insider-rikosriskien tilannekuva Suomessa vuosina 2012-2016. Tilannekuva perustuu poliisin tietoon tulleisiin rikosepäilyihin niistä elinkeinoelämään kohdistuvista rikoksista, joissa teko voi sisältää yritysten liikesalaisuustiedon väärinkäyttöä. Varsinaisen tilannekuvan lisäksi selvitettiin mahdollisina yrityssalaisuuden väärinkäytön esirikoksina toimivien rikoslain 24.luvun salakuuntelua ja salakuuntelun yritystä sekä 38.luvun tieto- ja viestintärikoksiin kuuluvien salassapitorikoksia ja –rikkomuksia koskevien rikosten insider-havaintojen osuus (Taulukko 6).

Poliisiasiain tietojärjestelmään tehtyjen hakujen yleisinä rajauksina ovat olleet seuraavat tekijät:

- rikosten epäilty alkamisaika on ollut aikavälillä 1.1.2012 – 31.12.2016
- tilannekuvasta on rajattu pois manner-Suomen ulkopuolella tapahtuneeksi ilmoitetut rikokset
- tilannekuvassa ei ole huomioitu poliisin, syyttäjän tai tuomioistuimen ratkaisuja ilmoituksiin liittyen, koska tilannekuvassa on haluttu esittää poliisin tietoon tulleiden insider-havaintojen määrä

RIKOSLAJI / VIITE (39/1889)	RIKOSNIMIKE	RIKOSILM. MÄÄRÄ 2012-2016	INSIDER-TUNNUS-MERKIT	Mies %	Nainen %	teknin en	ei-teknin en
YRITYS-SALAISUUS-RIKOKSET RL 30.luku	Yritysvakoilu	13*	9	100 %	0%	0	9
	Yritysvakoilun yritys	2	0	-	-	-	-
	Yrityssalaisuuden rikkominen	168**	136	73%	27%	2	134
	Yrityssalaisuuden rikkomisen yritys	4	4	100 %	0%	0	4
	Yrityssalaisuuden väärinkäyttö	3***	3	100 %	0%	0	3
VUOSINA 2012-2016 EPÄILTYJÄ INSIDER-RIKOKSIA YHTEENSÄ:			152	91 %	9 %	2	150

Taulukko 5: Vuosina 2012-2016 Poliisin tietoon tulleet liikesalaisuuksiin kohdistuneet epäillyt insider-rikokset ja tekijätiedot rikosnimikeittäin

RIKOSLAJI / VIITE (39/1889)	RIKOSNIMIKE	RIKOSILM. MÄÄRÄ 2012-2016	INSIDER-TUNNUS-MERKIT	Mies %	Nainen %	tekni -nen	ei-tekni -nen
YKSITYISYYTTÄ, RAUHAA JA KUNNIAA LOUKKAAVAT RIKOKSET RL 24.luku	Salakuuntelu	69	0	-	-	-	-
	Salakuuntelun yritys	2	0	-	-	-	-
TIETO- JA VIESTINTÄ-RIKOKSET RL 38.luku	Salassapitorikos	135	4	50%	50%	0	4
	Salassapito-rikkomus	51	0	-	-	-	-

Taulukko 6: Vuosina 2012-2016 Poliisin tietoon tulleet yrityssalaisuuden väärinkäytön mahdolliset esirikokset sekä niihin liittyvät epäillyt insider-rikokset ja tekijätiedot rikosnimikkeittäin

- tilannekuvassa on huomioitu samaan rikokseen liitetyt eri rikosnimikkeet, jotka aiheuttavat päällekkäisyyttä. Tästä on tehty huomiomerkintä taulukkoon 5 "*", "**" tai "***" ilmoitusten kokonaismäärästä kertovan lukuarvon yhteyteen:
  * kaksi rikosilmoitusta samasta tapauksesta. Insider-rikosten määrä on laskettu yhden rikosilmoituksen perusteella
  ** kokonaisluvusta (170 kpl) on poistettu kaksi (2 kpl) rikosilmoitusta, jotka ovat jo osa yritysvakoilua koskevia rikosilmoituksia (13 kpl)
  *** kokonaisluvusta (36 kpl) on poistettu 33 kpl rikosilmoituksia, jotka ovat jo osana joko yritysvakoilua (13 kpl) tai yrityssalaisuuden rikkomista (168 kpl) koskevia rikosilmoituksia

Insider-tunnusmerkkien määrittelynä (neljäs sarake vasemmalta) on käytetty seuraavia rajauksia:

- rikosilmoituksessa mainittu epäilty on henkilö, jolla on asemansa puolesta sisäistä tietoa yrityksestä ja voi olla organisaation nykyinen tai entinen työntekijä, harjoittelija tai sopimuskumppani
- epäillyn insider-rikoksen kohteena ollut tieto on suojattu yrityksen, ei yksityishenkilön edun vuoksi
- epäillyn insider-rikoksen ilmeisenä tavoitteena on ollut tiedon hyödyntäminen omaksi tai muiden hyödyksi, ei kohteena olevan yrityksen haitaksi tai väärinkäytösten paljastamiseksi

Taulukon 5 ja 6 ensimmäisessä sarakkeessa vasemmalta on ilmaistu rikoslain (39/1889) luku ja otsikko, johon siihen liitetyt rikosnimikkeet seuraavasta sarakkeesta liittyvät. Toisessa sarakkeessa on ilmoitettu teon rikosnimike. Kolmanteen sarakkeeseen on merkitty, montako ilmoitusta poliisiasiain tietojärjestelmään on tehty käyttämällä rekisterihakusanana toisessa sarakkeessa ilmoitettua rikosnimikettä. Neljäs sarake on tämän tutkimuksen kannalta merkittävin, sillä siinä on ilmaistu, monenko ilmoituksen sisällössä kuvattu tekotapa ja olosuhteet viittaavat edellä määriteltyyn insider-toimintaan. Viidenteen sarakkeeseen on merkitty miesten prosenttiosuus niistä ilmoituksista, joiden on arvioitu täyttäneen tämän tutkimuksen insider-rikoksen tunnusmerkit. Kuudennessa sarakkeessa on vastaavasti merkitty naisten prosenttiosuus ilmoituksista. Rikoksesta epäiltyjä saattoi olla useampi henkilö rikosilmoitusta kohden, joten samassa ilmoituksessa saattoi olla epäiltynä sekä naisia että miehiä. Tästä syystä naisten ja miesten osuus on kerrottu prosenttilukuna, jolloin on mahdollista kertoa molempien sukupuolten osuus kaikissa tässä tilannekuvassa määritellyissä insider-rikoksissa. Seitsemännessä sarakkeessa on niiden rikosilmoitusten lukumäärä, jotka on määritelty insider-toiminnaksi ja

joissa tekijä tai tekijät ovat olleet tietojärjestelmien järjestelmänvalvojan tehtävissä, vastaavissa tehtävissä, tai teossa on käytetty erityistä teknistä osaamista tietojen saamiseksi tai viemiseksi pois yrityksestä. Kahdeksannessa sarakkeessa on niiden rikosilmoitusten lukumäärä, jotka on määritelty insider-toiminnaksi ja joissa tekijä tai tekijät eivät ole olleet tietojärjestelmien järjestelmänvalvojan tehtävissä, sitä vastaavissa tehtävissä, tai teossa ei ole käytetty erityistä teknistä osaamista tietojen varastamiseksi yrityksestä. Taulukon 5 viimeisellä rivillä on ilmoitettu insider-rikoksia koskevat yhteenlasketut tiedot kaikista sarakkeista. On tärkeä huomata, että insider-teon tunnusmerkit täyttävien tekojen kokonaismäärä (152) on eri, kuin insider-tekijöiden kokonaismäärä, koska joistakin insider-tunnusmerkit täyttävistä teoista epäillään useita henkilöitä yhtäaikaisesti joko erikseen tai yhteistyössä tehdystä teosta.

Tilannekuva ja ilmoitustiedoista tehdyt tärkeimmät johtopäätökset on käsitelty seuraavaksi rikosnimikkeittäin:

YRITYSSALAISUUSRIKOKSET

RIKOSNIMIKE	RIKOSILM. MÄÄRÄ 2012-2016	INSIDEREITA	Mies %	Nainen %	tekninen	ei-tekninen
Yritysvakoilu	13*	9	100%	0%	0	9
Yritysvakoilun yritys	2	0	-	-	-	-

Yrityssalaisuusrikokset on määritelty rikoslain 30. luvussa. Näistä rikoksista tilannekuvaan on valittu viisi rikosnimikettä: yritysvakoilu, yritysvakoilun yritys, yrityssalaisuuden rikkominen, yrityssalaisuuden rikkomisen yritys ja yrityssalaisuuden väärinkäyttö. Rikoslain mukaiset yrityssalaisuusrikokset ovat tilannekuvan keskiössä, koska ainoastaan rikoslaki antaa yrityssalaisuuksille suojan työsuhteen päättymisen jälkeiselle ajalle (Vapaavuori 2016, 57).

Yrityssalaisuusrikoksiin kuuluva yritysvakoilu ja sen yritys on määritelty laissa (39/1889, 30. luku) seuraavasti:

4 § Yritysvakoilu

Joka oikeudettomasti hankkii tiedon toiselle kuuluvasta yrityssalaisuudesta 1) tunkeutumalla ulkopuolisilta suljettuun paikkaan taikka ulkopuolisilta suojattuun tietojärjestelmään, 2) hankkimalla haltuunsa tai jäljentämällä asiakirjan tai muun tallenteen taikka muulla siihen rinnastettavalla tavalla tai 3) käyttämällä teknistä erikoislaitetta tarkoituksin oikeudettomasti ilmaista tällainen salaisuus tai oikeudettomasti käyttää sitä, on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa rangaistusta, yritysvakoilusta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Yritys on rangaistava.

Yritysvakoiluepäilyksiä ja rikoksen yrityksiä on ilmoitettu yhteensä 15* vuosina 2012-2016. Näistä epäillyistä rikoksista 9 täyttää tässä tutkimuksessa käytetyn insider-teon tunnusmerkit.

Kaikki epäillyt insiderit ovat miehiä ja yhdessäkään tapauksessa tekijän tai tekijöiden ei havaittu olleen tietojärjestelmien järjestelmänvalvojan tehtävissä, sitä vastaavissa tehtävissä, tai rikoksen teossa ei havaittu käytetyn erityistä teknistä osaamista tietojen varastamiseksi yrityksestä.

Useissa epäillyissä insider-rikoksissa ilmeisenä tarkoituksena on ollut kopioida yrityksen tietoja oman samalle toimialalle perustettavan kilpailevan yrityksen käyttöön. Useissa epäillyissä tapauksissa insider-riskeihin liittyvänä haavoittuvuutena tunnistettiin tekijän liian laajat tiedonsaantioikeudet (need-to-know) ja pääsy- ja käyttöoikeudet, jotka ovat mahdollistaneet tiedon oikeudettoman hankkimisen yrityksestä.

RIKOSNIMIKE	RIKOSILM. MÄÄRÄ 2012-2016	INSIDEREITA	Mies %	Nainen %	tekninen	ei-tekninen
Yritys-salaisuuden rikkominen	168**	136	73%	27%	2	134
Yritys-salaisuuden rikkomisen yritys	4	4	100%	0%	0	4

Yrityssalaisuusrikoksiin kuuluva yrityssalaisuuden rikkominen ja sen yritys on määritelty laissa (39/1889, 30. luku) seuraavasti:

5 § Yrityssalaisuuden rikkominen

Joka hankkiakseen itselleen tai toiselle taloudellista hyötyä tai toista vahingoittaakseen oikeudettomasti ilmaisee toiselle kuuluvan yrityssalaisuuden tai oikeudettomasti käyttää tällaista yrityssalaisuutta, jonka hän on saanut tietoonsa 1) ollessaan toisen palveluksessa, 2) toimiessaan yhteisön tai säätiön hallintoneuvoston tai hallituksen jäsenenä, toimitusjohtajana, tilintarkastajana tai selvitysmiehenä taikka niihin

rinnastettavassa tehtävässä, 3) suorittaessaan tehtävää toisen puolesta tai muuten luottamuksellisessa liikesuhteessa tai 4) yrityksen saneerausmenettelyn yhteydessä, on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa rangaistusta, yrityssalaisuuden rikkomisesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Tämä pykälä ei koske tekoa, johon 1 momentin 1 kohdassa tarkoitettu on ryhtynyt kahden vuoden kuluttua palvelusaikansa päättymisestä. Yritys on rangaistava.

Yrityssalaisuuden rikkomiseen ja rikoksen yritykseen liittyviä epäilyjä on ilmoitettu yhteensä 168** vuosina 2012-2016. Näistä epäillyistä rikoksista 136 täyttää tässä tutkimuksessa käytetyn insider-teon tunnusmerkit.

Noin kolmessa neljäsosassa epäillyistä insider-rikoksista osallisena oli miehiä. Ainoastaan kahdessa epäillyssä rikoksessa tekijä tai tekijät ovat olleet tietojärjestelmien järjestelmänvalvojan tehtävissä, vastaavissa tehtävissä, tai rikoksen teossa on käytetty erityistä teknistä osaamista tietojen saamiseksi tai viemiseksi pois yrityksestä.

Useissa epäillyissä insider-rikoksissa tekijä oli kopioinut yrityksen asiakasrekisteritietoja tai muita liikesalaisuuksien piiriin kuuluvia tietoja, irtisanoutunut ja aloittanut työsuhteen kilpailevassa yrityksessä. Tiedon siirtoon oli käytetty muun muassa ulkoisia kovalevyjä tai matkapuhelimen muistia. Yrityssalaisuuden rikkomiseen liittyviä epäiltyjä insider-rikoksia tarkastellessa havaittiin, että Neuvostoliitossa syntyneiden epäiltyjen osuus on suurempi verrattuna muihin kuin Suomen kansalaisiin. Epäiltyjen insiderien toiminta- ja tekotapaan liittyen myös Saario & Vesterinen laatimassa selvityksessä 10 % vastanneista ilmoitti yrityksen havainneen tietojen luvatonta kopiointia ennen työntekijän siirtymistä pois yrityksen palveluksesta (2017, 21).

RIKOSNIMIKE	RIKOSILM. MÄÄRÄ 2012-2016	INSIDEREITA	Mies %	Nainen %	tekninen	ei-tekninen
Yritys-salaisuuden väärinkäyttö	3***	3	100%	0%	0	3

Yrityssalaisuusrikoksiin kuuluva yrityssalaisuuden väärinkäyttö on määritelty laissa (39/1889, 30. luku) seuraavasti:

6 § Yrityssalaisuuden väärinkäyttö

Joka oikeudettomasti 1) käyttää tässä laissa rangaistavaksi säädetyllä teolla tietoon saatua tai ilmaistua toiselle kuuluvaa yrityssalaisuutta elinkeinotoiminnassa taikka 2) hankkiakseen itselleen tai toiselle taloudellista hyötyä ilmaisee tällaisen salaisuuden, on tuomittava yrityssalaisuuden väärinkäytöstä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yrityssalaisuuden väärinkäyttöön liittyviä epäiltyjä rikoksia on ilmoitettu yhteensä kolme*** vuosina 2012-2016. Kaikki kolme epäiltyä rikosta täyttävät tässä tutkimuksessa käytetyn insider-teon tunnusmerkit.

Kaikissa epäillyissä rikoksissa osallisena oli ainoastaan miehiä. Yhdessäkään epäillyssä rikoksessa tekijän tai tekijöiden ei havaittu olleen tietojärjestelmien järjestelmänvalvojan tehtävissä, sitä vastaavissa tehtävissä, tai rikoksen teossa ei havaittu käytetyn erityistä teknistä osaamista tietojen varastamiseksi yrityksestä. Epäiltyjen insider-rikosten vähäisen määrän takia tekotavoista ei ole tehty yhteenvetoa tai johtopäätöksiä.

ESIRIKOKSET: YKSITYISYYTTÄ, RAUHAA JA KUNNIAA LOUKKAAVAT RIKOKSET

RIKOSNIMIKE	RIKOSILM. MÄÄRÄ 2012-2016	INSIDEREITA	Mies %	Nainen %	tekninen	ei-tekninen
Salakuuntelu	69	0	-	-	-	-
Salakuuntelun yritys	2	0	-	-	-	-

Rikoslain 24. luvussa on määritelty yksityisyyttä, rauhaa ja kunniaa loukkaavat rikokset. Näistä rikoksista tilannekuvaan on valittu kaksi rikosnimikettä: salakuuntelu ja salakuuntelun yritys. Vaikkakin 24. luvun rikosnimikkeet liittyvät lähtökohtaisesti ihmisten yksityiselämään liittyvään toimintaan ja tietoihin, salakuuntelu ja sen yritys voivat toimia yrityssalaisuuden väärinkäytön esirikoksina (Vapaavuori 2016, 153–154). Salakuuntelu ja sen yritys on määritelty laissa (39/1889, 24.luku) seuraavasti:

5 § Salakuuntelu

Joka oikeudettomasti teknisellä laitteella kuuntelee tai tallentaa 1) keskustelua, puhetta tai yksityiselämästä aiheutuvaa muuta ääntä, jota ei ole tarkoitettu hänen tietoonsa ja joka tapahtuu tai syntyy kotirauhan suojaamassa paikassa, taikka 2) muualla kuin kotirauhan suojaamassa paikassa salaa puhetta, jota ei ole tarkoitettu hänen eikä muunkaan ulkopuolisen tietoon, sellaisissa olosuhteissa, joissa puhujalla ei ole syytä olettaa ulkopuolisen kuulevan hänen puhettaan, on tuomittava salakuuntelusta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Yritys on rangaistava.

Salakuunteluepäilyksiä ja rikoksen yrityksiä on ilmoitettu yhteensä 71 vuosina 2012-2016.

Näistä epäillyistä rikoksista yksikään ei täytä tässä tutkimuksessa käytetyn insider-teon tunnusmerkkejä. Lähes kaikki epäillyt rikokset liittyivät perheiden sisäisiin riitoihin ja niihin liittyviin salakuunteluepäilyihin. Ilmoituksissa havaittiin kuitenkin myös tekotapoja, joissa nauhuri tai matkapuhelin oli kätketty jonkin organisaation toimitiloihin salakuuntelua varten, vaikkakaan teot eivät kohdistuneet organisaation tietoon.

Ilmoitusten joukossa oli myös epäiltyjä rikoksia, joissa yksityishenkilöt olivat asentaneet vakoiluohjelman matkapuhelimeen läheistensä vakoilemiseksi. Havaituilla rikoksilla ei ollut liittymäpintaa tämän tutkimuksen insider-riskien kanssa, mutta edellä mainitut tekotapakuvaukset osoittavat, että tiedustelu- ja turvallisuusviranomaisten lisäksi myös yksityishenkilöt pystyvät halutessaan käyttämään tekniikkaa onnistuneesti hyväkseen salakuuntelun toteuttamiseksi.

Ilmoitustietojen laadullisen tarkastelun perusteella voidaan päätellä, että rikoslaissa säädetyt ja tutkimuksen yhteydessä tarkastellut salakuuntelu- ja yritystapaukset eivät liity tutkimuksessa määriteltyihin insider-rikoksiin ja riskeihin.

ESIRIKOKSET: TIETO- JA VIESTINTÄRIKOKSET

RIKOSNIMIKE	RIKOSILM. MÄÄRÄ 2012-2016	INSIDEREITA	Mies %	Nainen %	tekninen	ei-tekninen
Salassapito-rikos	135	4	50%	50%	0	4
Salassapito-rikkomus	51	0	-	-	-	-

Rikoslain 38. luvussa on määritelty tieto- ja viestintärikokset. Näistä rikoksista tilannekuvaan on valittu kaksi rikosnimikettä: salassapitorikos ja salassapitorikkomus. Vaikkakin edellä mainitut 38. luvun rikosnimikkeet liittyvät lähtökohtaisesti muiden, kuin liikesalaisuustietojen väärinkäyttöön, salassapitorikos ja –rikkomus voivat myös toimia yrityssalaisuuden väärinkäytön esirikoksina. Salassapitorikos ja salassapitorikkomus on määritelty laissa (39/1889, 38. luku) seuraavasti:

1 § Salassapitorikos

Joka laissa tai asetuksessa säädetyn taikka viranomaisen lain nojalla erikseen määräämän salassapitovelvollisuuden vastaisesti 1) paljastaa salassa pidettävän seikan, josta hän on asemassaan, toimessaan tai tehtävää suorittaessaan saanut tiedon, taikka 2) käyttää tällaista salaisuutta omaksi tai toisen hyödyksi, on tuomittava, jollei teko ole rangaistava 40 luvun 5 §:n mukaan, salassapitorikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

2 § Salassapitorikkomus

Jos salassapitorikos, huomioon ottaen teon merkitys yksityisyyden tai luottamuksellisuuden suojan kannalta taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava salassapitorikkomuksesta sakkoon. Salassapitorikkomuksesta tuomitaan myös se, joka on syyllistynyt sellaiseen 1 §:ssä tarkoitettuun salassapitovelvollisuuden rikkomiseen, joka on erikseen säädetty salassapitorikkomuksena rangaistavaksi.

Salassapitorikokseen ja salassapitorikkomukseen liittyviä rikosepäilyjä on ilmoitettu yhteensä 186 vuosina 2012-2016. Näistä epäillyistä rikoksista neljä täyttää tässä tutkimuksessa käytetyn insider-teon tunnusmerkit.

Insider-rikosepäilyt jakautuivat sukupuolten välillä tasan. Yhdessäkään rikoksessa tekijän tai tekijöiden ei havaittu olleen tietojärjestelmien järjestelmänvalvojan tehtävissä, sitä vastaavissa tehtävissä, tai rikoksen teossa ei havaittu käytetyn erityistä teknistä osaamista tietojen varastamiseksi yrityksestä. Epäiltyjen insider-rikosten vähäisen määrän takia tekotavoista ei ole tehty yhteenvetoa tai johtopäätöksiä.

Tilannekuvaan liittymättömänä sivuhuomiona todettakoon, että suurin osa salassapitorikoksia ja –rikkomuksia koskevista rikosilmoituksista liittyi sosiaali- ja terveysalalla työskentelevien henkilöiden epäiltyyn henkilötietoihin kohdistuvaan urkintaan tai levittämiseen.

Yhdysvalloissa tehdyt havainnot sosiaali- ja terveysalalta ovat samansuuntaisia ja vuoden 2017 tietoturvapoikkeamia käsittelevässä raportissa lähes puolessa tilastoiduista tietojen väärinkäytöstapauksista tekijän motiivina ei ollut tiedon hyödyntäminen tai kohteen vahingoittaminen vaan hupi ("fun"). Toisaalta samoja henkilötietoja käytettiin Yhdysvalloissa myös taloudellisen hyödyn saamiseksi muun muassa identiteettivarkauksien muodossa, joten tiedon väärinkäytöstapaukset sosiaali- ja terveysalalla eivät johtuneet ainoastaan uteliaisuudesta (Verizon 2017, 22 & 48).

Ilmoitustietojen laadullisen tarkastelun perusteella voidaan päätellä, että rikoslaissa säädetyt ja tutkimuksen yhteydessä tarkastellut salassapitorikos- ja salassapitorikkomustapaukset eivät liity tässä tutkimuksessa määriteltyihin insider-rikoksiin ja riskeihin.

TILANNEKUVAN JOHTOPÄÄTÖKSET

Tilannekuvan perusteella vuosina 2012-2016 on epäilty yhteensä 152:ta insider-rikosta.

Tapauksista suurinta osaa (136) on tutkittu yrityssalaisuuden rikkomisena. Kaikista epäillyistä liikesalaisuuksiin kohdistuvista insider-rikoksista 91 %:ssa tekijä tai yksi tekijöistä oli mies ja 9 %:ssa tekijä tai yksi tekijöistä oli nainen. Kaikista epäillyistä insider-rikoksista ainoastaan kahdessa rikosilmoituksessa tekijät toimivat tietojärjestelmien järjestelmänvalvojan tehtävissä, sitä vastaavissa tehtävissä, tai teoissa käytettiin erityistä teknistä osaamista tietojen varastamiseksi yrityksestä. Tilannekuvan perusteella ei havaittu yhtään toimialaa, johon epäillyt insider-rikokset olisivat erityisesti kohdistuneet, vaan teot jakautuivat tasaisesti eri toimialoille. Useissa epäillyissä insider-rikoksissa teon tavoitteena oli liikesalaisuustiedon hyödyntäminen oman tai toisen kilpailevan yrityksen toiminnassa.

Vuosittaisia ilmoitusmääriä koskevien tilannekuvatietojen perusteella rikosilmoitusten määrät jakautuivat tasaisesti kaikille tarkasteluvuosille 2012-2016 lukuun ottamatta viimeisiä tarkasteluvuosia 2015-2016, joihin kohdentui vähemmän epäiltyjä rikoksia.

Rikosilmoitukset poliisiasiain tietojärjestelmässä on kirjattu sille päivämäärälle, jolloin teon toteuttaminen on alkanut. Tekojen ilmoitusajaksi on joissakin tapauksissa merkitty useamman vuoden ajanjakso, joten tästä syystä viiden vuoden otannan viimeisille tarkasteluvuosille (2015 ja 2016) on luultavasti vähemmän merkittyjä ilmoituksia. Näille vuosille sijoittuvien epäiltyjen insider-rikosten todellinen määrä selviää otannan perusteella vasta muutaman vuoden kuluttua.

Poliisin tietoon tulleiden insider-rikosten määrään saattaa vaikuttaa se, että yritykset pyrkivät välttämään maineriskejä ja jättävät sen takia ilmoittamatta poliisille epäillyistä rikoksista. Esimerkiksi Allianzin (2018, 5) tekemän laajan kyselyn perusteella maineriskit ovat yritysjohtajien ja riskienhallinnan asiantuntijoiden mielestä kymmenen merkittävimmän liiketoimintariskin joukossa vuonna 2018. Yhdysvaltalaisyliopiston vuonna 2014 julkaiseman eri yritys- ja viranomaislähteistä koostaman tilaston perusteella 75 % Yhdysvalloissa tapahtuneista insider-teoista käsiteltiin organisaatioiden sisäisesti (Carnegie Mellon University 2014, 7). Lisäksi Cappellin ym. samansuuntaisen vuonna 2011 laaditun tilaston mukaan ainoastaan 11 % tapauksista ilmoitettiin poliisille tai niistä nostettiin kanne (2012, 322-323.) Ulkopuolisten tekemät teot tulevatkin helpommin julkiseksi ja organisaatioiden on myös vaikeampi kiistää niitä (Cole & Ring 2005, 8 & 19).

Poliisin tietoon tulleiden insider-epäilyjen vähäinen määrä verrattuna yritysten omiin ilmoituksiin (Keskuskauppakamarin ja Helsingin seudun kauppakamarin kyselytutkimukset 2012-2017) Suomessa saattaa johtua myös yritysten salassapitosopimuksiin mahdollisesti kirjattavasta välityslausekkeesta, jonka perusteella salassapidon rikkomista koskevat riidat käsitellään välimiesoikeudessa (Huhtamäki 2014, 241). Tällaiset tapaukset, niiden osapuolet ja lopputulos eivät ole julkisia, eivätkä ne lähtökohtaisesti tule poliisin tietoon. Toisaalta myöskään muut siviiliasioina tuomioistuimissa käsitellyt liikesalaisuusloukkaukset eivät suoraan tule poliisin tietoon, vaikka ne ovatkin julkista tietoa. Esimerkiksi työsuhteen päättämisen yhteydessä on voitu vedota myös liikesalaisuuden oikeudettomaan käyttämiseen ja markkinaoikeudessa on voitu käsitellä sopimattomasta menettelystä elinkeinotoiminnassa annetun lain (1061/1978) alle kuuluvia liikesalaisuusasioita.

Tilannekuvatiedoissa on myös useita epäiltyjä insider-rikoksia, joissa asianomistajayritys on pyytänyt poliisia päättämään esitutkinnan, mikä voi viitata muun muassa välimiesoikeuden käyttöön tai epäillyn kanssa päästyyn sovintoon. Riippumatta välimiesoikeudessa käsiteltyjen insider-rikosten määrästä, yritysten omia havaintoja ja poliisin tietoon tulleita insider-ilmoituksia vertaamalla voi päätellä, että liikesalaisuustietoihin kohdistuva insider-toiminta on piilorikollisuutta. Piilorikollisuudella tarkoitetaan rikollista toimintaa, ”joka ei tule poliisin tietoon ja jota siten ei rikoksena rekisteröidä” (Tilastokeskus 2017). Tilannekuvassa käsitellyt yrityssalaisuusrikokset ovat lisäksi asianomistajarikoksia, joten poliisi ei oma-aloitteisesti lähde tutkimaan epäilyjä.

Sekä poliisin tietoon tulleiden että havaittujen, mutta ilmoittamatta jätettyjen epäiltyjen insider-rikosten lisäksi osa tekonsa toteuttaneista insidereista on pystynyt toimimaan onnistuneesti eikä ole koskaan jäänyt kiinni (Cole & Ring 2005, 314). Yhdysvaltalaisten tiedusteluanalyytikoiden arvion mukaan noin kolme neljästä insider-teosta jäisi kokonaan ilmoittamatta tai havaitsematta (NITTF 2016, 6). Toiminnan piilorikollisuuteen viittaavan luonteen vuoksi tilannekuvassa esitetyn määrällisen tiedon voidaan katsoa esittävän ainoastaan insider-rikosten jäävuoren huippua. Rikosilmoitusten sisältöä koskevien laadullisten tekotapa- ja tekijätietoihin perustuvien johtopäätösten voidaan kuitenkin olettaa koskevan laajemmin myös piilorikollisuudeksi jääviä tapauksia.

Taulukon 5 ulkopuolisten tilannekuvatietojen perusteella, yksityishenkilöiden tietosuojaan kohdistuvissa tapauksissa naiset ja yritysten liikesalaisuuksiin kohdistuvissa tapauksissa miehet ovat yliedustettuina.

Yhtenä naisten suuren osuuden sosiaali- ja terveysalan epäilyistä selittävänä tekijänä voi olla naisten suurempi määrä sote-alalla. Naisten osuus kuntasektorin (suurin sosiaali- ja terveysalan työnantaja) työntekijöistä oli 78,2 % tilannekuvaotoksen keskimmäisenä vuonna 2014. Vastaavasti miesten osuus yksityisen sektorin työntekijöistä oli 60,2 %. Miesten suurempaa osuutta (91 %) yrityssalaisuusrikoksissa ei kuitenkaan täysin selitä miesten suurempi osuus (60,2 %) yritysten työntekijöistä. (Tilastokeskus 2014, 41.) Charney selittää miesten suurempaa osuutta hyötymistarkoitukseen pyrkivissä insider-rikoksissa sillä, että miehet arvottavat työuralla menestymisen ja vaurauden tärkeämmäksi asiaksi elämässä useammin kuin naiset (2010, 53).

Tilannekuvaan sisällytettiin lisäksi tieto insidereiden jakautumisesta teknisessä asemassa oleviin ja ei-teknisessä asemissa oleviin insidereihin, koska erään Yhdysvalloissa tehdyn tutkimuksen mukaan yli puolet insidereista ja toisen tutkimuksen mukaan suuri osa, jotka veivät suojattavaa tietoa olivat teknisessä roolissa kohdeorganisaatiossa (Collins ym. 2016, 73; Cappelli ym. 2012, 315).

Tilannekuvan kaikista epäillyistä insider-rikoksista kuitenkin ainoastaan kahdessa rikoksessa tekijä tai tekijät ovat olleet tietojärjestelmien järjestelmänvalvojan tehtävissä, vastaavissa tehtävissä, tai rikoksen teossa on käytetty erityistä teknistä osaamista tietojen saamiseksi tai viemiseksi pois yrityksestä. Tätä tukee myös Mooren ym. (2011, 19) tutkimus, jossa tiedon varastamiseen liittyvissä insider-rikoksissa (n = 48) yhdessäkään ei havaittu erityistä järjestelmiin liittyvää roolia, vaikkakin muihin insider-kategorioihin liittyvissä insider-rikosepäilyissä teknisessä roolissa olevien epäiltyjen osuuden keskiarvo oli 8 %. Toisaalta tilannekuvan ulkopuolelle rajattiin rikoslain (39/1889) 38.luvun 8 § ja 8 a §mukaiset teot, joista osan toteuttaminen perustuu tekniseen osaamiseen.

Tilannekuvan perusteella liikesalaisuuksiin kohdistuvista yrityssalaisuusrikoksista suurin osa on insider-tekoja. Suurin osa (152 kpl / 80 %) ilmoitetuista yrityssalaisuusrikosepäilyistä täyttää tässä tutkimuksessa määritellyn insider-teon tunnusmerkit. Tästä syystä ilmirikollisuudesta kertovana suuntaa-antavana insider-rikostilannekuvan mittarina voidaan pitää myös pelkkiä yrityssalaisuusrikosepäilyjen ilmoitusmääriä ilman ilmoitusten laadullista sisällönanalyysiä.

Tilannekuvan ja rikosilmoitusmäärien tarkastelussa tulee ottaa huomioon, että se kuvaa rikosilmiötä, johon liittyvät tapaukset ovat korostuneesti piilorikollisuutta. Tilannekuvasta saatava hyöty perustuu tapausten laadullisen sisällön tarkasteluun ja siitä tehtäviin suuntaa-antaviin yleistyksiin tekotavoista ja tekijöistä. Tilannekuvasta ei tule tehdä johtopäätöksiä insider-ilmiön laajuudesta tai riskien todennäköisyydestä suhteessa muihin yritysturvallisuutta koskeviin vahinkoriskeihin, jotta yritysten riskien hallinnan tulokset eivät vääristy.

5 Insider-riskien hallinta

Three may keep a secret,
if two of them are dead

– Benjamin Franklin

Tässä luvussa esitellään insider-riskien hallintaa koskevat kirjallisuuskatsauksen ja asiantuntijahaastattelujen tulokset. Luvun aluksi käsitellään insider-riskien hallintaa prosessin näkökulmasta, jonka jälkeen riskien hallintaa koskevat toimenpiteet on jaettu ennen työsopimuksen solmimista koskeviin riskienhallintatoimenpiteisiin, työsuhteen aikaisiin riskienhallintatoimenpiteisiin ja työsuhteen päättymiseen liittyviin toimenpiteisiin.

Asiantuntijahaastattelujen tulokset on esitetty kommentaarina jokaisen alaluvun päätteeksi.

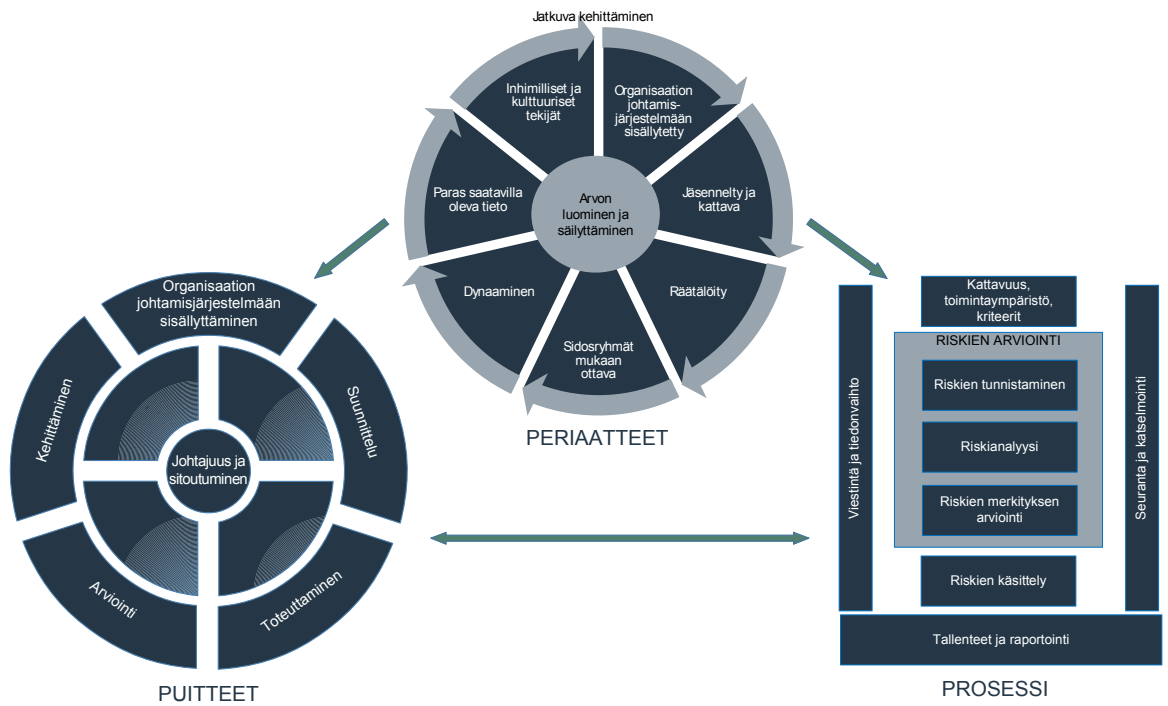
Insider-riskien hallintaa käsitellään ISO 31000- ja siihen perustuvan tietoturvallisuusriskejä käsittelevän ISO 27005-standardin viitekehyksessä. Riskien hallinta perustuu järjestelmälliseen ja prosessimaiseen lähestymistapaan, jossa insider-uhka muodostaa suojattavan liikesalaisuustiedon ja siihen liittyvien haavoittuvuuksien yhdistelmänä insider-riskejä, joita voidaan käsitellä ja hallita. Valitusta viitekehyksestä huolimatta jokaisen yrityksen tulee määritellä itse riskienhallintaan liittyvät toimintamallinsa, joihin vaikuttavat esimerkiksi tietoturvallisuuden hallintajärjestelmän laajuus, riskienhallinnan toimintaympäristö ja yrityksen toimiala.

Yrityksen on myös tärkeä käyttää insider-riskien arviointiin menetelmää, jonka se kokee vaivattomaksi, johon se luottaa ja joka tuottaa toistettavia tuloksia. (ISO 27005 2013, E.2 & 8.). Insider-riskien hallinta saattaa myös vaatia joissakin yrityksissä paradigman muutosta. Insider-riskien tunnistamiseksi ja hallinnaksi tulee luopua kehäpuolustukseen perustuvasta turvallisuusajattelusta, jossa kehän sisäpuolella olevia asioita suojataan ulkopuolelta tulevilta uhkilta, koska insider-uhka on jo valmiiksi kuvitteellisen kehän sisäpuolella (Saathoff, Nold & Holstege 2013, 26).

Yksittäisistä ja yleisistä riskienhallintakeinoista on pyritty poimimaan insider-tutkimuksissa eniten käsiteltyjä ja useimpiin yrityksiin soveltuvimpia yleisiä keinoja, joiden soveltaminen on kustannustehokasta (Return on Investment). Yksi insider-riskien hallintakeinojen olennainen lähde on myös uusittu ISO 27002:2017-standardi, jossa on käsitelty

tarkemmin tutkimuksissa yleisellä tasolla ilmenneitä hallintakeinoja. Useimmat hallintakeinoista voidaan toteuttaa sekä hallinnollisesti että teknisesti. Niiden samanaikaisella toteuttamisella pystytään joissain tilanteissa poistamaan toisen toteutustavan toteuttamattajättämisen aiheuttama haavoittuvuus. Käytännössä tällä tarkoitetaan esimerkiksi ihmisen toiminnan aiheuttamien haavoittuvuuksien poistamista teknisillä ratkaisuilla.

ISO 31000:2018-standardin mukaan riskienhallinnan tarkoituksena on arvon luominen ja säilyttäminen ja se myös parantaa suorituskykyä sekä tukee innovointia ja tavoitteiden saavuttamista (ISO 31000:2018, 4). Riskienhallinta perustuu kolmeen osatekijään, joita ovat periaatteet, puitteet ja prosessit (ISO 31000:2018, 4-6). Tämä kokonaisuus ja niiden suhde on kuvattu kuviossa 8.



Kuvio 8: Riskienhallinnan periaatteet, puitteet ja prosessi (mukaillen ISO 31000 2018)

Vaikuttavaan riskienhallintaan tarvitaan arvon luomista ja säilyttämistä tavoittelevia periaatteita, jotka on kuvattu kuvion 8 huipulla.

Periaatteiden mukaan riskienhallinnan tulee olla osa kaikkia organisaation toimintoja ja puitteet ja prosessi tulee sovittaa organisaation tavoitteisiin liittyvään toimintaympäristöön sopivaksi. Toimintamallin tulee olla jäsennelty ja kattava, jotta se tekee tulok-

sista yhdenmukaisempia ja vertailukelpoisia. Riskienhallinnan tulisi perustua oman ja sidosryhmien parhaaseen saatavilla olevaan historiatietoon, nykytilaa koskevaan tietoon ja tulevaisuutta koskeviin odotuksiin. Periaatteiden mukaan organisaation tulee ymmärtää, että riskit voivat muuttua toimintaympäristön muuttuessa ja ihmisten käyttäytyminen ja kulttuuri vaikuttavat riskienhallintaan kaikilla tasoilla. Riskienhallintaa tulee myös kehittää jatkuvasti oppimisen ja kokemusten johdosta. (ISO 31000:2018, 4)

Kuvion 8 vasemmassa reunassa on kuvattu riskienhallinnan puitteet, jonka keskiössä on organisaation ylimmän johdon sitoutuminen. Puitteiden tarkoituksena on auttaa riskienhallinnan kytkemisessä organisaation eri toimintoihin ja tehtäviin.

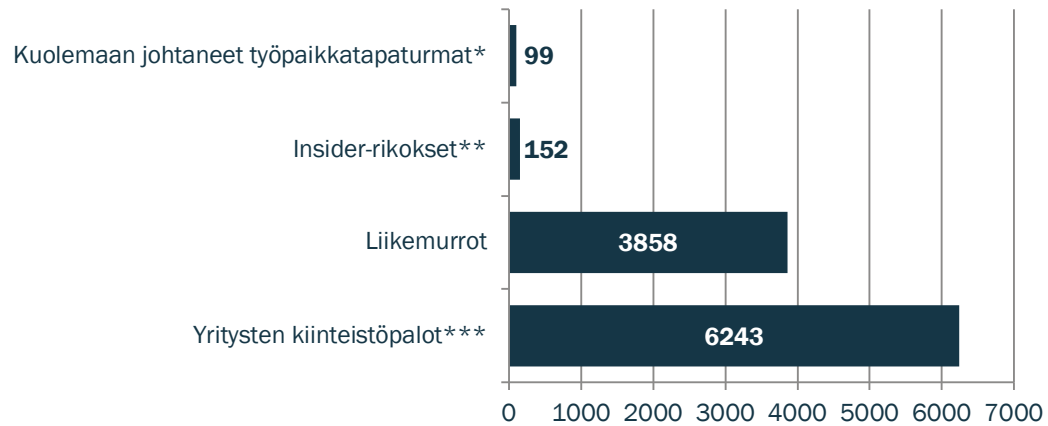
Olennaista on, että ylin johto on vastuussa riskienhallinnasta ja sen tulisi varmistaa, että toiminta on jalkautettu kaikkiin organisaation toimintoihin ja johtamisjärjestelmään. Puitteet perustuvat jatkuvan kehittämisen malliin (PDCA), jonka perusteella riskienhallinnan puitteet suunnitellaan ja toteutetaan ja jonka perusteella puitteita arvioidaan ja kehitetään. Olennaista on, että riskienhallinnan kehittäminen on jatkuvaa. (ISO 31000:2018, 5.1 - 5.7)

Käytännön työhön liittyvä riskienhallintaprosessi on kuvattu kuvion 8 oikeassa reunassa. Prosessi sisältää toimintaperiaatteiden, menettelyjen ja käytäntöjen järjestelmällisen soveltamisen viestintään ja tiedonvaihtoon sidosryhmien kanssa sekä soveltamiseen riskien arviointiin, käsittelyyn, seurantaan, katselmointiin, kirjaamiseen ja raportointiin. Riskienhallintaprosessi kuvataan usein lineaarisena järjestyksessä etenevänä prosessina, vaikka se on käytännössä iteratiivinen prosessi. (ISO 31000:2018, 6.1.) ISO 27005 ja 31000-viitekehyksiin perustuva insider-riskienhallintaprosessi on kuvattu liitteessä 1.

Riskienhallintaprosessin keskeisenä osana on riskien arviointi, joka sisältää riskien tunnistamiseen, analyysin ja merkityksen arviointiin liittyvä työvaiheet. Riskien arviointivaiheessa riskejä luokitellaan riskitason perusteella, joka perustuu muun muassa riskin todennäköisyyden ja seurausten vakavuuden tarkasteluun. Riskin todennäköisyyden määrittämiseksi käytetään usein tilastoja, jotta pyritään välttämään ihmisten mielipiteiden ja tuntemuksien mahdollisesti aiheuttamia vääristymiä.

Insider-riskien todennäköisyyden arviointi tilastotietojen perusteella ja lukumäärien vertailulla on kuitenkin ongelmallista, koska teot jäävät usein piilorikollisuudeksi. Tyypillisimpiin yritysten tunnistamiin vahinkoriskeihin ja niiden lukumääriin perustuva tilastollinen vertaaminen insider-riskien tilastoihin ei ole mielekästä (kuvio 9).

Jokainen työpaikalla tapahtuva kuolemantapaus, tulipalo tai liikemurto tulee lähtökohtaisesti yritysten ja viranomaisten tietoon toisin kuin insider-riskit. Riskien todennäköisyysvertailu täytyy myös suhteuttaa yrityksen toimintaympäristöön riskienhallintaprosessin mukaisesti, koska riskien todennäköisyys vaihtelee yrityksen ja sen toimialan mukaan.



Kuvio 9: Viranomaisten tietoon tulleiden toteutuneiden riskien lukumäärä Suomessa yhteensä vuosina 2012-2016 (Pelastusopisto 2017, 14; Tilastokeskus 2017a; Tilastokeskus 2015)

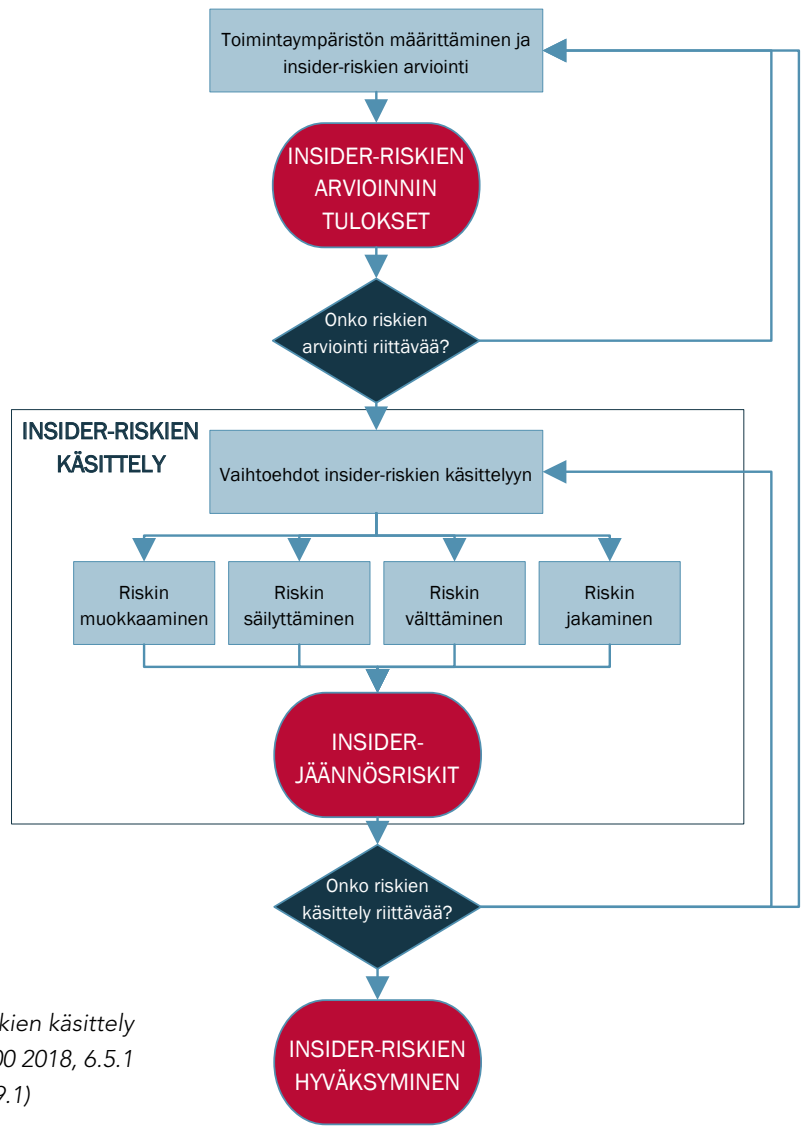
* tilasto kuvaa työpaikalla ja liikenteessä työtehtävää suorittaessa sattuneita kuolemaan johtaneita työtapaturmia. Luvusta puuttuu vuoden 2016 tiedot.
**insider-rikoksella viitataan tämän tutkimuksen tilannekuvatietoihin yrityssalaisuusrikoksista
*** luku sisältää liike-, toimisto-, teollisuus- ja varastorakennuspalot

Insider-riskien seurausten vakavuuden määrittäminen vahinkojen arvon perusteella on myös vaikeampaa, kuin esimerkiksi liikemurtojen tai tulipalojen aiheuttamien aineellisten vahinkojen ja seisokin tuottamien vahinkojen laskeminen, koska erityisesti tiedon menetyksen aiheuttamien välillisten vaikutusten arvioiminen on monimutkaista.

Useissa yhdysvaltalaistutkimuksissa on esitetty hyvinkin vaihtelevia arvioita insider-riskien aiheuttamista vahingoista yrityksille. Yhtenä harvoista suuntaa-antavista mittareista voidaan kuitenkin pitää vakuutusyhtiöiden tietopääoman paljastumisista maksamia todellisia korvaussummia yrityksille. Länsimaisten vakuutusyhtiöiden antamien vuosina 2014-2016 tapahtuneita insider-riskejä koskevien tietojen perusteella tietopääomaan ja liikesalaisuustietoihin kohdistuvien vahinkojen korvaussummat olivat keskimäärin suurimmat (864 964 $) kybervahinkojen viiteryhmässä. Kybervahinkoihin sisältyvistä insider-tapauksista maksettuja korvaustapahtumia oli lukumäärältään

vähemmän, kuin muita tietopääomaan kohdistuneita korvaustapahtumia, mutta insider-tapauksissa keskimääräinen korvaussumma oli korkeampi. (NetDiligence 2017, 12 & 25.) Korvaussummien tarkastelu ei voi kuitenkaan olla ainoa riskin vakavuutta kuvaava mittari, koska joidenkin yritysten koko olemassaolo saattaa perustua liikesalaisuuksien pysymiseen salassa.

Insider-riskien arvioinnin tulosten perusteella tarkastellaan arvioinnin riittävyyttä ja palataan tarvittaessa takaisin toimintaympäristön määrittelyvaiheeseen riskien arviointiin. Mikäli arviointi todetaan riittäväksi, siirrytään insider-riskien käsittelytavan valintaan. Käsittelyllä tarkoitetaan riskienhallinnan toistuvaa alaprosessia, jossa valitaan ja toteutetaan vaihtoehdot insider-riskien käsittelyyn (Kuvio 10). (ISO 31000 2018, 6.5.1-6.5.2.)



Kuvio 10: Insider-riskien käsittely (mukaillen ISO 31000 2018, 6.5.1 & ISO 27005 2013, 9.1)

Käsittelytapoja voi olla yksi tai useampi, eivätkä ne ole toisiaan poissulkevia:

- riskin torjuminen päättämällä olla aloittamatta tai jatkamatta riskin aiheuttavaa toimintaa
- riskin ottaminen tai lisääminen jonkin mahdollisuuden hyödyntämisen takia
- riskin lähteen poistaminen
- todennäköisyyden muuttaminen
- seurausten muuttaminen
- riskin jakaminen
- riskin säilyttäminen tietoon perustuvalla päätöksellä (ISO 31000:2018, 6.5.1.)

Insider-riskien käsittelytapojen valintaan tulisi vaikuttaa muun muassa käsittelytapojen kustannustehokkuus. Yritys saattaa esimerkiksi saada merkittävää hyötyä sekä kustannusten että turvallisuuden näkökulmasta eri käsittelytapojen yhdistelemisestä, esimerkiksi insider-riskien todennäköisyyksien pienentämisestä, seurausten vähentämisestä ja jäännösriskien jakamisesta tai säilyttämisestä. (ISO 27005:2013, 9.1.)

Samaan insider-riskiin kohdistettujen eri riskienkäsittelytapojen ja hallintakeinojen yhdistelmällä voidaan myös pyrkiä muodostamaan syvyyssuuntaisia turvallisuuskontrolleja yrityksen liikesalaisuustiedon suojaamiseksi.

Syvyyssuuntaisen turvallisuusajattelutavan mukaan riskejä hallitaan toisistaan riippumattomilla toimenpiteillä siten, että jos yksi hallintakeino pettää, toiset suojattavan arvon ympärille muodostetut hallintakeinot estävät riskin toteutumisen (Ydinenergialaki 990/1987 Luku 2a, 7 c §; Viega & McGraw 2002, 96-97). Yritykseen jalkautetut syvyyssuuntaiset turvallisuuskontrollit saattavat esimerkiksi vaikeuttaa insiderin tekemää kohteen tiedustelua ja teon toteuttamista sekä kasvattavat kiinnijäämisriskiä. Muun muassa Carnegie Mellon yliopiston tutkimuksessa korostetaan, että insider-riskejä voidaan pienentää ja ennaltaehkäistä tehokkaasti ainoastaan luomalla syvyyssuuntaisia turvallisuuskontrolleja (Silowash ym. 2012, 4).

Useissa tapauksissa insiderit ovat kuitenkin pystyneet kiertämään kohdeorganisaation toteuttamat erilaiset turvallisuuskontrollit (Blackwell 2009, 20).

Toisin kuin tahattomiin insider-uhkiin (tietämätön ja välinpitämätön) tahallisiin insidereihin on vaikea vaikuttaa suoraan koulutuksen tai ohjeistuksen keinoin, joten yritysten tulisi pyrkiä luomaan kiertämättömiä turvallisuuskontrolleja insider-riskien hallitsemiseksi. Kiertämättömillä turvallisuuskontrolleilla tarkoitetaan tässä tutkimuksessa

sellaisia kontrolleja, joiden toimintaperiaatteiden tunteminen ei poista niiden vaikuttavuutta. Tällaisten kontrollien luominen toteuttaa yhtä Saltzerin ja Schroederin jo 1970-luvulla esittämää tunnettua tietoturvallisuusperiaatetta, jonka mukaan turvallisuustoimenpiteiden suunnittelussa on lähdettävä ajatuksesta, että hyökkääjä (insider) tuntee toteutetut vastatoimenpiteet (1975, 1283).

Sekä Blackwell että Yhdysvaltain insider-työryhmä ovat esittäneet insider-riskien käsittelyn tavoitteeksi pelotevaikutukseen perustuvien näkyvien turvallisuustoimenpiteiden ja varoitusmerkkien toteuttamisen, millä viestitään oikeista toimintatavoista (Code of Conduct) ja korostetaan teon paljastumisen ja rangaistuksen todennäköisyyttä. (Blackwell 2009, 25 & 34; NITTF). Insider ei kuitenkaan aina toimi rationaalisesti ja voi pelotevaikutuksesta huolimatta varastaa tietoja. Pelotevaikutus kohdistuukin todennäköisesti tekijöihin, jotka eivät toimi tahallisesti (Straub & Welke 1998, 446.) Niillä saattaa kuitenkin olla vaikutusta sellaisiin itsenäisesti toimiviin tekijöihin, jotka eivät ole täysin varmoja teon toteuttamista.

Turvallisuustoimenpiteisiin perustuvan riskien käsittelyvaiheen jälkeen yrityksen tulee määrittää insider-jäännösriskit, joilla tarkoitetaan riskien käsittelyn jälkeen jäljellä olevia riskejä. Jäännösriskien hyväksymiseen saattaa liittyä merkittävää riskinottoa, joten yrityksen johdon tulisi päättää niiden hyväksymisestä. (ISO 27005:2013, 3.8 & 9.1.) Valittujen turvallisuustoimenpiteiden toteuttamisen jälkeen turvallisuustasoa tulee testata, jotta varmistutaan riskien hallintakeinojen vaikuttavuudesta ja käsittelyn riittävyydestä (Cole & Ring 2005, 35). Riskien arvioinnin tulisi myös olla jatkuvaa, koska insiderien tekotavat kehittyvät jatkuvasti (Cole & Ring 2005, 314).

Useissa tutkimuksissa (mm. Collins ym. 2016; Kont ym. 2015; Cappelli ym. 2012) esitetään yhtenä insider-riskien systemaattisena hallintatapana erikseen tai muuhun riskienhallintaan integroituna insider-riskien hallintaohjelman perustamista, jonka johdosta riskejä olisi mahdollista hallita järjestelmällisesti pistemäisen lähestymistavan sijaan. Hallintaohjelman tavoitteena olisi tukea yrityksen insider-riskien hallintaa sekä käsitellä eri kanavia pitkin vastaanotettuja havaintoja mahdollisesta insider-toiminnasta. Insider-työryhmä tarvitsisi toimiakseen tukea eri puolilta organisaatiota ja erityisen tärkeänä pidetään yrityksen henkilöstöhallinnon ja juristien antamaa asiantuntijatukea. Lisäksi yrityksen johdon tulisi antaa täysi tuki työryhmän toiminnalle. (Blankenship 2016, 7.; Kont ym. 2015, 23.)

Ohjelman toimintaan liittyy kuitenkin myös tunnistettuja riskejä. Blankenshipin mukaan suurin virhe on luoda omista työntekijöistä lisää tyytymättömiä potentiaalisia insider-uhkia huolimattomalla tai piittaamattomalla asenteella työntekijöiden yksityisyyttä tai työhyvinvointia kohtaan osana ohjelman toimintaa. (2016, 7-9.) Myös Kont ym. korostaa, että kysymykseen "kuka valvoo valvojia?" täytyy pystyä vastaamaan, kun ohjelman toimintaan liittyvä työryhmä perustetaan. Täydellistä läpinäkyvyyttä on mahdoton toteuttaa, mutta ohjelmalla täytyy olla henkilöstön luottamus. (2015, 24.)

5.1 Työsuhteen alun insider-riskien hallintakeinot

5.1.1 Rekrytointivaihe

Rekrytointivaiheen riskien hallintaan kuuluu olennaisesti, että kaikkien työnhakijoiden tausta tarkistetaan lain sallimin keinoin ja tarkastukset on suhteutettu liiketoiminnallisiin vaatimuksiin, tiedon luokitukseen ja arvioituihin riskeihin.

Työnhakijaan, joka hakeutuu liikesalaisuuksien käsittelyä edellyttäviin työtehtäviin, tulisi kohdistaa laajempia ja yksityiskohtaisempia taustatarkistuksia. Tarkistuksissa tulee kuitenkin ottaa kaikissa tilanteissa huomioon yksityisyyden suojaan liittyvät vaatimukset, kuten esimerkiksi työnhakijasta kerättäviä tietoja ja niiden käsittelyä koskevat rajoitukset. Yrityksen tulisi määritellä tarkasti tarkistuksia koskevat kriteerit ja työtehtäviä koskevat laajuudet sekä roolit, jotka osallistuvat taustatarkistusprosessiin (ISO 27001 2013, A.7.1.1.; ISO 27002 2017, 7.1.1.; 759/2004; 523/1999.)

Työntekijän rekrytointiin liittyvistä toimenpiteistä tulisi tehdä prosessi ja yksittäisiä rekrytointeja koskeva tarkistuslista, jossa on otettu huomioon muun muassa seuraavat hakijaan taustaan liittyvät näkökulmat:

- työnhakijan henkilöllisyyden varmistaminen virallisesta henkilöllisyysasiakirjasta
- lisätietoja hakijasta antavien henkilöiden selvittäminen. Mahdollisuuksien mukaan tulisi pyrkiä löytämään esimerkiksi yksi työelämästä ja yksi yksityiselämästä työnhakijan tunteva henkilö
- hakijan esittämien tietojen oikeellisuuden varmistaminen ottamalla yhteyttä suosittelijoihin, jotka on mainittu työhakemuksessa
- työhistorian tarkistaminen henkilöltä itseltään ja työtodistuksista
- koulutustaustan tarkistaminen koulu- ja tutkintotodistuksista
- taloudellisen tilanteen selvittäminen (edellyttää hakijan suostumusta)

- hakijan vastuuhenkilötietojen ja yrityskytkentöjen selvittäminen
- henkilöturvallisuusselvityksen hakeminen Suojelupoliisista (726/2014)
- huumausainetestauksen teettäminen (759/2004, 3.luku)
- henkilö- ja soveltuvuusarviointitestien teettäminen (759/2004, 13 §)
- salassapitoehdon sisällyttäminen työsopimukseen tai erillisen salassapitosopimuksen solmiminen (Vapaavuori 2016, 363)
- kilpailukieltosopimuksen solmiminen (55/2001, 3. luku)
- koeajan sisällyttäminen työsopimukseen (55/2001, 3. luku)

Osan edellä mainituista näkökulmista tulee ottaa huomioon myös työsuhteen aikana, esimerkiksi työntekijän toimenkuvan muuttuessa. (Valtiovarainministeriö 2008, 21.)

Taulukossa 7 on esitetty työntekijän taustaan liittyviä rekrytointivaiheessa tarkasteltavia uhkaindikaattoreita ja niiden korrelaatiota itsenäisesti toimivan insiderin ja yrityksen sisältä värvätyn insiderin profiileihin.

Korrelaation painoarvoa on kuvattu kolmiportaisella luokituksella matala, keskitaso ja korkea. Taulukon tietoja tarkasteltaessa on tärkeä huomata, että yhden tai useamman indikaattorin sopiminen tietyn työntekijän profiiliin ei tarkoita, että henkilö tulisi syyllistymään insider-tekoon. Myöskään työntekijä, jonka profiiliin yksikään indikaattori ei sovi, ei automaattisesti tarkoita sitä, etteikö hän voisi toteuttaa insider-tekoa. (NITTF 2016, 7; CPNI 2013, 11).

Rekrytointivaihe on kriittinen insider-riskien hallinnassa, koska riski on mahdollista poistaa kokonaan. Parker ym. on kuitenkin päätellyt insider- ja vakoilutapauksia koskevista tutkimustuloksista, että monet insiderit muuttuvat tyytymättömiksi ja valmiiksi toteuttamaan tekonsa vasta kohdeorganisaatiossa olevan työsuhteensa aikana, jolloin rekrytointivaiheen riskienhallintatoimenpiteillä on vaikeampi vaikuttaa insider-riskeihin (Parker 2004, 176).

Haastateltujen asiantuntijoiden mielestä rekrytointivaiheessa tulisi taulukon 7 mukaisesti pyrkiä tunnistamaan haavoittuvuuksia, jotka voivat altistaa insider-toiminnalle.

Haastateltava C mainitsee yksityiskohtana hakijan lyhyisiin työsuhteisiin perustuvan työhistorian, jonka syyt tulisi selvittää. Haastateltava A:n mukaan insider-riskien hallinnassa pitäisi keskittyä erityisesti niihin insider-profiileihin (itsenäisesti toimivat), joiden motivaation syntyyn voidaan vaikuttaa yrityksen omin keinoin muun muassa työtyytymättömyyttä vähentämällä. Haastateltava A olisi joissain tilanteessa valmis käsittelemään ja hyväksymään värvätyn ja solutetun insider-riskin jäännösriskinä, koska niiden hallitseminen on huomattavasti vaikeampaa.

INDIKAATTORI	ITSENÄINEN TOIMIJA	VÄRVÄTTY
Viihtyminen organisaation perusarvoja vastaan ajattelevien ihmisten kanssa	keskitaso	korkea
Rikoksiin syyllistyminen	korkea	keskitaso
Riippuvuudet (alkoholi, huumeet, pelaaminen)	korkea	keskitaso
Taustalla psyykkisiä tai tunnepuolen ongelmia	keskitaso	keskitaso
Velkaantuneisuus	korkea	keskitaso
Huonoon harkintakykyyn viittaava seksuaalinen käytös	keskitaso	keskitaso
Sitoutuminen toimintaan, joka voi aiheuttaa eturistiriitoja	korkea	korkea
Oma liiketoiminta	korkea	keskitaso
Sosiaalisen median aktiivisuus	matala	matala
Aiempien työnantajien määrä ja työsuhteen keskimääräinen kesto	korkea	matala
Varojen yli eläminen	korkea	korkea
Sukulaissuhteita ulkomaille (ulkomaan sidonnaisuudet)	matala	korkea
Yli kolmenkymmenen ja erityisesti yli neljänkymmenen vuoden ikä	korkea	korkea

Taulukko 7: Työntekijän taustaan liittyvät rekrytointivaiheen insider-indikaattorit ja henkilökohtaiset haavoittuvuudet vakoiluun ryhtymiselle (mukaillen Kont ym. 2015, 32; Fischer 1998; Herbig 2008, 7)

Haastateltavat näkivät henkilöturvallisuusselvityksiin ja salassapitosopimuksiin perustuvat riskien hallintakeinot perustyökaluina, mutta useat korostivat kokonaistiedon merkitystä, johon kuuluu erilaisten tarkistusten ristiinvertailu työhistoria- ja koulutustiedoista yrityskytkentöihin ja rikostaustaan. Myös hakijan soveltuvuuden merkitys ilmeni yhtenä välillisenä keinona hallita insider-riskiä. Tehtävään soveltumaton henkilö saattaa ajan kuluessa muuttua tyytymättömäksi, jolloin mahdollisuus henkilön insider-toiminnalle kasvaa.

Haastateltava E:n mukaan rekrytointivaiheen insider-indikaattoritietoja tulisi pyrkiä havaitsemaan myös hakijan sidonnaisuuksista: ”Kun yrityksissä tehdään vastapuoliriskin hallintaa, niin tämä on vähän niin kuin samanlainen sen yksittäisen henkilön näkökulmasta, että pyritään tarkastelemaan sitä taustaa kokonaisuutena ja arvioidaan, että onko sillä joitakin vaikutuksia mahdollisesti siihen työsuhteeseen tai liikesalaisuuden suojaan ja rikostausta on vain yksi osa sitä, joten väittäisin, että erilaiset sidonnaisuudet ja aikaisemmat työtehtävät ovat vielä keskeisempi kysymys tällä hetkellä Suomessa”. Haastateltava tarkensi vastaustaan viittaamalla muun muassa hakijan muihin osakkuuksiin tai hallituspaikkoihin samalla alalla olevissa yrityksissä.

5.1.2 Henkilöturvallisuusselvitys

Työnhakijoiden taustojen rekisteriperusteinen selvittäminen on merkittävä osa insider-riskien hallintaa.

Muun muassa Yhdysvaltojen IT-sektoria koskevan tutkimuksen mukaan 38 %:lla kiinnijääneistä insidereista oli päihteisiin, petoksiin ja varkauksiin liittyvää rikoshistoriaa. (Kowalski ym. 2008, 31). Tämän tutkimuksen yhteydessä ei kartoitettu erilaisia kaupallisia vaihtoehtoja työntekijöiden taustaselvityksen teettämiseen, vaan on keskitytty laissa (726/2014) säädettyyn mahdollisuuteen hakea henkilöturvallisuusselvityksiä.

Henkilöturvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain (726/2014, 3 §) mukaista henkilön nuhteettomuuden tai luotettavuuden varmistamiseksi laadittavaa selvitystä henkilön taustasta. Selvityksen teettämisestä on ilmoitettava työpaikkailmoituksessa tai muulla sopivalla tavalla (726/2014, 4 §). Lisäksi selvityksen teettämiseen tarvitaan kohteen suostumus, josta käy ilmi, että henkilö on saanut tiedon muun muassa luotettavuuden seurannan tarkoituksesta ja käytöstä (5 §).

Selvityksen hakemisen edellytyksenä on, että yritys hallinnoi esimerkiksi erittäin merkittävää yksityistä taloudellista etua, selvityksen kohteena oleva henkilö tulee toimimaan tehtävässä, jossa on mahdollista aiheuttaa vahinkoa suojattavalle edulle ja yritys on tunnistanut suojattaviin tietoihin kohdistuvat riskit ja toteuttanut turvallisuustoimenpiteitä tietojen suojaamiseksi (726/2014, 1 § & 18-22 §). Yritys voi hakea selvitystä tilanteen mukaan joko suppeana tai perusmuotoisena.

Selvitys voidaan laatia tehtävään valittavasta tai sitä hoitavasta, joka saa tietoja liikesalaisuuksista tai kehitystyöstä ja tiedon oikeudeton käyttö tai luovuttaminen aiheuttaa yritykselle merkittävää taloudellista vahinkoa. Tämän lisäksi selvityksen laatimisen edellytyksenä on, että ”yritykseen voi sen toimialan tai toiminnan vuoksi kohdistua yritysvakoilua tai selvitys on tarpeen erittäin tärkeän yksityisen taloudellisen edun suojaamiseksi” (726/2014, 22 §)

Insider-riskien hallinnan kannalta merkittävää on suppean ja perusmuotoisen selvityksen tietolähteisiin liittyvät erot. Toisin kuin perusmuotoisen selvityksen kohdalla, suppeaa turvallisuusselvitystä laadittaessa ei oteta huomioon Suojelupoliisin toiminnallista tietojärjestelmää, pääesikunnan turvallisuustietorekisteriä, keskusrikospoliisin epäiltyjen tietojärjestelmää eikä muun muassa ulosotto- ja luottotietorekisterin tietoja (726/2014, 25 § & 30 §).

Suojelupoliisin ja pääesikunnan rekisterit liittyvät laittoman tiedustelun torjuntaan, epäiltyjen tietojärjestelmä rikostiedustelu- ja havaintotietoihin sekä ulosotto- ja luottotietorekisterit kohteen velkaantuneisuuteen ja taloudelliseen tilanteeseen yleisesti (Poliisihallitus 2017; 509/1995 3 §; 1251/1995, 11 §). Edellä mainittujen rekisterien puuttuminen suppean turvallisuusselvityksen tietolähteistä heikentää kyseisen selvityksen vaikuttavuutta verrattuna perusmuotoiseen selvitykseen, koska puuttuvissa tietolähteissä voi olla insider-uhkan ennaltaehkäisemisen kannalta relevanttia, jopa kriittistä tietoa.

Sekä Contosin (2006, 55) että Yhdysvaltain Kansallisen tiedustelupalvelun asettaman työryhmän (Clarke, Morell, Stone, Sunstein & Swire 2014, 177) mukaan organisaatioiden tulisi insider-riskien hallitsemiseksi tehdä säännöllisesti henkilöstön taustojen uusintatarkastus, jotta voidaan varmistua työntekijöiden nuhteettomuudesta myös työsuhteen aikana.

Turvallisuusselvityslain perusteella laadittavaan henkilöturvallisuusselvitykseen kuuluu osana nuhteettomuusseuranta, jossa selvitettyjen henkilöiden mahdolliset uudet rikosepäilyt voidaan havaita poliisiasiain tietojärjestelmään tehtävien rekisteriajojen johdosta (Suojelupoliisi 2017). Nuhteettomuusseuranta poistaa aiemman turvallisuusselvityslain (177/2002) mahdollistaman tilanteen, jossa kerran selvitetty henkilö saattaa syyllistyä rekrytointivaiheen jälkeen rikoksiin työnantajan tietämättä.

Parker ym. myöntää henkilöturvallisuusselvitysten arvon, mutta toteaa samalla, että selvityksiä ei pitäisi pitää ihmelääkkeenä insider-riskien hallinnassa (2004, 177-178). Selvitysten tärkeän merkityksen vuoksi organisaatiot taipuvat kuitenkin virheellisesti ajattelemaan, että rekrytoitu henkilö tai hyväksytty sopimuskumppani olisi selvityksen läpäistyään vastedes täysin luotettava. Nimeämättömän Yhdysvaltalaisen tiedustelulähteen mukaan henkilöturvallisuusselvityksen läpikäyneet henkilöt olisivat kuitenkin osallisena jopa 85 %:ssa insider-rikoksista (Cole & Ring 2005, 5 & 33.) Taustatarkistuksena laadittavaa henkilöturvallisuusselvitystä voidaan kuitenkin pitää yhtenä merkittävänä osana yrityksen insider-riskien hallintaa.

Haastateltavat olivat pääosin samaa mieltä Parkerin ym. kanssa henkilöturvallisuusselvitysten vaikuttavuudesta insider-riskien hallintaan ja toivat esiin selvityksen hyötyjä. Haastateltava D totesi kuitenkin, että "…(henkilöturvallisuusselvitysmenettely) on hyvä, mutta käyttäjät uskovat siihen liikaa", millä haastateltava viittasi Parkerin ym. tavoin useiden organisaatioiden ajatukseen pitää selvitettyjä henkilöitä automaattisesti luotettuina henkilöinä.

Muun muassa Haastateltava A ja E toivat esiin, että selvityksillä voidaan karsia työnhakijoista lähinnä selvimmät insider-tapaukset, mutta ongelmana on, että pelkkien rekisteritietojen perusteella on käytännössä mahdotonta luoda kokonaiskuvaa insiderista. Epäsuorina viitteinä pidettiin muun muassa tilannetta, jossa työntekijä on täysin välinpitämätön yhteiskunnallisista määräyksistä. Se indikoi, että henkilö todennäköisesti rikkoo myös muita sääntöjä (Haastateltava B).

Haastateltava B korostikin nuhteettomuusseurannan merkitystä, jos työntekijästä saadaan uutta tietoa työsuhteen aikana tapahtuneista muutoksista. Haastatteluissa tuotiin myös esiin, että työntekijän taustalla mahdollisesti olevien liikesalaisuuksien suojaan liittyvien siviilioikeudellisten toimenpiteiden selvittäminen vaatii toisenlaisia työkaluja (Haastateltava E).

Selvityksen heikkoudeksi todettiin sen historia- ja rikostietoihin painottuva luonne, jonka avulla ei päästä kiinni kaikkiin mahdollisiin olemassa oleviin indikaattoreihin. Insiderin paljastavat indikaattorit voivat olla myös epäsuoria ja havaittavissa jostain muualta, kuin henkilöturvallisuusselvitysten sisällöstä. Toisaalta selvitysten merkityksen insider-riskien hallinnan perustyökaluna todettiin olevan kiistaton erityisesti sen helppouden ja suomalaisten rekisteritietojen kattavuuden vuoksi. Rekrytointivaiheen insider-riskien hallinnan todettiin silti olevan kokonaisuus, ei pelkkä turvallisuusselvitys.

Kirjallisuuskatsauksen ja haastattelujen perusteella henkilöturvallisuusselvityksiä voisi verrata tietojärjestelmissä käytettäviin virustorjuntaohjelmiin. Ohjelmat kuuluvat osaksi jokaista suojattavaa tietojärjestelmää pysäyttäen suurimman osan uhkista. Niiden toiminta perustuu kuitenkin aiemmista virustartunnoista saatuihin näytteisiin, joten ohjelma ei pysty havaitsemaan niin sanottuja nollapäiväuhkia, joista ohjelmalla ei ole entuudestaan vertailunäytettä. Vasta työsuhteen aikana aktivoituvaa ja rekisteritiedoiltaan puhdasta insideria voidaan pitää inhimillisenä nollapäiväuhkana yritykselle.

5.1.3 Salassapitosopimus

Salassapitosopimuksen tekeminen on osa insider-riskien ennalta ehkäiseviä riskienhallintakeinoja, jonka vaikutus on sekä juridinen että preventiivinen (Vapaavuori 2016, 325). Liikesalaisuuksien käsittelyyn osallistuvien henkilöiden tulisi allekirjoittaa salassapitosopimus tai heidän työsopimukseensa olisi kirjattava salassapitoehto ennen pääsyoikeuden saamista liikesalaisuuksia sisältäviin tietoihin.

Yritys voi salassapitosopimuksella osoittaa sekä salassapitotahdon että tosiasiallisen salassapidon, millä on merkitystä mahdollisissa sopimusrikkomusta koskevissa erimielisyyksissä ja insider-rikosten oikeuskäsittelyssä (Vapaavuori 2016, 208.)

Työntekijällä on lakiin perustuva salassapitovelvoite, mutta sopimuksella velvoitetta voidaan täsmentää ja ulottaa koskemaan myös työsuhteen päättymisen jälkeistä aikaa (Vapaavuori 2016, 209)

Sopimuksessa voidaan esittää selvästi se, kenelle liikesalaisuustietoa voidaan luovuttaa ja mikä on tiedon sallittu käyttötarkoitus, mikä helpottaa yrityksen näyttötaakkaa mahdollisissa insider-rikostapauksissa (Vapaavuori 2016, 209). Suomessa ei ole erillistä salassapitosopimuksia koskevaa lainsäädäntöä, joten sopimuksissa noudatetaan tavallisia sopimusoikeudellisia periaatteita (Vapaavuori 2016, 211).

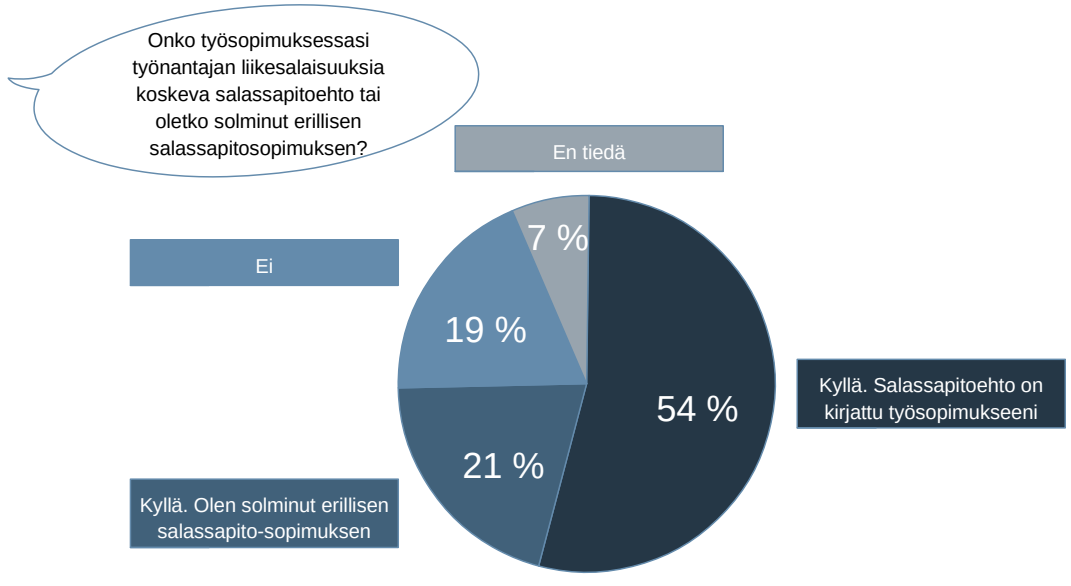
Sopimuksen hyöty perustuu käännettyyn todistustaakkaan, jonka perusteella sopimusta rikkovan osapuolen tulee osoittaa sopimuksen mukainen toimintansa välttyäkseen vahingonkorvausvastuulta. Sopimukseen voidaan myös ottaa sopimussakkoehto, jolla voidaan saavuttaa ennaltaestävä pelotevaikutus. (Vapaavuori 2016, 238, 112 & 209.) Salassapitosopimukseen perustuvaa korvausvaatimusta koskee kuitenkin vanhentumislaki (728/2003), jonka perusteella korvausvaatimus alkaa vanhentua siitä hetkestä, kun yritys havaitsee insiderin käyttäneen oikeudettomasti liikesalaisuustietoa (Työ- ja elinkeinoministeriö 2018, 68).

Yrityksillä on hyvä olla useita eri salassapitosopimusmalleja eri tilanteita varten. Sopimusmalleja tarvitaan yritysten välisiin kauppoihin, mutta etenkin omia työntekijöitä ja vierailijoita varten. Vierailijoita varten laadittava salassapitosopimus on tarpeen, jos vierailijoilla on mahdollisuus nähdä tai saada tietoonsa liikesalaisuuksia koskevaa tietoa vierailunsa aikana (Vapaavuori 2016, 205). Vapaavuori on teoksessaan pohtinut salassapitosopimuksen ja –sitoumuksen juridista eroa. Hän suosittelee yksipuolisen salassapitositoumuksen käyttöä tilanteissa, joissa liikesalaisuuksien parissa työskenteleviä henkilöitä on paljon, koska sitoumusten hallinnointi on helpompaa. Sitoumuksen velvoitteisiin voi myös lähtökohtaisesti vedota laajempi piiri esimerkiksi saman konsernin sisällä, koska sopimuksen toista osapuolta ei ole nimetty. (Vapaavuori 2016, 219)

Usein itse sopimus saatetaan määritellä salassa pidettäväksi. Tätä tulisi kuitenkin välttää, jotta pois lähtevällä työntekijällä on mahdollisuus kertoa sopimusvelvoitteistaan uudelle työntekijälle. Sopimuksen tarkempi sisältö voidaan kuitenkin määritellä salassa pidettäväksi. (Vapaavuori 2016, 224.) Vapaavuori esittää myös, että salassapitosopimukseen sisällytettäisiin vaatimus ilmoittaa työnantajalle tiedon paljastumisesta tai tiedosta, että joku työntekijöistä loukkaa yrityksen liikesalaisuuksia (Vapaavuori 2016, 344). Tämä on merkittävä huomio, koska vaatimus liittyy suoraan myöhemmin tässä tutkimuksessa käsiteltäviin insider-tekijöiden havaitsemis- ja ilmoittamiskeinoihin.

Salassapitovelvollisuus on rajattu uudessa liikesalaisuuslaissa (2018) palvelusaikaan, mutta velvollisuutta voidaan pidentää sopimuksin (HE 49/2018, 41). Lailla ei ole merkittävää vaikutusta salassapitosopimuksiin, joten se ei poista tarvetta sopimusten käyttämiseen (HE 49/2018, 45).

Salassapitovelvollisuuden sopimusperusteinen pidentäminen on perusteltua viitaten aiemmin esiteltyyn Yhdysvaltalaistutkimukseen niin sanotusta 60 päivän säännöstä sekä poliisiasiain tietojärjestelmään tehtyihin hakuihin, joiden molempien perusteella liikesalaisuuden suojaa rikotaan useimmin työsuhteen päättymishetkellä tai sen jälkeen (Cappelli ym. 2012, 75-76; Epäiltyjen insider-rikosten tilannekuva luku 4.3). Sopimuksen voimassaoloaikaa ei tulisikaan erikseen rajata, jotta yritys ei vahingossa tule luopuneeksi oikeudestaan lakisääteiseen suojaan. Rajoittamaton salassapitoaika ei ole kohtuuton, koska suojattava tieto menettää joka tapauksessa jossakin vaiheessa liikesalaisuuden luonteen ja salassapitovelvoitteet päättyvät. (Vapaavuori 338 & 346.)



Kuvio 11: Työsopimuksessa olevien salassapitoehtojen tai salassapitosopimusten määrän laajuus yrityksissä työskentelevien akavalaisten keskuudessa (mukaillen Akava 2017)

Korkeakoulutettujen työmarkkinakeskusjärjestö Akava laati keväällä 2017 selvityksen yrityksissä työskentelevien jäsentensä työsopimuksissa olevien salassapitoehtojen yleisyydestä ja piirteistä (Kuvio 11). Kyselyyn vastasi 2119 akavalaista. Vastaukset vaihtelivat työntekijäryhmittäin, joten yllä olevassa kuviossa on otettu huomioon ainoastaan vastaajien keskiarvo.

Selvityksen perusteella 74 %:lla vastanneista on työsopimukseen kirjattu salassapitoehto tai he ovat solmineet erillisen salassapitosopimuksen. Selvityksessä on lisäksi tarkennettu, että näistä vastaajista 32 %:lla salassapidon voimassaolo on rajattu. Edelleen näistä 32 %:sta puolella salassapitoehto on voimassa korkeintaan kuusi kuukautta työsuhteen päättymisen jälkeen, 19 %:lla 6-12 kuukautta ja 31 %:lla yli vuoden. (Akava 2017.)

Vaikkakin salassapitosopimuksen merkitys erityisesti oikeudellisen suojan saamiseksi on merkittävä, Mooren ym. tutkimista insidereista 41 % varasti tietoa työnantajaltaan huolimatta allekirjoitetusta salassapitosopimuksesta (2011, 6). Myöskään Cappellin ym. havaitsemissa insider-rikoksissa etenkään kolmannelle osapuolelle toimivat tekijät eivät piitanneet heitä koskevista salassapitovelvoitteista (2012, 79).

Haastateltujen suomalaisasiantuntijoiden vastaukset olivat linjassa Mooren ym. (2011) ja Cappellin ym. (2012) Yhdysvaltalaisten tutkimustulosten kanssa salassapitosopimusten vaikuttavuudesta. Vastaukset olivat myös samankaltaisia henkilöturvallisuusselvityksiä koskevan pohdinnan kanssa, jossa useat totesivat sopimusten olevan helposti sovellettava rekrytointivaiheen perustyökalu.

Jotkin vastaajat olivat suoraan sitä mieltä, että sopimuksilla ei ole minkäänlaista vaikutusta insidereihin. Haastateltava A toteaa, että ”jos tulee varta vasten tekemään haittaa tai tulee voimakas motivaatio tehdä teko, ei sopimuksella ole merkitystä”. Toisaalta pyydettäessä tarkennusta, Haastateltava A ja muutamat muut asiantuntijat kertoivat sopimuksen merkityksettömyyden liittyvän erityisesti kolmannelle osapuolelle toimiviin insidereihin. Salassapitosopimuksilla todettiin olevan mahdollinen vaikutus itsenäisesti toimivaan insideriin, jonka päätös rikoksen toteuttamiseksi ei ole täysin kypsynyt. Tällaisissa tapauksissa salassapitosopimuksella voi olla ennaltaestävä vaikutus.

Haastateltava D:n mukaan ennaltaestävän vaikutuksen ehtona on kuitenkin, että yritys on avoin ja kertoo selvästi yrityksen käyttävän kaikkia lain mahdollistamia keinoja liikesalaisuuksien loukkaustapauksissa. Tällöin on mahdollista, että insider-rikoksen toteuttamisesta epävarma tekijä luopuisi suunnitelmistaan.

5.2 Työsuhteen aikaiset sekä yleiset insider-riskien hallintakeinot

5.2.1 Turvallisuuspolitiikka

Turvallisuuspolitiikan ja siitä johdettujen ohjeiden tarkoituksena on tarjota johdon tuki insider-riskien hallinnalle liiketoiminnallisten ja lainsäädännöllisten vaatimusten mukaisesti (ISO 27001 2013, A 5.5.1; ISO 27002 2017, 5.1.1; Cappelli ym. 2012, xxii; Parker ym. 2004, 179; Cole & Ring 2005, 20).

Riskien hallintaa tukevien politiikkojen tulee olla yksiselitteisiä ja jalkautettu ja niistä tulee selvästi käydä ilmi, mikä ei ole liikesalaisuuksien hyväksyttävää käyttöä. Adoben laatiman kyselytutkimuksen perusteella politiikkojen jalkauttaminen ei ole itsestäänselvyys, sillä kolmasosa vastanneiden suomalaisyritysten työntekijöistä ei tiennyt, onko heidän yrityksessä toimintaperiaatteita yrityksen sisäisten tietojen käsittelyyn (Liiten 2017).

Politiikat, jotka ymmärretään väärin, joiden tiedottamisessa on epäonnistuttu tai joita ei ole jalkautettu ja valvottu, voivat seuraustensa perusteella aiheuttaa muun muassa työtyytymättömyyttä. Politiikkojen ja ohjeiden noudattaminen tuleekin koskettaa koko henkilöstöä ilman poikkeuksia, jotta yritys välttyy erimielisyyksiltä, jotka voivat vaikuttaa insider-riskin juurisyihin (Collins 2016, 33; Blackwell 2009, 24).

Politiikkojen taustalla olevat perustelut tulisi selittää, koska työntekijät hyväksyvät ja noudattavat paremmin sellaisia ohjeita, joita he ymmärtävät. Eräs vastaaja on Kauppakamarien yritysten rikosturvallisuutta kartoittaneessa kyselyssä vastannut, että ”turvallisuusasiat esitetään yleensä liian yleisellä tasolla ilman konkreettisia ohjeita” (2012, 30).

Turvallisuuspolitiikkaa tukemaan tuleekin luoda asiakohtaisia ohjeita, joissa määritellään politiikan mukaiset toimenpiteet (ISO 27002 2017, 5.1.1.; Cappelli ym. 2012, xxii). Ohjeistuksien on liityttävä insider-rikosten toteuttamistapoihin ja -vaiheisiin ja niiden tulisi olla korostuneen yksiselitteisiä seuraavien sääntöjen määrittelyssä:

- yrityksen järjestelmien ja tietojen hyväksyttävä käyttö ja tietojen luokittelu
- tietojärjestelmien ylläpitotilien käyttö
- työssä luotujen tietojen omistusoikeudet
- työntekijöiden suorituksen arviointi, mukaan lukien ylennyksiä ja taloudellisia bonuksia koskevat vaatimukset
- prosessit ja menettelyt työntekijöiden erimielisyyksien käsittelemiseksi (ISO 27002 2017, 5.1.1; Collins 2016, 33.)

Asiatuntijat näkivät turvallisuuspolitiikan vaikutuksen muodostuvan erityisesti johdon osoittaman tuen kautta. ”On tärkeää, että johdon tasolla asti on kirjattu, miten yrityksessä suhtaudutaan liikesalaisuuksiin ja mitkä on pelisäännöt” (Haastateltava E). Uuden liikesalaisuuslain voimaantulon jälkeen arvioidaan, onko yrityksessä toteutettu riittäviä toimenpiteitä tiedon suojaamiseksi, joten on osoitettava että toimintatavat ovat selvät sekä johdolle että henkilöstölle. Haastateltava D totesi myös, että politiikkojen uskottavuuden ja vaikuttavuuden kannalta on tärkeää, että ”ne on tehty yrityksessä, eikä niitä ole vain kopioitu muualta”.

Haastateltava B korosti myös politiikkojen merkitystä koko henkilöstön sitouttamisessa turvallisuustyöhön: ”ihmisten on koettava, että tiedon turvaaminen on tärkeätä. Jos ihmiset kokevat, että turvallisuus kuuluu ainoastaan turvallisuusasiantuntijoiden tehtäviin, ne eivät sitoudu siihen”. Sitouttaminen ei vaikuta välittömästi insideriin itseensä,

mutta myöhemmin käsiteltävien riskien hallintakeinojen tehokkaan toteutumisen edellytyksenä on koko muun henkilöstön osallistaminen insider-riskien hallintaan muun muassa havaintojen tekijöinä.

Haastateltava F viittasi kuitenkin politiikan välittömän vaikutuksen puuttumiseen sanomalla, että "(politiikalla) ei ole minkäänlaista vaikutusta tahallisten insidereiden toimintaan, koska heillä on se oma motiivi ja tämä ei millään lailla vaikuta siihen".

Turvallisuuspolitiikalla voidaankin nähdä olevan ainoastaan välillinen vaikutus tahallisten insider-riskien hallintaan. Vaikutus on kuitenkin merkittävä, koska politiikka osoittaa johdon tuen toteutettaville riskien hallintakeinoille. Politiikka ja ohjeistus eivät siis suoranaisesti vaikuta insideriin ja toimi riskien hallintakeinoina, mutta ne luovat yritykselle ja sen turvallisuustoiminnalle puitteet ja resurssit insider-riskeihin välittömästi vaikuttavien toimenpiteiden luomiseksi.

5.2.2 Suojattavan tiedon tunnistaminen, luokittelu ja priorisointi

Insider-riskien hallintatoimenpiteiden kohdentamiseksi tulee tunnistaa ja määritellä suojattava liikesalaisuustieto. Yrityksen tiedoille saatava liikesalaisuuden suoja on tallenneriippumaton, joten tieto voi olla missä formaatissa tahansa (paperi, sähköinen, suullinen, kuva, video) (HE 49/2018, 55).

Mikäli tietoja ei ole tunnistettu, turvallisuustoiminta ei ole kustannustehokasta ja lisäksi määrittelyn puuttuminen voi johtaa tilanteeseen, jossa salassapitoehtoa ei katsota olevan olemassa ja tarvittava tieto ei saa liikesalaisuuden suojaa (Blankenship 2016, 9; ISO 27002 2017; 8.1.1; Vapaavuori 2016, 63).

Saario & Vesterinen laatiman selvityksen mukaan merkittävä osa Suomessa toimivista yrityksistä ei osaa sanoa, mitä tietoja yrityksen oma työntekijä voisi yrityksestä viedä, joten liiketoiminnalle kriittistä suojattavaa tietoa ei ole tunnistettu. Lähes puolet (43 %) yrityksistä tunnisti kuitenkin liikesalaisuuksiin kohdistuvan yleisen tiedusteluriskin. (2017, 25.)

Vaikka liikesalaisuus ymmärretään yleensä tiedoksi, joka on tiedon syntymisestä lähtien salaista, voi liikesalaisuus kuitenkin muodostua myös julkisten tietojen yhdistelmästä. Tiedot voivat yhteen koottuna tai tietyllä tavalla järjestettynä luoda liikesalaisuutena pidettävän kokonaisuuden, joka nauttii liikesalaisuuden lakisuojaa. Muun muassa Helsingin, Turun ja Kouvolan hovioikeudet ovat yrityssalaisuuksia koskevissa ratkaisuissaan päätyneet tälle kannalle (HE 49/2018, 53.)

Suojattavan liikesalaisuustiedon tunnistamisen jälkeen tieto on luokiteltava tiedon arvon ja kriittisyyden sekä tiedon paljastumisen tai muokkaamisen aiheuttamien seurausten perusteella (ISO 27001 2013, A.8.2.1). Luokittelu helpottaa henkilöstöä käsittelemään ja säilyttämään tietoa oikein. Se myös poistaa tarpeen eri tietojen tilannekohtaisille riskiarvioille ja samalla vähentää tarvetta kalliille erikseen toteutettaville turvallisuusratkaisuille. Saario & Vesterisen mukaan ainoastaan puolella (48 %) selvitykseen vastanneista yrityksistä oli liikesalaisuuksia koskeva luokittelu- ja käsittelyohje (2017, 25).

Yrityksen tietojen luokittelu voidaan toteuttaa esimerkiksi neliportaisesti (Taulukko 8).

TIEDON LUOKKA	TIEDON ILMITULON VAIKUTUS YRITYKSEEN
4	Tiedon ilmitulo ei aiheuta vahinkoa yritykselle
3	Tiedon ilmitulo aiheuttaa vähäisiä taloudellisia tai toiminnallisia vahinkoja yritykselle
2	Tiedon ilmitulo aiheuttaa merkittäviä lyhytaikaisia seurauksia toiminnalle tai operatiivisten tavoitteiden saavuttamiselle
1	Tiedon ilmitulo aiheuttaa vakavia seurauksia strategisten tavoitteiden saavuttamiselle tai vaarantaa yrityksen olemassaolon

Taulukko 8: Esimerkki tiedon luokittelusta ja luokittelukriteereistä (mukaillen ISO 27002 2017)

Politiikkaan perustuvan tasalaatuisen luokittelun seurauksena tiedot voidaan merkitä yhtenäisellä tavalla, jotta henkilöstö osaa käsitellä tietoja turvallisesti. Vapaavuori muistuttaa, että tietojen merkitseminen salaiseksi ei kuitenkaan ole ehdoton edellytys liikesalaisuuden oikeudelliselle suojalle. Merkintä kuitenkin korostaa liikesalaisuudelle asetetun salassapitotahdon ja tosiasiallisen salassapidon vaatimuksen täyttymistä ja osoittaa tietoa käsitteleville henkilöille selvästi tiedon salaisen luonteen.

On kuitenkin vältettävä laatimasta ohjeistusta, jonka mukaan vain luokitellut ja merkityt tiedot ovat liikesalaisuuksia. Mikäli ohjeistuksen mukainen merkintä puuttuisi tai se olisi tehty väärin, yritys saattaisi menettää oikeudellisen suojan. Tästä syystä on tärkeä laatia ohjeistus, jonka mukaan myös muut liikesalaisuudeksi katsottavat tiedot, kuin ohjeen mukaisesti luokitellut ja oikein merkityt tiedot säilyttävät asemansa merkinnöistä huolimatta (2016, 60 & 86).

Yritys voi myös jättää tarkoituksella merkitsemättä jotkin liikesalaisuudet, koska insiderin on helpompi tunnistaa merkityt tiedot arvokkaiksi (ISO 27002 2017, 8.2.2) Yritys voi merkitsemättä jättämisen lisäksi jättää kaikkein kriittisimmän tiedon kokonaan dokumentoimatta, jolloin tieto säilyy ainoastaan muistinvaraisena (Vapaavuori 2016, 83-84).

Liikesalaisuustiedon mahdollisen merkitsemisen jälkeen se on luetteloitava ja luetteloa on ylläpidettävä tietojen ehdottoman jäljitettävyyden varmistamiseksi (ISO 27001 2013, A.8.1.1). Tiedoilla tulee lisäksi olla nimetty omistaja, jonka vastuulla on varmistaa, että tiedot on inventoitu tasaisin väliajoin, ne on luokiteltu oikein ja tiedon tuhoaminen tapahtuu ohjeiden mukaisesti, jotta tietovarkaus on mahdollista havaita (ISO 27002 2017, 8.1.2).

Haastateltujen asiantuntijoiden mukaan suojattavan liikesalaisuustiedon tunnistaminen, luokittelu ja priorisointi-menettely on yksinkertainen, mutta mahdollisesti työläs prosessi, jota useat yritykset eivät ole toteuttaneet.

Tietojen tunnistamiseen ja luokitteluun liittyvän vaikeuden syynä pohdittiin haastatteluissa muun muassa liikesalaisuustietojen hajallaan oloa sekä luokittelutavan jalkauttamista yrityksessä, mitkä molemmat vaativat luokittelupäätöksen aloitusvaiheessa merkittäviä ponnisteluja yrityksessä. Luokittelupäätöksen tekeminen on tärkeää, sillä suojattavan tiedon tunnistaminen luo pohjan insider-riskien hallinnalle.

Haastateltava D korosti luokittelun tärkeyttä toteamalla, että lopulta tiedon luokittelussakin on kyse yrityksen toiminnan jatkuvuuden hallinnasta, joka on elinehto yrityksille. Hän kertoi lisäksi esimerkin suomalaisesta yrityksestä, joka oli pitänyt pitkäkestoiseen tuotekehitykseen perustuneen tuotteensa keskeisimpiä teknisiä tietoja internet-sivuillaan. Myöhemmin yritys teki havainnon, että ulkomainen kilpailija markkinoi täysin identtistä tuotetta alan messuilla. Yritys oli räikeällä tavalla laiminlyönyt liikesalaisuustietoihin liittyvän tunnistamisen, luokittelun ja suojaamisen ja sen vuoksi menettänyt omaan tuotekehitykseensä perustuneen kilpailuedun alan markkinoilla.

Haastateltava C korosti konkreettisena yksityiskohtana ISO 270001-standardissa mainittua tiedon omistajuutta osana insider-riskien hallintaa viittaamalla sanontaan "kaikkien murhe ei ole kenenkään murhe". Silloin kun jokaisella liikesalaisuustiedolla on selvä omistaja ja omistajalla vastuu tiedon hallinnasta, on mahdollista luottaa riskien hallinnan jatkuvuuteen ja riskien arvioinnin perusteella suunniteltujen riskinkäsittelytapojen toteuttamiseen.

5.2.3 Tiedonsaantitarpeen rajaaminen

Tiedon tunnistamisen, luokittelun ja priorisoinnin jälkeen yrityksen tulee tunnistaa henkilöt, keiden on työtehtäviensä perusteella välttämätöntä käsitellä liikesalaisuuksia, koska tiettyyn asiaryhmään valtuuttaminen ei tulisi tarkoittaa automaattista pääsyoikeutta muihin samalle tasolle luokiteltuihin asiaryhmiin (Collins ym. 2016, 11; Blackwell 2009, 56; Valtiovarainministeriö 2008, 37).

Rikoslain uudistamiseen liittyvissä lain perusteluissa (HE 66/1988, 93) esitetään, että "yrityssalaisuus voisi lakata olemasta salaisuus sen jälkeen, kun se on tullut riittävän monen tietoon." Liikesalaisuuden tuntevien piirin tulee siis olla rajattu ja yksilöitävissä. On tärkeä ottaa huomioon, että ratkaisevaa ei ole tiedon tuntevien henkilöiden lukumäärä, vaan ketkä henkilöt tuntevat sen. (Vapaavuori 2016, 67.) Tätä tiedonsaantitarpeen rajausta kutsutaan usein myös sen englanninkielisellä vastineella "need-to-know".

Tiedonsaantitarpeen määrittely on edellä mainitun oikeudellisen näkökulman lisäksi yksi tärkeimmistä insider-riskien todennäköisyyteen ja erityisesti vakavuuteen vaikuttava riskienhallintakeino.

Tiedonsaantitarpeen puutteellinen toteuttaminen on vaikuttanut merkittävästi vahinkoihin, joita insider-vakoilutapaukset ovat yhdysvaltalaisorganisaatioissa aiheuttaneet (DHRA 2017). Periaatteen tehokas toteuttaminen saattaa kuitenkin olla vaikeata, mikäli yrityksen hierarkia ja rakenne on matala ja toiminta perustuu siihen, että henkilöstö käsittelee keskenään samoja tietoja (Contos 2006, 64). Millettin raportissa ongelma on ilmaistu seuraavasti: "Collaborate with everybody but build systems that are resistant to attack" (2000, 7.)

Henkilöstön saaminen noudattamaan tiukkaa rajausta voi vaatia liikesalaisuuksia käsitteleviltä työntekijöiltä ajattelutapamuutosta, koska ihmiset haluavat luontaisesti auttaa muita ja olla yhteistyökykyisiä. Tämä saattaa johtaa siihen, että henkilöstö keskustelee tiedoista tai vastaa liikesalaisuuksia koskeviin kysymyksiin kysyttäessä, vaikka he tietäisivät toimivansa väärin, koska kieltäytyminen sosiaalisessa kanssakäymisessä on vaikeata. (CDSE 2017.) Samaa ihmisluonteeseen liittyvää haavoittuvuutta käyttävät sekä insiderit että tiedustelupalvelut, jotka pyrkivät saamaan kohdehenkilöstä tarvittavaa tietoa tavallisen keskustelun varjolla.

Suomalaisasiantuntijoiden haastatteluissa tiedonsaantitarpeen rajaus nähtiin merkittävänä tekijänä insider-riskien hallinnassa.

Rajauksen todettiin hankaloittavan insiderin tiedonhankintatyötä, mutta toisaalta sen todettiin myös olevan riippuvainen henkilöstön kyvystä ja halusta noudattaa periaatetta. Muun muassa haastateltava F nosti CDSE:n (2017) väittämän mukaisesti esiin tiedonsaantitarpeen rajaamiseen liittyvän periaatteen inhimillisen haavoittuvuuden: ”me ihmiset olemme aika sinisilmäisiä, joten usein riittää, että hän (insider) kysyy kollegalta tai joltain muulta apua ja kaikki ovat valmiina auttamaan”.

Toisena tiedonsaantitarpeen rajauksen jalkauttamiseen liittyvänä haasteena koettiin sen tiedon käytettävyyttä ja työskentelyä mahdollisesti hankaloittava vaikutus. Yritysten tulisi löytää tasapaino tiedon luottamuksellisuuden ja käytettävyyden suojaamisen väliltä.

Haastateltava A pohti ”missä vaiheessa jotain tietoa suojataan niin paljon, että se on jo liiketoiminnalle haitallista? Tasapainon löytäminen on haasteellista. Miten olla turvallisesti avoin ja avoin turvallisesti?” Rajaamisen todettiin olevan mahdotonta tilanteessa, jossa se ei ole olemassa olevien henkilöresurssien vuoksi mahdollista.

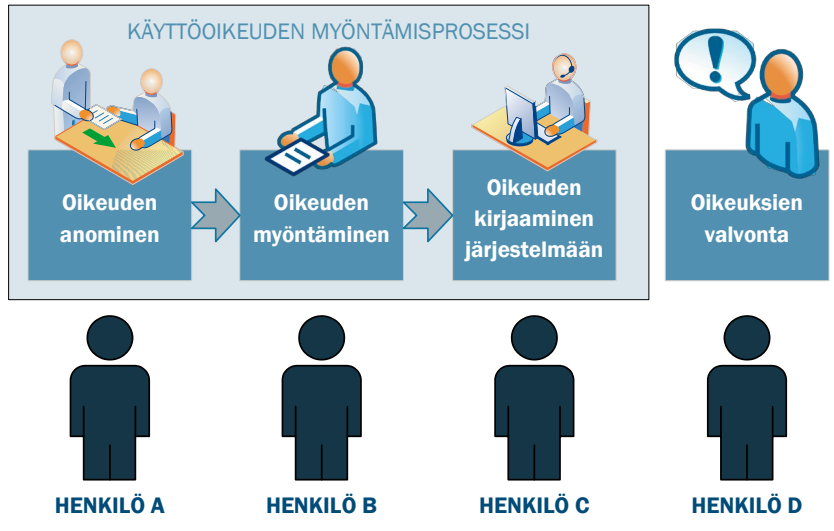
Haastateltava B:n mukaan on useita tehtäviä, jotka ovat yksittäisten henkilöiden varassa, eikä tehtäviin ole osoittaa useampia henkilöitä, joten tiedonsaantitarpeen rajaaminen on käytännössä mahdotonta. Haastateltava C sitoi tiedonsaantitarpeen rajauksen haasteet tiedon käytettävyyden kautta suoraan liiketoiminnan jatkuvuuden vaarantumiseen ja keskeytysriskeihin. ”Mikäli tietty tieto on rajattu liian tiukasti, joitakin toimintoja ei voida jatkaa muiden työntekijöiden toimesta erityistilanteissa.”

5.2.4 Tehtävien eriyttäminen

Tehtävien eriyttämisellä tarkoitetaan yhteen prosessiin liittyvien suoritteiden jakamista useiden henkilöiden kesken, jotta insiderilla ei ole mahdollista varastaa tietoa ilman yhteistyötä muiden työntekijöiden kanssa, mikä lisää insiderin paljastumisen todennäköisyyttä (ISO 27002 2017, 6.1.2).

Tehtävien eriyttämisellä voidaan vaikuttaa myös riskin seurausten vakavuuteen, koska tehokkaasti eriytetyillä valtuuksilla voidaan estää yksittäisen insiderin toiminta kokonaiskuvan muodostamiseksi tietystä tiedosta tai käyttöoikeuden saamisesta rajattuun tietojärjestelmään.

Collins ym. pitävät tehtävien eriyttämistä yhtenä tehokkaimmista insider-riskien hallintakeinoista ja suosittelee sen jalkauttamista osaksi kaikkia liiketoimintaprosesseja. (2016, 97-98.) Esimerkkinä tehtävien eriyttämisestä voidaan käyttää ohjelmiston käyttöoikeuksien myöntämistä, joka on jaettu kolmeen osaan kolmelle eri henkilölle.



Kuvio 12: Tehtävien eriyttäminen (mukaillen Valtiovarainministeriö 2008, 30)

Kuviossa 12 on otettu mallia valtionhallinnon tietoturvallisuuden johtoryhmän ohjeesta, jossa kuvataan eriytetty tietojärjestelmän käyttöoikeuden myöntämisprosessi, jossa yksikään henkilö ei ole käsittelyketjussa vastuussa enempää kuin yhdestä käsittelyketjun kolmesta suorituksesta.

Esimerkkiprosessissa on kolme eriytettyä toimijaa: Henkilö A on käyttöoikeuden tarvitsija, Henkilö B oikeuden myöntäjä ja Henkilö C oikeuden järjestäjä. Lisäksi kuviossa on myöntämisprosessista täysin erillään oleva Henkilö D, joka valvoo tietojärjestelmän käyttöoikeuksia. Tehtävien eriyttämisellä estetään vaarallisten työyhdistelmien muodostuminen tietylle henkilölle.

Useat organisaatiot käyttävät vaarallisten työyhdistelmien estämisessä myös niin sanotun ”kahden henkilön” tai ”neljän silmän” (four eyes) sääntöä. Tällä tarkoitetaan yhtenä toteutusesimerkkinä vaatimusta kahden työntekijän yhtäaikaisesta läsnäolosta jonkin tietyn toimenpiteen suorittamiseksi (Collins ym. 2016, 97). Esimerkkinä tilanne, jossa siirrettävälle muistitikulle voidaan kopioida yrityksen tietojärjestelmästä tietoa ainoastaan kahden työntekijän läsnä ollessa. Säännön tehokkuus perustuu siihen, että työntekijät eivät tutkimusten mukaan yleensä toimi epärehellisesti tilanteissa, joissa he

joutuvat tekemään yhteistyötä muiden työntekijöiden kanssa (Collins ym. 2016, 97). Colen ja Ringin mukaan liikesalaisuustietoja käsitteleviä henkilöitä tulisi lisäksi mahdollisuuksien mukaan vaihtaa aika-ajoin, jotta mahdollisella insiderilla ei olisi yhtä paljon aikaa suunnitella ja toteuttaa tekoa (2005, 15).

Kuten tiedonsaantitarpeen tehokkaan rajauksen toteuttaminen, myös työtehtävien eriyttäminen voi olla vaikeata etenkin pienille yrityksille, koska yrityksissä ei välttämättä ole tarpeeksi henkilöstöä eriyttämisen toteuttamiseksi. (ISO 27002:2017, 6.1.2). Tehtävien eriyttäminen voi myös haitata liiketoimintaa, jolloin tulee riskienhallinnan periaatteiden mukaisesti löytää tasapaino turvallisuuden ja liiketoiminnan välillä. (Collins ym. 2016, 98.)

Tehtävien eriyttäminen koettiin haastateltavien kesken tehokkaaksi keinoksi hallita insider-riskejä, mutta niiden täysimääräinen toteuttaminen voi lopulta tuottaa ongelmia. Periaatteen jalkauttamisessa tunnistettiin samoja haasteita, kuin tiedonsaantitarpeen rajaamisessa.

Työtehtävien eriyttämistä varten tarvittavia rooleja ei ole kaikissa liikesalaisuustiedon suojaamiseen liittyvissä tehtävissä tarpeeksi. Vaarallisten työyhdistelmien välttäminen voi myös tarvittavista resursseista huolimatta vähentää tiedon käytettävyyttä ja jäykistää toimintatapoja liian paljon.

Haastateltava F totesi, että: ”Puhutaan yleensä, että tietoturva hankaloittaa asioita, niin tämähän on juuri siitä se esimerkki, johon me emme halua enää henkilöstön näkökulmasta mennä, ellei siihen ole jotain selkeää tarvetta”. Useat haastateltavat mainitsivatkin, että vaarallisten työyhdistelmien tarkastelu tulisi lähinnä kohdistaa kaikkein arvokkaimpiin liikesalaisuustietoihin kohdistuviin prosesseihin.

Haastateltava G korosti myös vaarallisten työyhdistelmien purkamiseen tähtäävien toimenpiteiden laadukasta toteutusta. Pelkästään kahden henkilön sisällyttäminen jonkin prosessin työvaiheeseen ilman laadullista näkökulmaa ei riitä. Hän kertoo esimerkin tapauksesta, jossa insider pystyi toteuttamaan teon neljän silmän periaatteen jalkautuksesta huolimatta. Tekijän lisäksi eräässä työvaiheessa toisena henkilönä mukana ollut työntekijä ei tuntenut työvaiheen substanssia yhtä hyvin kuin insider, joten toisen henkilön tuottamalla valvonnalla ei ollut tosiasiallista merkitystä kyseisen insider-riskin hallinnassa.

5.2.5 Vähimpien oikeuksien periaate

Lähes kolmella neljäsosalla Cappellin ym. havaitsemista insidereista oli organisaation hyväksymä pääsyoikeus varastamiinsa tietoihin. Tämä ei kuitenkaan tarkoita, että kaikilla havaituilla insidereilla olisi ollut työtehtävistä johtuva välttämätön tarve pääsyoikeuteen juuri kyseisiin tietoihin (2012, 71).

Työntekijöille tulisikin antaa pääsy- ja käyttöoikeuksia eri tietoihin ainoastaan sen verran kuin henkilöllä on välttämätöntä hänen työtehtävänsä hoitamiseksi (Saltzer & Schroeder 1975, 1283). Tätä Saltzerin ja Schroederin edelleen validia sääntöä kutsutaan vähimpien oikeuksien periaatteeksi (least privilege).

Työtehtävien eriyttämiseen ja vähimpien oikeuksien periaatteeseen perustuvilla pääsyoikeuksilla on ratkaiseva merkitys insider-riskien hallinnassa. Estämällä käyttäjän pääsy yhdestä roolista käsin toisessa roolissa sallittuihin tietoihin rajoittaa mahdollisen insiderin aiheuttamaa vahinkoa (Collins ym. 2016, 98.) Toisaalta myös insider-riskien todennäköisyys kasvaa, koska mahdollisuudet tiedon väärinkäyttöön kasvavat, mitä useammalla henkilöllä on oikeudet (Cole & Ring 2005, 8-9). Insider on myös huomattavasti vaikeampi paljastaa, mikäli hänellä on pääsyoikeus tietoon ja hän käyttää tietoa väärin, kuin että insiderilla ei ole pääsyoikeutta, jolloin pyrkimykset päästä tietoon käsiksi voidaan havaita helpommin (Cole & Ring 2005, 21).

Edellä mainittuun pohdintaan liittyen Cole ja Ring ovat tunnistaneet kaksi käyttö- ja pääsyoikeuksiin liittyvää tarkistuskysymystä, jotka tulisi käsitellä insider-riskeihin liittyvien haavoittuvuuksien tunnistamiseksi:

1. Monellako henkilöllä on pääsy johonkin tiettyyn liikesalaisuuksia sisältävään tietoon?
2. Moneenko liikesalaisuuksia sisältäviin tietoihin yksittäisellä henkilöllä on pääsy?

Vapaavuori (2016, 69-70) tukee oikeudellisesta näkökulmasta Cole & Ringin esittämiä insider-riskien hallintaan liittyviä kysymyksiä esittämällä liikesalaisuuksien tosiasiallisen salassapitoehdon käsittelyn yhteydessä oman pohdintansa ”keiden ylipäätään on tarpeen tuntea tiettyä tietoa ja tuleeko jokaisen tuntea kaikki asiaan liittyvä tieto”. Mahdollisen tietovuodon tapahtuessa yritys voi menettää tiedolle asetetun oikeudellisen suojan, jos liikesalaisuus on tullut kokonaan julkiseksi. Tästä syystä on tärkeä pyrkiä rajaamaan käyttö- ja pääsyoikeudet tarkasti, jolloin liikesalaisuuden suojan menettävä tiedon osuus on mahdollisimman pieni liikesalaisuuksien kokonaisuudesta. (2016,

69-70.) Vähimpien oikeuksien periaatteen jalkauttaminen mahdollistaa myös mahdollisen sisäisen tutkinnan tai rikostutkinnan tarkemman kohdistamisen ja teon havaitsemisen (Kont 2015, 29; Saltzer & Schroeder 1975, 1283).

Yritykset voivat tukea vähimpien oikeuksien periaatteen toteuttamista fyysisin, hallinnollisin ja teknisin keinoin (Collins ym. 2016, 98). Periaatteen oikeanlaisella, mutta tehokkaalla toteuttamisella ei estetä kenenkään työntekoa, mutta estetään pääsy sellaisiin tietoihin, joita työntekijä ei tarvitse työssään (Blackwell 2009, 56; Cole & Ring 2005, 10).

Yrityksen tulisi myös ylläpitää vähimpien oikeuksien periaatteen tehokasta toteuttamista jatkuvasti, koska työntekijät vaihtavat yrityksen sisällä tehtäviä ja projekteja. Työntekijän vaihtaessa tehtävää hänen pääsy- ja käyttöoikeuksien laajuus tulisi arvioida jokaisen muutoksen jälkeen uudelleen. Collins ym. (2016, 97) ovat tutkimuksissaan havainneet, että valitettavan usein organisaatiot antavat työntekijöille tarvittavat uudet pääsy- ja käyttöoikeudet ilman, että työntekijöiltä kumotaan aiempaan tehtävään liittyviä uudessa tehtävän suorittamiseksi tarpeettomia oikeuksia. (Collins ym. 2016, 97; Cappelli ym. 2012, 71.)

Liikesalaisuuksiin kohdistuvien pääsy- ja käyttöoikeuksien rajaamisen lisäksi täytyy muistaa, että on henkilöitä, joilla ei ole pääsy- ja käyttöoikeutta tietoon, mutta jotka pääsevät liikkumaan tiloissa, joissa liikesalaisuuksia käsitellään ja säilytetään (Cole & Ring 2005, 11). Tällaisia kulkuoikeuksia pitäisi pystyä rajoittamaan, jotta insider, jolla ei ole suoraa pääsyä tietoon ei saa tiedusteltua tiedon suojaamiseksi suunniteltuja turvallisuustoimenpiteitä (Blackwell 2009, 58).

Pääsy- ja kulkuoikeuksiin liittyvät haavoittuvuudet ovat mahdollistaneet useiden insider-rikosten toteuttamisen (Cole & Ring 2005, 13; Collins 2016, 98. Yrityksen on toteutettava muodollinen pääsyoikeuksien myöntämisprosessi, jonka perusteella voidaan antaa tai kumota pääsyoikeus minkä tahansa tyyppiseltä käyttäjältä mihin tahansa järjestelmään, palveluun tai tilaan (ISO 27001 2013, 9.2.2).

Suomalaisasiantuntijoiden mukaan vähimpien oikeuksien periaatteen noudattamisella on merkittävä vaikutus insider-riskien hallintaan, mutta haastateltavat esittivät myös tähän periaatteeseen liittyviä esimerkkejä puutteellisesta toteutuksesta suomalaisyrityksissä. Vaikka periaate olisi toteutettu työsuhteen alkuvaiheessa onnistuneesti, esitettiin epäilys siitä, otetaanko tehtäviä vaihtaneelta tai toisiin tehtäviin siirretyltä työntekijältä aidosti ylimääräiset aiempaan tehtävään liittyvät oikeudet pois vai seuraavatko vanhat pääsy- ja käyttöoikeudet mukana (Haastateltava B ja D).

5.2.6 Henkilöstön koulutus

Yhdysvaltalaisen Crowd Research Partnersin vuonna 2016 tekemässä kyselytutkimuksessa vastaajat (62 %) pitivät koulutuksen puutetta kaikista suurimpana syynä insider-riskien todennäköisyyden kasvuun (2016, 15).

Yrityksen henkilöstön koulutus on tutkitusti merkittävä osa tietoturvallisuutta, koska ihmisen rooli tietoturvallisuuden toteuttajana on olennainen (Nykänen 2011, 19). Koulutuksella voidaan vaikuttaa välittömästi tahattomasti toimiviin insidereihin (tietämättömät ja välinpitämättömät) sekä välillisesti tahallisesti toimiviin insidereihin (Gelles 2016, 3-5; Collins ym. 2016, 64).

Insider-riskien hallinnaksi tulee järjestää kahdentyyppistä koulutusta. Koulutusaiheet on esitystavan selkeyden vuoksi erotettu toisistaan taulukossa 9.

KOULUTUS	KOHDERYHMÄ	KOULUTUSTAVOITE
Koulutus liikesalaisuuksien tietoturvallisuudesta ydinsisältö: – tiedon luokittelu – tiedon turvallinen käsittely ja säilytys – tiedon turvallisen käsittelyn ja säilytyksen merkitys yritykselle – tietoturvarikkomuksista johtuvat seuraukset ja kurinpitoprosessi – turvallisuusvastaavien yhteystiedot – osoite, josta on saatavissa lisätietoa yrityksen turvallisuusasioista	– liikesalaisuuksien kanssa säännöllisesti ja epäsäännöllisesti työskentelevä henkilöstö	– tietämättömyydestä johtuvien insider-riskien pienentäminen tiedon käsittelyyn liittyvien ohjeiden jalkautuksella – välinpitämättömyydestä johtuvien insider-riskien pienentäminen tietoturva-rikkomuksista johtuvista seurauksista ja kurinpito-prosessista muistuttamalla – työntekijän tietämättömyyteen vetoamisen ennalta estäminen liikesalaisuuksien väärinkäyttöä koskeviin erimielisyyksiin liittyen
Koulutus insider-riskeistä ydinsisältö: – insider-riskien seuraukset yritykselle – aidot esimerkit insider-riskeistä – henkilöstöön kohdistuvien vaikuttamisyritysten tunnistaminen – insider-riskien tunnistaminen – anonyymi ilmoittamiskanava ja sen käyttäminen – työntekijöiden valvonta eri järjestelmissä – insider-riskien käsittelyprosessi ja kurinpitoprosessi	– koko henkilöstö	– tahallisuudesta johtuvien insider-riskien pienentäminen henkilöstön valveutuneisuuden kohottamisella ja ilmoittamiskanavasta tiedottamalla – tahallisuudesta johtuvien insider-riskien pienentäminen insiderille johtuvista seurauksista muistuttamalla

Taulukko 9: Insider-riskien hallinnaksi järjestettävä koulutus

Taulukon 9 ensimmäisellä rivillä kuvatun liikesalaisuuksien tietoturvallisuutta koskevan koulutuksen tarkoituksena on jalkauttaa yrityksen liikesalaisuuksien tietoturvallisuutta koskevat ohjeet, jotka koskevat tiedon luokittelua, käsittelyä ja säilytystä.

Koulutuksen kohderyhmänä tulisi olla liikesalaisuuksien käsittely- ja säilytysprosessiin osallistuva henkilöstö, jotta liikesalaisuuksia koskeva salassapitotahto toteutuu. Koulutus tulisi lisäksi kohdentaa yrityksen hierarkiassa alempana työskenteleville ja sellaisille henkilöille, jotka eivät säännöllisesti työskentele yrityssalaisuuksien parissa, koska mitä korkeammassa asemassa yrityksessä työntekijä on, sitä korkeampi lojaliteettivelvoite hänellä on yritystä kohtaa. (Vapaavuori 2016, 45; HE 66/1988, 92.)

Koulutuksen tavoitteena on tietämättömyydestä johtuvien insider-riskien pienentäminen tietoturvallisuusohjeiden jalkauttamisen avulla. Toinen tavoite on välinpitämättömyydestä johtuvien insider-riskien pienentäminen tietoturvarikkomuksista johtuvista seurauksista ja kurinpitoprosessista muistuttamalla. (ISO 27002 2017, 7.2.3; Gelles 2016, 4; Nykänen 2011, 19-20.) Tietämättömyydestä ja välinpitämättömyydestä johtuvien riskien pienentämiseksi henkilöstöä tulisi kannustaa ilmoittamaan omista virheistään ilman pelkoa sanktioista. (Collins ym. 2016, 61).

Liikesalaisuuksien tietoturvallisuutta koskevalla koulutuksella voidaan pyrkiä myös ennalta estämään tilanne, jossa työntekijä vetoaisi tietämättömyyteensä liikesalaisuuksia koskevissa erimielisyyksissä. Tietämättömyyteen vetoamisesta on havaintoja myös vuosia 2012-2016 käsittelevässä insider-rikostilannekuvassa. Toisaalta korkein oikeus on ennakkopäätöksessään päätynyt siihen ratkaisuun, että yrityksen käsityksellä tiedon salaisesta luonteesta on suurempi painoarvo kuin työntekijän käsityksellä (Vapaavuori 2016, 62; HE 157/2000, 79; KKO:2013:17.)

Liikesalaisuuksia sisältävien tietojen käsittelyprosessiin liittyvän koulutuksen tulisi olla jatkuvaa (Blackwell 2009, 56; Moore ym. 2014, 9). Henkilöstön tietoja tulee päivittää etenkin, jos koulutuksessa käsiteltyihin politiikkoihin tai ohjeisiin on tullut muutoksia (ISO 27001 2013, A.7.2.2).

Taulukon toisella rivillä kuvatun insider-riskejä koskevan koulutuksen tavoitteena on tahallisuudesta johtuvien insider-riskien pienentäminen välillisesti henkilöstön valveutuneisuuden kohottamisella ja oikeiden reagoimistoimenpiteiden kouluttamisella (Gelles 2016, 4; Collins ym. 2016, 64).

Lisäksi tavoitteena on tehdä henkilöstöstä valveutuneita tunnistamaan insider-uhkia ja –riskejä, jalkauttaa anonyymi ilmoittamiskanava henkilöstön käyttöön, tehdä yrityksen insider-riskien käsittelyprosessista läpinäkyvä ja tuoda esiin insider-toiminnan seuraukset ja kurinpitoprosessi henkilöstölle hienovaraisesti. (Blankenship 2016, 11; Parker 2004, 179-180; Cole & Ring 2005, 305.) Kurinpitoprosessin esiintuomisesta ollaan kuitenkin erimielisiä, koska muun muassa Lee & Lee on tutkimuksessaan kyseenalaistanut rangaistusten korostamisen vaikuttavuuden osana tietoturvallisuusriskien hallintaa (2002, 58).

Henkilöstö tulisi myös kouluttaa tunnistamaan heihin kohdistuvat sosiaalisen vaikuttamisen yritykset, koska useisiin insider-tapauksiin perustuvassa yhdysvaltalaistutkimuksessa havaittiin, että insiderit saattavat käyttää sosiaalisen vaikuttamisen keinoja kollegoihinsa esimerkiksi saadakseen heiltä suoraan tietoja tai pääsyn haluamiinsa tietoihin.

Collins ym. esittää lisäksi, että koulutuksessa tulisi mainita projekteista, joissa käsitellään liikesalaisuuksia ja joihin insider-riskit saattavat kohdistua. (Collins ym. 2016, 62.) Erityisesti liikesalaisuuksia sisältävän tiedon kanssa työskenteleviä henkilöitä ja esimiehiä tulisi muistuttaa, että myös vapaa-ajalla tapahtuvalla toiminnalla voi olla vaikutusta tiedon suojaamiseen. Liikesalaisuuksia sisältävää tietoa käsittelevien tai pääsyoikeuteen vaikuttavien henkilöiden heikkouksia voidaan käyttää henkilöä itseään vastaan, jolloin henkilö voidaan yrittää värvätä (Cole & Ring 2005, 324).

Cole & Ring esittää, että insider-riskeihin liittyvää 1-2 tunnin koulutusta tulisi järjestää säännöllisesti, jopa kvartaaleittain, jotta koulutuksella voidaan saavuttaa jatkuva ennaltaehkäisevä vaikutus (2005, 305). Collins ym. (2016, 62) taas esittää koulutusväliksi vuotta. Formaalien koulutusten lisäksi tulisi myös toteuttaa erilaisia turvallisuustietoisuuden tasoa nostavia toimenpiteitä, kuten esimerkiksi teemapäiviä tai painettuja ohjevihkoja ja uutiskirjeitä (ISO 27002 2017, 7.2.2).

Koulutuksia suunnitellessa on myös tärkeä ottaa huomioon Puhakaisen ja Siposen (2010, 757-776) sekä Nykäsen (2011, 20-28) tutkimukset **vaikuttavasta tietoturvallisuuskoulutuksesta:**

- Tietoturvallisuustietoisuus muodostuu tietämyksestä ja asenteesta. Koulutuksella voidaan kehittää henkilöstön tietoisuutta, mikä vaikuttaa ihmisten motivaatioon ja asenteisiin ja tukee toivottua tietoturvakäyttäytymistä
- Koulutuksen tulee olla jatkuvaa, hyvin suunniteltua ja tavoitteellista, jotta henkilöstö saa riittävästi tietoturvallista toimintaa tukevaa informaatiota. Koulutuksen vaikuttavuutta pitää pystyä arvioimaan

- Koulutuksen suunnittelun tulee pohjautua ihmisen käyttäytymiseen liittyviin teorioihin
- Koulutus tulisi sitoa normaaliin työskentelyyn, jotta koulutettavat eivät pitäisi tietoturvallisuutta omasta työstä erillisenä saarekkeena. Koulutuksessa tulisi käyttää oppimistehtäviä, joilla on henkilökohtaista merkitystä koulutettaville, jotta näkyvät seuraukset koulutettavalle ja muille ovat selvästi nähtävissä
- Tulee käyttää sellaisia menetelmiä, joka motivoi ja saa ihmiset ajattelemaan
- Koulutuksen tulisi olla vuorovaikutteista ja koulutettavien tulisi pystyä keskustelemaan käsiteltävistä aiheista
- Ylimmän johdon koulutukselle antama näkyvä tuki on välttämätöntä, jotta henkilöstö omaksuu koulutetut asiat ja noudattaa niitä

Haastateltavien mielestä tietoturvallisuuteen liittyvä koulutus on aina hyödyllistä, mutta insider-riskien hallintaan liittyvä koulutus tulee kohdistaa oikein, jotta se olisi vaikuttavaa.

Haastateltava A:n mukaan yleinen tietoturvallisuuskoulutus vaikuttaa ainoastaan tahattomiin insidereihin, mutta jos koulutus käsittelee valvontaa ja sanktioita voi vaikutus laajeta myös tahallisiin itsenäisesti toimiviin insidereihin. Toisaalta hän huomautti, että on ”vaikea nähdä, että minkään tyyppisellä koulutuksella olisi vaikutusta”, millä hän viittasi kolmannelle osapuolelle toimiviin värvättyihin tai yritykseen solutettuihin insidereihin. Myös Haastateltava C totesi, että ”jos puhutaan valtiollisesti ohjatuista toimijoista, niin (koulutuksen) vaikutus laimenee, koska työntekijä on jo toisen isännän palveluksessa”.

Haastateltavat B ja D näkivät, että turvallisuusasioiden lisäksi henkilöstöllä tulisi olla tieto insider-uhkista ja jo pelkkä asioista puhuminen nostaa kynnystä toimia väärin.

Sanktioiden esiin tuomisella nähtiin sekä positiivinen että negatiivinen vaikutus. Sanktioilla todettiin olevan ennaltaestävä vaikutus, mutta se saattaa aiheuttaa myös niin sanottua opittua avuttomuutta, joka voi tehdä henkilöstöstä ylivarovaista ja passiivista virheiden tekemisen pelossa. Sanktioista puhumisella nähtiin olevan mahdollisuus vaikuttaa itsenäisesti toimiviin insidereihin, mutta varmempana pidettiin sen negatiivista vaikutusta muuhun henkilöstöön. Haastateltava F:n mukaan ”sillä, että lähtee edes suunnittelemaan vertaisvalvontaa, sanktioita tai muuta vastaavaa saa mittavia vahinkoja aikaan työtyytyväisyydessä.”

Yhtenä ajatuksena esitettiin, että tahallisia insidereita koskevan koulutuksen kanssa tulisi edetä hitaasti askel kerrallaan, koska yhdellä kertaa esitettynä aihe voi aiheuttaa voimakkaita negatiivisia reaktioita henkilöstön keskuudessa. Aihetta voitaisiin lähestyä aluksi tahattomiin insidereihin liittyvän teeman kautta, jolloin henkilöstölle saadaan viestittyä pehmeällä tavalla, että myös he voivat itse olla riskin lähde. Tämän jälkeen olisi mahdollista kouluttaa henkilöstöä tekemään havaintoja ympäristöstään ja ilmoittamaan niistä. Pidemmän ajan kuluessa olisi mahdollista siirtyä puhumaan henkilöstössä olevista tahallisista uhkista ja niihin liittyvien havaintojen ilmoittamisesta, koska yrityksessä olisi siihen mennessä totuttu pitämään myös omia työntekijöitä riskin lähteenä ja ihmislähtöisistä turvallisuushavainnoista ilmoittaminen olisi tässä vaiheessa jo osa turvallisuuskulttuuria.

”Väittäisin, että aika monessa organisaatiossa kyllä tiedetään, että meillä on sellainen henkilö, joka on aika utelias, mutta tavallaan tuota kautta (henkilöstön koulutuksella insider-tekijää koskevista indikaattoreista) ehkä voitaisiin jopa tällainen henkilö saada kiinni” (Haastateltava F).

5.2.7 Työhyvinvointi

Kuten aiemmin on esitetty, insiderin motivaatiolähteenä voivat olla hyvin erilaiset asiat. Riippumatta motivaation lähteestä, työpaikan olosuhteet vaikuttavat merkittävästi työntekijöiden hyvinvointiin ja teon motivaatio voi olla välittömästi johdettu työpaikan huonoista olosuhteista. Tyytymättömyys on ollut useiden havaittujen insidertekojen motivaation juurisyy (CPNI 2013, 10).

Sisältä värvättyjen insidereiden ensisijaisena motivaation lähteenä on harvoin viha, mutta huonoilla työolosuhteilla voi olla vaa`ankielimerkitys, jos henkilö on kahden vaiheilla ryhtyykö hän laittomaan tekoon vai ei. Yleensä vihan tunne kasvaa ajan saatossa ja siihen vaikuttaminen voi estää insider-uhkan muodostumisen. (Cole & Ring 2005, 306 & 310.)

Hollingerin empiirisessä tutkimuksessa (1986, 53-71) sosiaalisen siteen vaikutuksesta työnantajaa kohtaan tehtyihin rikoksiin havaittiin, että työntekijät toteuttavat työnantajaan kohdistuvia rikoksia sitä herkemmin, mitä heikommin he ovat sitoutuneet organisaatioonsa. Yritys voi yrittää vaikuttaa ongelmaan työhyvinvoinnin, oikeudenmukaisen ja tasapuolisen kohtelun, tehokkaan sisäisen viestinnän sekä epäkohtiin puuttuvan toiminnan kautta. (Blackwell 2009, 23-24, 34 & 51.)

Voidaan myös kysyä luovatko insider-riskien hallintaa varten asetetut liian tiukat turvallisuuskontrollit paradoksin, jossa kontrollien kasvaessa työntekijöiden työhyvinvointi laskee ja kasvava tyytymättömyys luo insider-uhkan? Tutkimusten mukaan osa tyytymättömistä insidereista ei edes välitä kiinnijäämisriskistä, koska heidän ainoa tavoitteensa on päästä työnantajan kanssa "tasoihin". Tämä tekee tyytymättömyydestä motivaationsa saavista insidereista vaikeita pysäyttää. (NITTF 2016, 6.)

Psykologi Frederick Herzberg (1968, 56) esittää edelleen 2000-luvulla laajasti viitatussa kaksifaktoriteoriassa, että työtyytyväisyys ja työtyytymättömyys ovat riippumattomia toisistaan, eivätkä ne ole toistensa vastakohtia. Tutkimus pyrkii osoittamaan vääräksi yleisen tavan esittää työtyytyväisyyttä lisäävien tekijöiden olevan samalla työtyytymättömyyttä vähentäviä tekijöitä.

Herzbergin tutkimustulokset osoittavat, että niin sanotuilla motivaatiotekijöillä on merkittävin vaikutus työtyytyväisyyteen ja hygieniatekijöillä työtyytymättömyyteen. Herzbergin kaksifaktoriteoriaan liittyvät tutkimustulokset on tiivistetty taulukkoon 10.

KAKSIFAKTORITEORIA			
MOTIVAATIOTEKIJÄT		HYGIENIATEKIJÄT	
Työtyytyväisyys	Saavutukset	Yrityspolitiikka ja johto	Ei-työtyytymättömyys
	Tunnustuksen saaminen	Esimiessuhde	
	Työ itsessään	Työolot	
	Vastuun kokeminen	Palkka	
	Etenemismahdollisuudet	Asema	
	Henkilökohtainen kasvu	Suhde kollegoihin	
		Suhde alaisiin	
		Henkilökohtainen elämä	
Ei-työtyytyväisyys		Turvallisuus	Työtyytymättömyys

Taulukko 10: Työasenteisiin vaikuttavat tekijät (mukaillen Herzberg 1968, 56-58)

Taulukossa 10 motivaatiotekijät liittyvät ihmisten kokemiin seurauksiin siitä, mitä he työssään tekevät. Motivaatiotekijöiden läsnäolo tyydyttää työntekijän työlle asettamat perusvaatimukset ja lisää työntekijän tuottavuutta ja työtyytyväisyyttä.

Toisin kuin motivaatiotekijät, hygieniatekijät liittyvät työympäristöön. Hygieniatekijöihin liittyvien olosuhteiden parantaminen voi vähentää työtyytymättömyyttä, mutta se ei merkittävästi lisää työtyytyväisyyttä. Kaksifaktoriteorian perusteella yritysten tulisi huolehtia sekä hygieniatekijöistä että motivaatiotekijöistä, jotta voidaan ennaltaehkäistä työntekijöiden työtyytymättömyyttä sekä parantaa työtyytyväisyyttä. (Miner 2005, 63.)

Ihmisten käyttäytyminen tarjoaa monia mahdollisuuksia virheisiin, erityisesti niille, jotka kiirehtivät suorittamaan useita tehtäviä korkeassa stressiympäristössä. Virheiden lisäksi työpaikasta johtuva korkea stressi aiheuttaa huonon mielen lisäksi suuremmat mahdollisuudet haitallisen insider-toiminnan syntyyn. Tällöin tuottavuuden edistäminen saattaa vaikuttaa negatiivisesti sekä tehokkuuteen että turvallisuuteen. Kun työntekijät kiirehtivät, he tekevät enemmän virheitä ja tuntevat, että heidän huolenaiheitaan ei oteta vakavasti ja heille saattaa kehittyä negatiivisia tunteita yritystä ja johtoa kohtaan. Virheet voivat ilmetä esimerkiksi siten, että työntekijä ei tunnista häneen kohdistettuja sosiaalisen vaikuttamisen merkkejä, työntekijä voi olla piittaamaton turvallisuusohjeita kohtaan tai työntekijä voi vahingossa paljastaa liikesalaisuuksia jakaessaan julkista tietoa ulkopuolisille. (Collins 2016, 57.)

Yritys voi pienentää insider-riskien todennäköisyyttä toimenpiteillä, jotka vähentävät työntekijöiden stressitasoa erityisesti niissä tehtävissä, jotka liittyvät liikesalaisuuksien käsittelyketjuun.

Stressitasoa on mahdollista vähentää keskittymällä sellaisten toimintatapojen ja käytäntöjen luomiseen, jotka tarjoavat työntekijöille enemmän aikaa tavoitteiden saavuttamiseen, muuttamalla johtamistapaa projektisuuntautuneisesta johtamistavasta ihmisiin suuntautuneemmaksi ja antamalla aikaa tehtävien suunnitteluun ja yritystä hyödyttävien uusien ideoiden keksimiseen. Esimerkiksi asiantuntijatyötä tekevien ja tuotantolinjatyötä tekevien kokemukset sopivista työtehon mittaustavoista voivat erota merkittävästi. (Collins 2016, 57 & 142.)

Työhyvinvointi-teemaa käsitelleet asiantuntijat olivat yksimielisiä työhyvinvoinnin vaikututuksesta insider-riskien hallintaan.

Haastateltava B totesi, että ”on paljon korkeampi kynnys lähteä pettämään oma yritys, jos työhyvinvoinnista on huolehdittu hyvin”. Lisäksi haastateltavat A ja E argumentoivat lähes identtisesti useiden Herzbergin tutkimuksissa esiin tuotujen yleisten työhyvinvointia ja sitoutumista lisäävien tekijöiden puolesta. Työhyvinvoinnin todettiin olevan sidoksissa enemmän työntekoon liittyviin tekijöihin, kuin ulkoisiin muun muassa työvälineitä koskeviin tekijöihin.

Työhyvinvoinnin ja muiden työssäoloa tukevien toimenpiteiden vaikutuksen koettiin kohdistuvan erityisesti työntekijöihin, jotka ovat jostain syystä menettäneet elämänhallintansa ja ovat enemmän haavoittuvia värväykselle (Haastateltava B). Yhtenä tällaisena hallinnollisena keinona korostettiin muun muassa hyvin toteutettua päihdeohjelmaa, joka on työterveyshuoltolain (1383/2001) mukaan pakollinen yrityksille, jotka teettävät huumausainetestejä työntekijöistään (Haastateltava D).

Haastateltava A kertoi työhyvinvoinnin merkitykseen liittyvänä esimerkkinä tapauksen omaa tutkimustaan varten haastattelemastaan henkilöstä. Henkilö toimi yrityksessä myyjänä ja yrityksen johto oli sovitusta poiketen jättänyt maksamatta hänelle kuuluvat bonukset yhdessä käydyistä keskusteluista huolimatta. Haastateltava A oli samoihin aikoihin haastatellut myyjää yrityksen tietoturvallisuudesta, johon myyjä oli vastannut, että yrityksen tietoturvallisuutta koskevat ohjeet ”eivät voisi vähempää kiinnostaa tällä hetkellä”. Viitaten haastateltavien yhteiseen näkemykseen työhyvinvoinnin vaikuttavuudesta ja Haastateltava A:n esimerkkiin työntekijän reaktiosta voidaan ajatella, että työhyvinvoinnin ongelmat luovat niiden keston ajaksi selvän aikaikkunan sekä värväykselle että itsenäisesti toimivalle insiderille aktivoitua.

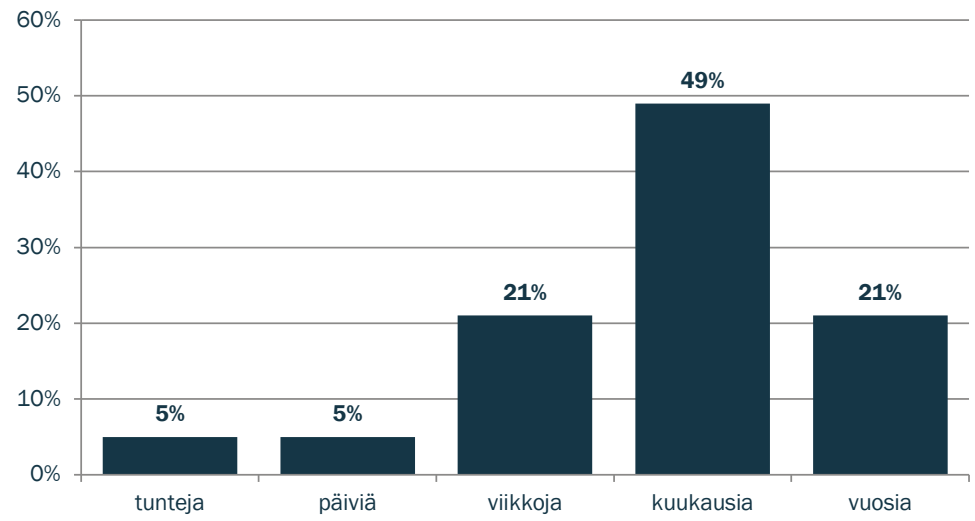
5.3 Teon paljastaminen ja työsuhteen päättymisvaiheen riskien hallintakeinot

5.3.1 Teon havaitseminen

Proaktiivisten riskienhallintatoimenpiteiden sijaan muun muassa Cole & Ring ovat painottaneet, että insider-teon ja sen ennusmerkkien havaitseminen on teon ennaltaehkäisemiseen pyrkimistä tärkeämpää, jotta rikolliseen toimintaan voidaan puuttua ajoissa ja estää laajemmat vahingot.

Etenkin suunnitelmallisesti ja jälkiään peitellen toimivien insiderien tekoja on vaikea ennaltaehkäistä, jolloin tärkeämmäksi muodostuu teon havaitseminen. Ongelmana on, että usein insider paljastuu vasta vahingon tapahduttua, eikä ennen sitä. Yritys saattaa huomata teon vasta kuukausien, jopa vuosien kuluttua tai ei huomaa tekoa koskaan. Havainnon viivästyminen haittaa teon selvittämistä, koska muun muassa erilaisia lokitietoja ei säilytetä pysyvästi ja epäillyn insiderin taustaan tai käytökseen liittyviä asioita voi olla mahdoton selvittää jälkikäteen. (2005, 16, 37-38 & 312-313.)

Myös Jackson korostaa insiderin havaitsemisen merkitystä toteamalla, että vaikka rekryitointivaihe olisi suoritettu aukottomasti ihmiset muuttuvat ajan kuluessa, saattavat tulla tyytymättömiksi ja voivat kääntyä työnantajaansa vastaan (2012, 283). Usein itsenäisesti toimivan insiderin toteuttaman rikoksen viimeisenä laukaisimena toimii esimerkiksi työsuhteen päättämisestä saatu tieto tai kurinpidollinen tapahtuma (Blackwell 2009, 34). Tarkemmin tarkasteltuna insiderin havaitseminen ei välttämättä kohdistu itse tekoon vaan rikoksen valmistelun ja/tai kolmannen osapuolen suorittaman värväyksen aiheuttamiin muutoksiin työntekijässä.



Kuvio 13: Pääsy- ja käyttöoikeuksien väärinkäytön havaitsemiseen kulunut aika tekohetkestä laskettuna (n=358) (mukaillen Verizon 2016, 38)

Kuviossa 13 on esitetty vuonna 2016 havaittujen pääsy- ja käyttöoikeuksien väärinkäytöstapauksen havaitsemisaika tekoajankohdasta laskettuna. Verizonin ja sen yhteistyökumppaneiden tietoihin perustuva kuvio esittää niiden vuonna 2016 havaittujen insider-tapausten havaitsemiseen kulunutta aikaa, joista oli saatavissa teko- ja havaitsemisajankohtatieto (n = 358).

Tilastojen perusteella insider-teko havaittiin 70 %:ssä tapauksista vasta kuukausien tai vuosien päästä teon tapahtumis- tai alkamisajankohdasta. Ainoastaan 10 % tapauksista havaittiin päivien sisällä tekohetkestä. (Verizon 2016, 38). Myös CPNI on tutkinut insider-riskien havaitsemisaikaa ja todennut, että vain hieman yli puolet tutkituista tapauksista (n=120) havaittiin edes vuoden sisällä (2013, 9).Suomessa poliisiasiain tietojärjestelmään kohdistettujen tilannekuvarekisterihakujen perusteella havaittiin joidenkin insider-tapausten teko- ja havaitsemisajan välin olevan Verizonin tilastojen mukaisesti kuukausia tai jopa vuosia.

Cappellin ym. esittää tutkimustulostensa johtopäätöksenä, että yrityksestä pois lähtevän työntekijän verkkokäyttäytymistä ja sähköpostin käyttöä tulisi valvoa tarkemmin kolmekymmentä päivää ennen työsuhteen päättymistä ja kolmekymmentä päivää työsuhteen päättymisen jälkeen, koska useimmat insiderit vievät tietoa 60 päivän aikaikkunassa ennen tai jälkeen työsuhteen päättymishetkestä (2012, 75-76). Tämä on kuitenkin suomalaisyrityksille ongelmallista nykyisen tietosuojalainsäädännön vuoksi. Kuvion 12 perusteella yritykset voisivat kuitenkin hyötyä pidempikestoisesta monitoroinnista työsuhteen päättymishetkellä, koska vain harva insider-teko havaittiin tuntien, päivien tai edes viikkojen sisällä tekohetkestä.

Useissa havaituissa insider-tapauksissa joku muu henkilö tekijän lisäksi oli tiennyt tulevasta teosta etukäteen tai oli epäillyt jotain tapahtuvan.

Niissä tapauksissa, joissa kohdeorganisaation ulkopuolinen on tiennyt teosta etukäteen, insider on itse kertonut asiasta henkilölle. Tämä henkilö on usein insiderin puoliso tai hyvä ystävä. Jotkin insiderit saattavat myös kehuskella tulevalla tai tapahtuneella teolla läheisilleen tai ystävilleen. Tämän voidaan olettaa tapahtuvan etenkin silloin, jos insider on halunnut kostaa työnantajalleen ja hän haluaa huomiota teolleen, koska tekijä ei saa täyttä tyydytystä teostaan, jos kukaan ei tiedä hänen tehneen sitä. (Cole & Ring 2005, 205, 316.) Insidereilla on lisäksi taipumusta samaan, kuin muilla varkailla tai petoksen tekijöillä: heistä tulee ahneita (Contos 2006, 59). Colen ja Ringin mukaan noin puolet insidereista on jäänyt kiinni, kun tekijä on tarjonnut tietoja kilpailevalle yritykselle, joka on ottanut yhteyttä viranomaisiin (2005, 21).

Olennaista uhkan havaitsemisessa on tunnistaa muutokset käyttäytymisessä. Erityisesti insiderin esimiehillä ja kollegoilla on mahdollisuus tunnistaa insider käytöksen perusteella, koska he käyvät jatkuvasti keskusteluja henkilön kanssa ja ovat hänen kanssaan

tekemisissä päivittäin (Blankenship 2016, 7). Cappellin ym. tutkimusten mukaan 72 % tekijän paljastaneista kohdeorganisaation työntekijöistä olikin ei-teknisessä roolissa ja insiderin paljastuminen perustui muuhun kuin tekniseen valvontaan (2012, 74).

Cole & Ring (2005, 307) nostavat erityisesti näkyvän vihan tunteen yhdeksi merkittävimmistä insider-indikaattoreista, koska vihan tunnetta on vaikea peitellä muilta kollegoilta ja esimiehiltä. Myös tyytymättömyyden merkit ovat usein nähtävissä kauan ennen insiderin toteuttamaa tekoa (Collins ym. 2016, 64). Shaw ym. mainitsee kuitenkin tutkimuksessaan, että nykytekniikalla saattaa olla haitallinen vaikutus insider-uhkan havaitsemiseen. Havaitsemisen vaikeutta voi kasvattaa muun muassa kasvokkain tai puhelimessa käytyjen keskustelujen siirtyminen enenevässä määrin erilaisiin pikaviestintäsovelluksiin ja sähköpostiin, jossa tyytymättömyys, stressi ja muut voimakkaat tunteet saattavat jäädä helpommin muilta huomaamatta. (Shaw ym. 1998, 27-47.) Insiderin havaitsemista saattaa vaikeuttaa myös henkilön tuntema vahva omistajuus liikesalaisuustietoon, jota hän on ollut mukana luomassa. Insider ei tällaisessa tilanteessa koe välttämättä toimivansa väärin varastaessaan tietoa, jolloin hänen käyttäytymisensä ei kaikilta osin muutu tekoa toteutettaessa. (Cappelli ym. 2012, 81.)

Etenkin yritykseen suunnitellusti solutettua insideria ja hänen toteuttamaa tekoa voi olla äärimmäisen vaikea havaita, koska ulkomaisten tiedustelupalvelujen Suomeen kohdistama toiminta on luonteeltaan pitkäkestoista ja mahdollisella insiderilla ei ole toimissaan kiire (Suojelupoliisi 2018, 20; Cole & Ring 2005, 324).

Myös yrityksen sisältä värväämän insiderin havaitseminen on vaikeampaa, koska etenkin tiedustelupalvelulle toimiva henkilö on kurinalaisempi, hän huolehtii operaatioturvallisuudesta eikä vaaranna tiedonhankintaa kehuskelemalla teollaan (Cole & Ring 2005, 316). Kolmannen osapuolen värväämän insiderin motiivina ei myöskään välttämättä ole tyytymättömyys työnantajaa kohtaan, vaan taloudellinen hyöty. Taloudellista hyötyä tavoittelevan insiderin ei tarvitse peitellä vihan tai tyytymättömyyden tunnettaan, joten insider-uhkan havaitseminen käyttäytymisen perusteella on vaikeampaa. Toisaalta kolmannen osapuolen värvätylle insiderille asettamat vaatimukset kasvavat yleensä ajan kuluessa. Tämä saattaa aiheuttaa muutoksia insiderin käytöksessä, mikäli tekijä joutuu hankkimaan tietoa koko ajan enemmän ja nopeammin. (Cole & Ring 2005, 312.)

Taulukossa 11 on kuvattu insider-uhkaan liittyviä indikaattoreita, joilla voidaan pyrkiä tunnistamaan henkilö, jolla saattaa olla kohonnut riski toimia insiderina.

	INSIDER-UHKAINDIKAATTORIT		
	LUONTEENPIIRTEET	**ELÄMÄNTAPAMUUTOKSET JA HENKILÖKOHTAISIIN OLOSUHTEISIIN LIITTYVÄT HAAVOITTUVUUDET**	**TYÖPAIKKAKÄYTTÄYTYMINEN**
SELITE	Luonteenpiirteet on määritelty yksilön ominaispiirteiksi, jotka liittyvät tilanteeseen vastaamiseen ja vuoro- vaikutukseen muiden kanssa	Elämäntapamuutokset ovat määritelty sellaisiksi muutoksiksi henkilökohtaisissa olosuhteissa, jotka saattavat lisätä stressiä tai rasitusta ja johtaa tyytymättömyyteen. Henkilökohtaisiin olosuhteisiin liittyvät haavoittuvuudet määriteltiin ongelmiksi, jotka voisivat tehdä henkilön haavoittuvaksi	Työpaikkakäyttäytymiseen liittyvät toimintamallit luokiteltiin joko epäilyttäväksi (odottamattomat tai vaikeasti selitettävissä olevat toimet, jotka aiheuttavat huolta) tai luvattomaksi (toimet, jotka voivat olla osa normaalia työn roolia, mutta ovat luvattomia) toiminnaksi
HYÖDYNTÄMINEN	Luonteenpiirteitä pidettiin erityisen tärkeinä, kun havaittiinhuomattavia merkkejä, joilla oli selvä ja kielteinen vaikutus työhön ja/tai kollegoihin	Elämäntapamuutosten ja henkilökohtaisiin olosuhteisiin liittyvien haavoittuvuuksien katsottiin olevan erityisen mielenkiintoisia, kun havainnoissa esiintyi toistuvia ja/tai selkeitä merkkejä, joilla oli merkittävä kielteinen vaikutus	Työpaikkakäyttäytymistä koskevia havaintoja pidettiin erityisen mielenkiintoisina, kun havaittiin toistuvia merkkejä ja työntekijällä ei todennäköisesti ollut riittävää selitystä toiminnalleen
	Epäkypsä esimerkiksi henkilöltä puuttuu elämän- kokemusta, hän on naiivi ja vaatii kohtuutonta ohjausta, hänellä on vaikeuksia tehdä omaa elämää koskevia päätöksiä	**Huono työasenne** esimerkiksi ei noudata vakiintuneita menettelytapoja, ei lue tai noudata yrityksen antamia ilmoituksia ja ohjeita	**Epätavallinen tietojen kopiointi** esimerkiksi käyttää tietokonetta sellaisten liikesalaisuuksien kopioimiseen, jotka eivät liity työtehtäviin, peittää tai poistaa tiedon luokitusmerkinnät asiakirjoista kopioinnin yhteydessä, kopioi tiedot muissa työhuoneissa, vaikka kopiokoneita olisi käytettävissä lähempänäkin
	Alhainen itsetunto esimerkiksi luottamuksen puute, hän on erittäin riippuvainen tunnustuksesta ja kiitoksesta, hänellä on vaikeuksia selvitä vastoinkäymisistä ja vaikeista tehtävistä	**Stressi** esimerkiksi alakuloinen, aiempaa hermostuneempi, on muistiongelmia, päätösten tekeminen on vaikeata, keskittymiskyvyttömyyttä ja/tai sekaannusta	**Epätavallinen IT-toiminta** esimerkiksi suorittaa avainsanahakuja arkaluonteisessa tietokannassa, johon työntekijällä ei ole tiedonsaantitarvetta, toimii organisaation tietojärjestelmissä epätavallisella tavalla ennen ulkomaan matkaa
	Moraaliton ja epäeettinen esimerkiksi henkilöltä puuttuvat moraaliset arvot, hän toimii häikäilemättömällä tavalla ja ei osoita katumusta, käyttäytyy epäeettisesti	**Haavoittuva elämäntapa** esimerkiksi hyödynnettävissä oleva heikkous, kuten vakava taloudellinen, alkoholi-, uhkapeli- tai huumeongelma, voi olla hylännyt työnantajan tarjoamia työterveyspalveluja tai jättänyt huomioimatta hoitosuosituksia	**Liikesalaisuuksien luvaton käsittely** esimerkiksi säilyttää tai siirtää liikesalaisuustietoja sopimattomalla tavalla ilman hyväksyntää, luovuttaa tietoja sopimattomalla tavalla ilman lupaa tai vastaanottajan tiedon-saantitarpeen tarkastamista, pyytää muita hankkimaan pääsyoikeuden tietoon, johon hänellä itsellään ei ole oikeutta
	Pinnallinen esimerkiksi on vaikeasti tutustuttava, herättää ihmisissä erilaisia mielipiteitä työpaikalla	**Haavoittuva työprofiili** esimerkiksi on pääsy liikesalaisuuksia sisältäviin tietoihin ja mahdollisuus auttaa ulkopuolisia pääsemään tietoihin käsiksi	**Tietoturvariikkomukset** esimerkiksi pettää annetun luottamusaseman, rikkoo tietoturvallisuusmääräyksiä
	Taipuvainen haaveiluun esimerkiksi uskoo, että työyhteisö harjoittaa toimintaa, joka ei perustu todellisuuteen, haluaa luoda vaikutelman, että he harjoittavat jotain erityistä	**Viimeaikaiset negatiiviset elämäntapahtumat** esimerkiksi työpaikkaongelmat, jotka johtavat statuksen menetykseen, merkittävä vammautuminen, perheenjäsenen tai läheisen ystävän kuolema, parisuhteen päättyminen, taloudelliset vaikeudet	
	Levoton ja impulsiivinen esimerkiksi vaatii jatkuvasti virikkeitä eikä voi sietää ikävystymistä, tarvitsee tai etsii hetkellistä tyydytystä ja tekee sitä, mikä tuntuu sillä hetkellä hyvältä, siirtyy jatkuvasti yhdestä asiasta toiseen		
	Velvollisuudentunnoton esimerkiksi ei noudata sääntöjä, laiminlyö velvollisuuksia, eikä ole kiinnostunut tehtävistä ja vaatimuksista, ei osoita tarpeeksi huomiota yksityiskohtiin, eikä keskity		
	Manipuloiva esimerkiksi käyttää viehätystään ja on hyvin vakuuttava saadakseen tahtonsa läpi, ylläpitää suhteita ja manipuloi muita palvelemaan omaa etuaan, pyrkii saavuttamaan minkä tahansa aseman tai toimimaan tavalla, joka hyödyttää häntä itseään		
	Tunteiltaan epävakaa esimerkiksi on altis liioitelluille mielialan vaihteluille, ylireagoi ongelmiin, valittaa merkityksettömistä tai vähäpätöisistä asioista		
	Todisteet psykologisista häiriöistä tai persoonallisuushäiriöistä		

Taulukko 11: Työsuhteen aikana käytettävät insider-uhkaindikaattorit (mukaillen CPNI 2013, 11-12)

Taulukon tiedot perustuvat pääosin CPNI:n tutkimusraportissa (2013, 11-12) esittämiin arvioihin insider-tekijöiden tunnusmerkeistä. Tutkimuksessa tarkasteltiin erilaisiin luonteenpiirteisiin, elämäntapaan ja yksityiselämän olosuhteisiin sekä työpaikalla tapahtuvaan käyttäytymiseen liittyvien tekijöiden vaikutusta insider-uhkien todennäköisyyteen niissä tapauksissa, joita on saadun aineiston perusteella pystytty tutkimaan tarkemmin.

Taulukkoa tarkastellessa on huomioitava, että sen sisältämät insider-uhkaindikaattorit perustuvat tutkimuksiin, joissa on tutkittu tietoon kohdistuvien oikeudettomien hankkimis- ja käyttämistapausten lisäksi myös muihin insider-riskilajeihin liittyviä tekijöitä. Huomionarvoista on myös, että yhden tai useamman indikaattorin sopiminen tietyn työntekijän profiiliin ei tarkoita, että henkilö olisi insider. Myöskään työntekijä, jonka profiiliin yksikään indikaattori ei sovi, ei automaattisesti tarkoita sitä, ettei hän voisi olla insider. (NITTF 2016, 7; CPNI 2013, 11.)

Collins ym. mukaan (2016, 61) on kuitenkin olemassa tiettyjä merkkejä, jotka voidaan yhdistää henkilöihin, joilla saattaa olla kohonnut riski toimia insiderina.

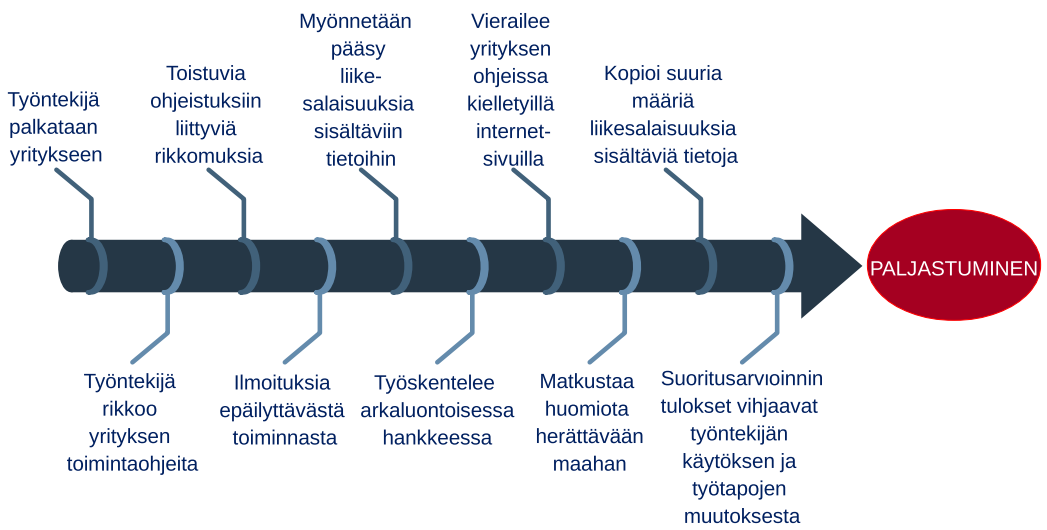
Parker ym. (2004) tutkimuksen johtopäätöksissä korostetaan erityisesti, että insider-toiminnan aikaikkuna tulisi pitää mahdollisimman pienenä ja tekoon puuttuminen tulisi tehdä välittömästi, kun siitä on viitteitä.

Insider-tapauksista tehdyn otannan perusteella on huomattu, että henkilön työskentelyyn liittyvien ongelmien alkamisesta kului kahdestatoista päivästä yhdeksääntoista kuukautta aikaa ennen insider-rikoksen toteuttamista. Tämän aikaikkunan aikana yrityksillä olisi ollut aikaa havaita ja estää tuleva teko kokonaan. (Parker ym. 2004, 190-191 & 200.) Vaikka suurin osa insider-rikoksista toteutettiin kuukautta ennen tai kuukausi jälkeen irtisanoutumisen, se ei poissulje sitä, etteikö tiedon varastaminen olisi alkanut jo aiemmin (Cappelli ym. 2012, 75). Kont ym. mukaan (2015, 10) useissa tutkituissa insider-tapauksissa oli ollut havaittavissa varoitusmerkkejä jo ennen tekoa. Havaintoja ei kuitenkaan seurattu ja hallittu järjestelmällisesti, joten insider-rikoksia ei pystytty ennaltaestämään.

Myös Yhdysvaltain Kansallisen insider-työryhmän mukaan insider-rikoksen havaitsemiseksi tulisi olla useampia eri indikaattoreita, koska useista eri lähteistä yhteen koottu tieto voi luoda kokonaiskuvan, jonka perusteella insider paljastuu (NITTF, 2). Mikäli indikaattoritietoja tallennetaan, tulee ottaa huomioon voimassaoleva lainsäädäntö,

jonka mukaan tiedoista muodostuu henkilörekisteri. Henkilöstöön kohdistuva valvonta tulee myös käsitellä yhteistoimintaneuvotteluissa, jossa täytyy kuvata valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät (334/2007, 19 §).

Kuviossa 14 on esitetty kuvitteellinen insider-rikoksen aikajana työsuhteen alkamisesta insiderin paljastumiseen. Aikajanalle on merkitty insiderin työsuhteen aikana tapahtuvia toimia, jotka voivat indikoida insider-uhkasta. Yrityksen ja sen henkilöstön tulisi pystyä Parker ym. (2004) johtopäätöksiin viitaten havaitsemaan insider-indikaattorien hiljaisia signaaleja ja puuttumaan toimintaan jo ennen rikoksen tapahtumista.



Kuvio 14: Esimerkki mahdollisista indikaattoritiedoista ennen insider-rikoksen toteuttamista ja sen paljastumista (mukaillen Gelles 2016, 101)

Suomalaisasiantuntijoiden näkemys teon havaitsemisesta ja sen systemaattisesta toteutuksesta vaihtelivat.

Yksikään haastateltavista ei kieltänyt havaintojen mahdollista merkitystä, mutta ongelmia nähtiin tietosuojalainsäädännön vaatimuksissa sekä jo koulutus-teeman yhteydessä käydystä keskustelusta havainnointitoiminnan jalkauttamisesta työyhteisöön.

Eriävistä mielipiteistä huolimatta monet olivat yhtä mieltä Haastateltava B:n ja Blankenshipin (2016) kanssa siitä, että työyhteisö havaitsee usein muutokset ihmisen käytöksessä, puheissa ja arvoissa. Asiantuntijoiden mielipiteet uhka-indikaattorien luomisesta hajosivat, mutta suuri osa oli sitä mieltä, että yrityksellä tulisi olla huolellisesti ja suunnitelmallisesti toteutettuja indikaattoreita (Haastateltavat B, C, D ja E).

Osan mielestä indikaattorien olemassaolo voi joidenkin muiden insider-riskienhallintakeinojen tapaan vaikuttaa negatiivisesti henkilöstön asenteisiin, minkä nähtiin ylittävän indikaattorien antaman hyödyn.

Muutamat haastateltavat sivusivat eri tavoin insider-riskien hallinnan toteuttamista systemaattisesti, jotta yritys säilyttää kokonaiskuvan riskeistä.

Haastateltava B:n mukaan insider-riskien hallintaa varten luotava erillinen tai olemassa oleviin johtamisjärjestelmärakenteisiin integroitu hallintaohjelma olisi ammattimainen lähestymistapa insider-riskeihin. Ohjelman laajuus ja toteuttamistapa olisivat muun riskien hallinnan tapaan yritys- ja toimintaympäristökohtaista. Haastateltava B kuitenkin huomauttaa, että: ”meillä on totuttu luottamaan ihmisiin ja monet kokevat, että tällaisen (insider-riskienhallintaohjelman) luominen olisi epäluottamuslause henkilöstöä kohtaan ja henkilöstöjärjestöt olisivat takajaloillaan.”

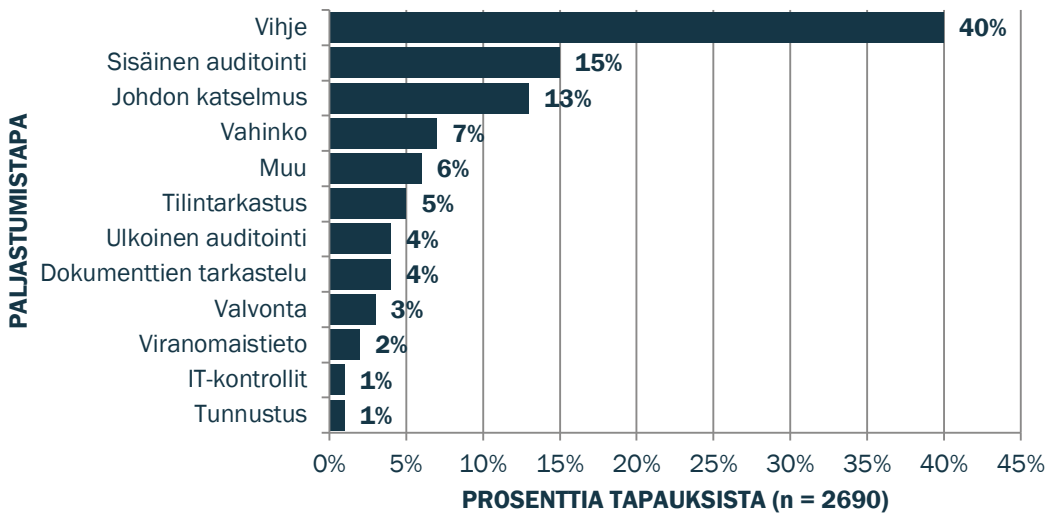
Ohjelmaa tai muunlaista systemaattista lähestymistapaa käsitelleiden haastateltavien mukaan myös tämän teeman yhteydessä korostuu sisäinen viestintä ja sen onnistuminen, koska toiminnan kohteena on oma henkilöstö.

5.3.2 Havaintojen ilmoittaminen

Kuviossa 15 on Yhdysvaltalaisen petostutkintaan erikoistuneen järjestön (ACFE) tilasto vuosina 2016 ja 2017 tapahtuneista petoksista ja niiden paljastumistavoista.

Vaikka petoksen tekijän profiili ja tekotavat eroavat osin insidereista, kuviosta voi huomata, että useissa insider-tutkimuksissakin mainittu vihjeisiin perustuva teon paljastaminen on selvästi (40 %) merkittävin tapa, jolla petosrikokset paljastuivat. 14 % näistä vihjeistä oli anonyymejä. Anonyymin vihjeen antamismahdollisuus mahdollistaa sellaisten henkilöiden vihjeiden antamisen, jotka eivät halua paljastaa henkilöllisyyttään.

Vihjeet vastaanotettiin useimmiten (42 %) varta vasten ilmoittamiskanavaksi perustetun puhelinnumeron kautta. Toiseksi eniten vihjeitä vastaanotettiin sähköpostitse (26 %) ja kolmanneksi eniten sähköisen lomakkeen kautta (23 %). ACFE esittää johtopäätöksenään, että yritykset voivat hyötyä, jos ne mahdollistavat useita eri ilmoittamiskanavia vihjeiden antamiseen. (ACFE 2018, 19.)



Kuvio 15: Petosten paljastumistapa (mukaillen ACFE 2018, 17)

Yrityksen johdon tulisi varmistaa, että yrityksessä on luotu anonyymi ilmoittamiskanava, jonka kautta henkilöstö voi luottamuksellisesti ja anonyymisti kertoa insider-riskejä koskevista havainnoistaan (ISO 27002 2017, 7.2.1). On äärimmäisen tärkeää, että henkilöstö tuntee voivansa tehdä ilmoituksia luottamuksellisesti tai anonyymisti siten, että ilmoittaja ei missään tilanteessa paljastu. Luottamuksen rikkominen saattaa johtaa tilanteeseen, jossa henkilöstö ei enää tee ilmoituksia. (NITTF 2017; Cole & Ring 2005, 317.)

Blankenshipin (2016, 11) tekemissä insider-ilmoituskanavaa koskevissa haastatteluissa ilmeni, että sanalla ”raportointi” oli negatiivinen konnotaatio työntekijöiden keskuudessa, mistä syystä tässä tutkimuksessa on päädytty käyttämään anonyymin raportoinnin sijasta termiä ”anonyymi ilmoittaminen”. Anonyymi ilmoittaminen mahdollistaa työntekijöiden ilmoittaa epäilyttävästä käytöksestä tai sisältä tai ulkopäin yritetystä värväyksestä pelkäämättä jälkiseurauksia (Collins ym. 2016, 63-64).

ACFE:n petoksia koskevan tutkimuksen mukaan 32 % työntekijöistä ilmoittaisi havainnoistaan lähiesimiehelleen, mikäli yrityksessä ei olisi valmista ilmoituskanavaa (2018, 19). Parkerin ym. mukaan insider-havaintojen ilmoittamisväylän tulisi kuitenkin erota linjajohdon ilmoittamisketjusta. Esimiehet saattavat jättää kertomatta epämieluisia tietoja alaisistaan eteenpäin, koska pelkäävät, että heidän luullaan olevan kykenemättömiä johtamaan alaisiaan (Parker ym. 2004, 180).

Työntekijöitä tulisi rohkaista kertomaan havaintoja epäilyttävästä käytöksestä, jonka he ovat yrityksessä havainneet, koska edelliseen lukuun viitaten kollegat ja esimiehet havaitsevat todennäköisimmin epäilyttävät teot tai muutokset työntekijöissä (Parker 2004, 181). Yritys voi palkita kannustinluonteisilla palkkioilla tai lahjoilla ilmoituksista, koska pieni ja rahassa mitattuna mitätön palkitseminenkin voi motivoida henkilöstöä (Collins ym. 2016, 143).

Ennen ilmoituskanavan käyttöönottoa yrityksen tulee kuitenkin neuvotella työntekijöiden edustajien kanssa muun muassa kanavan käyttöönotosta ja kerättävistä tiedoista sekä laatia rekisteriseloste. Ilmoituskanavan luomisen yhteydessä tulee myös kiinnittää huomiota henkilöstölle suunnattuun sisäiseen viestintään kanavan asianmukaisesta käyttötarkoituksesta ja tietojen tarpeellisuusvaatimuksesta. (TSV 2010, 8-10.) Lain mukaan työnantajan tulisi kerätä työntekijää koskevat tiedot ensisijaisesti henkilöltä itseltään, mutta yritys voi poiketa tästä kahdella edellytyksellä: tiedot ovat työsuhteen kannalta välittömästi tarpeellisia ja tietojen hankintaan on selvä peruste, joka liittyy työntekijän luotettavuuden selvittämiseen. (729/2004, 3-4 §; TSV 2010, 6.) Vastaanotettavien henkilötietojen käsittelyssä tulee varmistua, että se on oikeasuhtaista sillä tavoiteltuun oikeutettuun päämäärään nähden (HE 9/2018, 130).

Yrityksen tulee muistaa, että ilmoituskanavien kautta vastaanotettuihin ja talletettuihin viesteihin sovelletaan tulevan tietosuojalain (HE 9/2018) mukaista tarkastusoikeutta, jonka perusteella jokaisella on oikeus saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on talletettu tai, ettei rekisterissä ole häntä koskevia tietoja. Henkilön tarkastusoikeuden piiriin kuuluvat myös tietolähteet, joista henkilötiedot on kerätty. Henkilöllä on siis lähtökohtaisesti oikeus saada tietää ilmoituksen tehnyt henkilö, ellei kanava tue anonyymiä ilmoittamista. (TSV 2010, 9.)

Asiantuntijoiden insider-tekijästä ilmoittamiseen liittyvät haastatteluvastaukset hajosivat kaikista teemoista eniten.

Muun muassa Haastateltava A ei kokenut, että toisiin työntekijöihin kohdistuva ilmoittaminen olisi toimiva tapa hallita insider-riskejä. Haastateltava B korosti, että aihe on herkkä, mutta piti anonyymiä ilmoittamiskanavaa osana insider-riskien hallinnan kokonaisuutta. Haastateltava C ei pitänyt ilmoittamiskanavan luomista vieraana, mutta korosti kanavaan liittyvän viestinnän onnistumista. Hän ei myöskään nähnyt Collins ym. tapaan (2016, 63-64) tarpeellisena erottaa ilmoittamiskanavaa yrityksen whistleblower-kanavasta. Haastateltava E:n mukaan ilmoittamiskanava on osoittautunut hyväksi

ratkaisuksi, mutta totesi osin Parkerista ym. (2004, 180) poiketen, että on tärkeää, että myös esimieskanava on käytettävissä. Haastateltava G tosin mainitsee, että monessa tapauksessa oma esimies ei ole oikea taho kertoa havainnosta, koska esimies voi olla itse ilmoituksen kohteena tai osallisena.

Ilmoittamiskanavan käyttöön varauksella suhtautuneet asiantuntijat pohtivat, että ilmoittamiskanava ei ole suomalaisille luonteva tapa ilmoittaa väärinkäytöksistä.

Kanavan sijasta todettiin, että suomalaiset keskustelevat todennäköisemmin kollegoiden kanssa toisia työntekijöitä koskevista epäilyistä tai muutoksesta käytöksessä. Haastateltava A vertasikin ilmoittamiskanavaa muihin Yhdysvaltalaisiin yleisiin Business Conducting-ohjeisiin sisältyviin käytänteisiin, joista osa on vieraita suomalaiseen organisaatiokulttuurin tuotuna.

Ne asiantuntijat, jotka kokivat ilmoittamiskanavan implementoinnin tärkeänä, korostivat kaikki viestinnän tärkeyttä. Omaan henkilöstöön kohdistuvasta valvonnasta ja ilmoittamiskanavasta puhuminen koettiin yleisesti hankalaksi ja sellaiseksi aiheeksi, mistä ei välttämättä haluta puhua suoraan henkilöstölle.

Haastateltava B esitti ongelman ratkaisemiseksi ilmoittamiskanavaan liittyvän prosessin rakentamista, jossa luodaan selvät lainsäädännön vaatimuksiin perustuvat käytänteet indikaattoreille, ilmoittamiselle ja ilmoitusten käsittelylle, jolloin prosessi kestää mistä näkökulmasta tahansa tapahtuvan tarkastelun.

Haastateltava C:n mukaan yksi viestinnällinen keino on kääntää kanavaa koskeva viesti kollegan käräyttämisestä sellaiseksi, että ilmoittaminen on myös henkilöstön etu: ”…ajatus on, että jokainen ymmärtää, mitä se (insiderista ilmoittaminen) tarkoittaa ja sillä ei ole kaverin pettämisen kanssa mitään tekemistä. Ilmoittamatta jättäminen on koko työyhteisön pettämistä”. Ilmoittamiskanava nähtiin myös yhtenä ennaltaestävänä pelotekeinona vastata työympäristön, tekniikan ja insider-riskejä koskevan toimintaympäristön muutokseen, jonka takia pelko kiinnijäämisestä on pienentynyt.

Asiantuntijat olivat ilmoittamiskanavan hyödystä erimielisiä, mutta mikäli yritys perustaa ilmoittamiskanavan, tulisi siitä luoda läpinäkyvä prosessi, jolla on johdon tuki ja henkilöstön hyväksyntä.

5.3.3 Puuttuminen ja sisäinen tutkinta

Yhdysvaltalaistutkimuksen mukaan kaksi merkittävintä syytä, miksi insider-rikoksen uhriksi joutuneet organisaatiot eivät ole ilmoittaneet teosta viranomaisille ovat ne, että organisaatiot eivät ole pystyneet tarkasti määrittelemään epäiltyä ja organisaatioilla ei ole ollut tarpeeksi todisteita mahdollista oikeusprosessia varten (CSO Magazine, U.S. Secret Service, Software Engineering Institute 2011). Epäillyn määrittäminen ja todisteiden kerääminen yrityksen sisäisesti on yksi keino hallita insider-riskien seurauksia ja pienentää riskien vakavuutta.

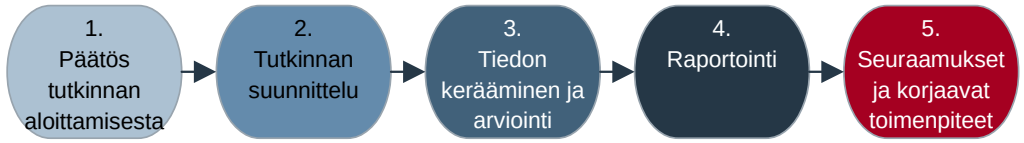
Kun yritys saa tiedon työntekijän huolestuttavasta käytöksestä tai insider-epäilystä, se voi toimia eri tavoin riskien hallitsemiseksi. Esimerkiksi työntekijän pääsyoikeutta yrityksen tiloihin ja liikesalaisuuksiin on hyvä arvioida välittömästi uudelleen ja tarvittaessa rajoittaa. Yrityksellä on tärkeä olla myös työterveyshuollon kanssa sovittu toimintamalli työntekijöiden tukemiseksi. (Collins ym. 2016, 38).

Havaintoilmoituksia varten tulee myös olla luotuna tutkintaprosessi, jonka avulla selvitetään epäilyyn liittyvät tapahtumat ja korjaavat riskienhallintatoimenpiteet. Cole & Ring esittävät kuitenkin myös vaihtoehdon suoraan irtisanoa epäilty henkilö, jolloin ei tarvitse käyttää resursseja tapauksen tutkimiseen (2005, 325). Tutkimatta jättämisen myötä insider-tapaukset voivat kuitenkin jäädä piilorikollisuudeksi ja tapauksista saatavia tietoja ei voida välttämättä käyttää osana yrityksen riskienhallintaa ja turvallisuustoiminnan jatkuvaa parantamista.

Sisäisen tutkintaprosessin pitää olla suunniteltu etukäteen, koska tutkittavat tapaukset ovat arkaluontoisia ja niillä voi olla merkittävä vaikutus yritykseen ja työntekijöihin. Useimpien ihmisten on vaikea myöntää, että luotettu työkaveri, esimies tai alainen on toiminut tahallisesti omaa työnantajaa ja työyhteisöään kohtaan (Contos 2006, 60).

Tutkintaprosessista on hyvä luoda ohje, joka hyväksytetään yrityksen ylimmällä johdolla. Hyvin suoritetun tutkinnan perusteella on mahdollista selvittää riskien juurisyy, jonka perusteella voidaan arvioida nykyisten riskienhallintatoimenpiteiden tehokkuus ja ennalta estää samankaltaiset riskit tulevaisuudessa. (Ratsula 2016, 253-254; ISO 27005 2013, 12.) Collinsin mukaan kaikki insider-rikokseen viittaavat epäilyttävää tai häiritsevää käytöstä koskevat ilmoitukset tulee tutkia ja dokumentoida (2016, 140).

Ennen tutkinnan aloittamista on tärkeä selvittää onko teon kohteena ollut tieto luokiteltu liikesalaisuudeksi, onko sitä suojattu tarvittavin keinoin ja onko epäilty ollut tietoinen tiedon statuksesta, jotta tutkinnan tuloksena voidaan näyttää toteen, että teko kohdistui liikesalaisuuksiin ja tieto nautti liikesalaisuuden suojaa (Vapaavuori 2016, 46).



Kuvio 16: Sisäisen tutkintaprosessin vaiheet (mukaillen Ratsula 2016a, 283)

Kuviossa 16 on annettu esimerkki yrityksen sisäisestä tutkintaprosessista havaittuun insider-rikokseen tai sen epäilyyn liittyen. Malli perustuu Ratsulan (2016a) esittelemään väärinkäytösten tutkintaprosessiin. Laadun varmistamiseksi tutkintaprosessissa tulisi olla ainakin viisi kuviossa esitettyä vaihetta.

1. Tutkinnan aloittaminen liittyy aina esiin tuotuun insider-epäilyyn. Ilmoitus voidaan vastaanottaa henkilökohtaisesti tai anonyymin ilmoituskanavan kautta. Epäilys voi tulla ilmi myös muun muassa sisäisen tai ulkoisen auditoinnin perusteella. Yrityksen on hyvä määritellä yhteyspiste tai henkilö, joka vastaanottaa kaikki ilmoitukset. Tällöin ilmoituksia arvioidaan samoilla kriteereillä, kuin tehdään päätös tutkinnan aloittamisesta. Päätöksentekoon tulisi osallistua useampi henkilö.

Tutkintaa ei välttämättä aloiteta, mikäli päätöksentekijöillä ei ole tarpeeksi tietoa epäilystä. Tämä voi johtua muun muassa vajavaisilla tiedoilla saadusta anonyymistä ilmoituksesta, jonka ilmoittajaan ei saada yhteyttä lisätietojen saamiseksi. Tutkinnan aloittamista ei kuitenkaan tulisi evätä sillä perusteella, ettei epäily vaikuta alkutietojen perusteella merkitykselliseltä tai vakavalta. (Ratsula 2016, 255-256.)

Mikäli tutkinta päätetään jättää aloittamatta, on vastaanotettu ilmoitus kuitenkin hyvä tallentaa. Tutkinnan aloittamatta jättäminen on hyvä perustella ennalta määritellyille tahoille yrityksessä sekä epäilyn ilmoittajalle, jos henkilö on tiedossa. Ilmoittajalle annettava perustelu on tärkeää, jotta yrityksen päätös ei vaikuta ilmoituksen vähättelyltä ja jotta päätöksellä ei olisi vaikutusta matalalla pidettävään ilmoituskynnykseen. (Ratsula 2016, 255-256.)

Tutkinnan aloittamiseen johtavasta päätöksestä on kerrottava tarvittaville tahoille, jotka on määritelty prosessiohjeessa. Tiedon saajia voivat olla muun muassa toimitusjohtaja ja se johtoryhmään kuuluva jäsen, jonka vastuualueelle epäilys kohdistuu. Tutkinnasta tulee tiedottaa ainoastaan niille henkilöille, joille on välttämätöntä tiedottaa asiasta tiedonsaantitarpeen periaatetta noudattaen. Tiedonsaantitarpeen tiukka rajaus suojaa tutkinnan onnistumista sekä ilmoituksen tekijää ja epäiltyä. Päätöksen jälkeen tulee määrätä tutkinnan käytännön toteuttamisesta vastuussa oleva toiminto, joka voi olla tilanteen mukaan esimerkiksi turvallisuusyksikkö tai henkilöstöhallinto. (Ratsula 2016, 255-256.)

Tutkinnan toteuttavan tahon tulee olla asiantunteva sekä riippumaton. Tutkinta tulisi aloittaa mahdollisimman pian, jotta mahdollinen insider-rikos ei pääse jatkumaan. Myös todistusaineiston keruu on vaikeampaa ajan kuluessa, koska dokumentteja saatetaan muuttaa tai tuhota, järjestelmien lokitiedostot häviävät ja ajan kuluessa ihmiset unohtavat haastattelutilanteissa etenkin yksityiskohtia (Ratsula 2016, 255-256; Cole & Ring 312-313).

Päätöksentekovaiheessa tulee erikseen arvioida, tekeekö yritys suoraan rikosilmoituksen ja siirtää epäilyn viranomaisten tutkittavaksi. Lisäksi tulee arvioida onko mahdollisten lisävahinkojen välttämiseksi ja tutkinnan onnistumiseksi päätettävä epäillyn insiderin työsuhde ja vapautettava hänet työvelvoitteesta tai siirrettävä hänet toisiin tehtäviin tutkinnan ajaksi. Myös epäillyn pääsyä omalle työpisteelleen ja yrityksen tietoihin voi olla järkevää rajoittaa. (Ratsula 2016, 255-256; Valtiovarainministeriö 2008, 25.)

2. Tutkinnan suunnitteluvaiheessa tulee määritellä tutkinnan tavoitteet. Suunnitelmassa tulee määritellä lisäksi muun muassa tarkasteltavat dokumentit, haastateltavat henkilöt, tutkinnan aikataulu, raportointi ja lainsäädännölliset rajoitteet. Suunnittelussa tulee myös ottaa huomioon epävarmuustekijät, joita voi olla esimerkiksi tarvittavan dokumentaation puuttuminen tai tutkinnan kannalta tärkeiden haastateltavien poistuminen yrityksestä. (Ratsula 2016, 257-259.)

Myös lainsäädäntö saattaa asettaa rajoituksia tutkinnalle. Muun muassa epäillyn insiderin sähköpostin välitystietojen käsittely osana tutkintaa edellyttää tietoyhteiskuntakaaressa mainittujen vaatimusten täyttymistä sekä ennakkoilmoitusta tietosuojavaltuutetulle (917/2014, 18. luku).

Suunnitteluvaiheessa määritellään, minkä osastojen tai henkilöiden on tärkeä osallistua tutkintaan. Tarvittaessa tulee hankkia erikoisosaamista – esimerkiksi tietojärjestelmiin liittyen – puuttuvan tietotaidon saamiseksi tutkintaryhmään. Suositeltavaa on kytkeä tutkintaan ainakin yksi yrityksen lakimies, jotta tutkinnan oikeudellinen näkökulma tulee huomioitua. Suunnitteluvaiheessa on hyvä arvioida myös tutkinnan mahdollinen vaikutus työyhteisöön sekä sisäiseen ja ulkoiseen viestintään liittyvät kysymykset, jos tapaus tulee julkisuuteen tai siitä halutaan tiedottaa. (Ratsula 2016, 257-259.)

3. Suunnittelun jälkeen aloitetaan konkreettinen tutkintavaihe ja todistusaineiston kerääminen. Johtopäätösten tekemiseksi tulee kerätä puolueetonta aineistoa, jonka lisäksi tulee arvioida aineiston hyödynnettävyys mahdollisessa oikeudenkäynnissä. Yrityksellä on oikeus luovuttaa viranomaiselle muun muassa aiemmin mainitun tietoyhteiskuntakaaren perusteella keräämänsä tiedot epäillyn insiderin sähköpostiliikenteestä (917/2014, 156 §).

Aineistoa voidaan kerätä esimerkiksi ihmisiltä, tietojärjestelmistä tai paperiasiakirjoista. Tiedon kerääminen kannattaa aloittaa taustoittamalla tilanne ja asettamalla tapahtumat aikajärjestykseen. On tärkeää pystyä määrittelemään, mitä on alkutietojen perusteella tapahtunut, milloin on tapahtunut, ketkä ovat osallisia ja jatkuuko epäilty toiminta edelleen.

Haastatteluihin tulee valmistautua perehtymällä tiedossa oleviin faktatietoihin insider-epäilystä. Tutkintaan liittyvät haastattelut on hyvä aloittaa ilmoituksen tehneestä henkilöstä, jos hänen henkilöllisyytensä on tiedossa. Ilmoituksen tehneen henkilön antamien tietojen perusteella haastatellaan muut asianosaiset ja sellaiset henkilöt, jotka voivat auttaa tapahtumien selvittämisessä. Tiedonkeruun turvaamiseksi Ratsula muistuttaa, että sisäistä tutkintaa koskevassa ohjeessa on hyvä olla maininta jokaisen työntekijän velvollisuudesta avustaa tarvittaessa tutkintaa (Ratsula 2016, 260-261; 2016a, 288).

Viimeiseksi haastatellaan epäiltyä insideria. Haastatteluun valmistauduttaessa on tärkeä ottaa huomioon, että epäillyn kanssa käytävää vastakkainasettelua välttävä keskustelu voi saada insiderin paljastamaan toimintansa (Cole & Ring 2005, 298). Tätä tukee myös Charneyn (2010 & 2014) tutkimus, jossa korostetaan tilanteesta ulospääsemisen mahdollistamista insiderille.

Tiedonkeruuvaiheessa on huolehdittava tiedonsaantitarpeen rajauksesta ja sen noudattamisesta, jolloin tutkinnan tiedot eivät tule ulkopuolisten tietoon. Tämä tulee muistaa erityisesti muille osastoille mahdollisesti tehtävien tietopyyntöjen laadinnan yhteydessä, jolloin tulee miettiä, kuinka pyynnöt perustellaan ja kuinka paljon kerrotaan keskeneräisestä tutkinnasta. (Ratsula 2016a, 287).

4. Tutkinnan aikana on tärkeä päivittää raporttia, jonka myötä jokainen tutkinnan vaihe tulee dokumentoitua tarvittavalla tarkkuudella. Raportissa ei esitetä tutkinnan suorittaneiden mielipiteitä, vaan todisteaineistoon perustuvia faktoja tapahtumista. Raportin valmistuttua se tulee jakaa ennalta määritellyille tahoille, joihin tulee lukeutua vähintään ne henkilöt, jotka päättävät mahdollisista seuraamuksista. On myös asiallista tiedottaa alkuperäisen ilmoituksen tehnyttä työntekijää siitä, että esille nostettua epäilyä on käsitelty yrityksessä.

Raportin jakelulaajuutta harkitessa tulee pohtia myös, missä vaiheessa epäillyn esimiehelle ilmoitetaan tutkinnasta. (Ratsula 2016a, 291; Ratsula 2016, 264-265.)

5. Raportin jakelu päättää tutkinnan ja aloittaa korjaavien, mahdollisesti insiderin työsuhdetta koskevien toimenpiteiden toteuttamisen. Tutkintaryhmän ei tulisi osallistua toimenpiteiden päättämiseen eikä edes niiden suunnitteluun, vaan siitä tulisi vastata linjajohto. Ennen toimenpiteiden toteuttamista tulee kuitenkin kuulla uudelleen epäiltyä insideria, jotta hänellä on mahdollisuus kertoa oma näkemys tutkinnan johtopäätöksistä. (Ratsula 2016, 257-259.)

Epäillyn insider-teon tutkinta- ja puuttumisprosessin yhteydessä on hyvä ottaa huomioon, että liikesalaisuustiedon paljastamista ei lähtökohtaisesti pidetä rangaistavana tekona, jos työntekijä ilmoittaa työnantajan lakia rikkovista liikesalaisuutena pitämistä toimista viranomaisille tai julkisuuteen. Liikesalaisuuden paljastaminen saattaa kuitenkin rikkoa työntekijän lojaliteettivelvoitetta tai salassapitosopimusta yritystä kohtaan. (HE 66/1988, 84; Vapaavuori 2016, 76.)

Suomalaisasiantuntijat pitivät yleisesti sisäisen tutkinnan suorittamista ja valmiutta sen suorittamiseen osana insider-riskien hallintaa vahinkojen rajoittamismielessä. Sisäisen tutkinnan merkitys on erityisen suuri, jos teosta ei ole havaintovaiheessa vielä riittävästi todisteita.

Haastateltava G näkee sisäisen tutkinnan suorittamisen tärkeänä yrityksen etujen varmistamiseksi, jos epäillään insider-rikosta: ”Ellei yhtiö tutki itse tapausta, niin syytä epäillä-kynnys ei ylity ja poliisi ei tutki tapausta”. Tähän perustuu myös alkuperäinen ajatus vähän sovelletun Lex Nokia-lainsäädännön voimaansaattamiseksi ja siitä, että yritykset voisivat itse kerätä näyttöä viranomaisille. Lisäksi tutkinnan koettiin mahdollistavan riskien hallintaan sisältyvien korjaavien toimenpiteiden tekemisen: ”Tapaus kannattaa selvittää, jotta tulevaisuudessa voidaan estää ennalta vastaavat tapaukset” (Haasteltava E).

Useissa vastauksissa kävi ilmi, että mitä suuremmista yrityksistä puhutaan, sen todennäköisemmin sillä on kyky tutkia väärinkäytöksiä. Toisaalta useissa tapauksissa voidaan joutua hankkimaan tietoteknistä tukea näytön saamiseksi.

Yrityksen omaan henkilöstöön perustuvan, mutta erityisesti alihankintana toteutettavan sisäisen tutkinnan keinojen laillisuuteen tulee kuitenkin kiinnittää korostuneesti huomiota. Haastateltavat toivat esiin, että vastuu tutkinnan laillisesta toteuttamisesta on yrityksessä, eivätkä esimerkiksi hankitut tietotekniset asiatuntijat välttämättä tunne lainsäädännön rajoitteita. Haastateltava D kertoo tapauksista, joissa yritys on vastentahtoisesti joutunut sopimaan insider-rikoksen epäillyn kanssa, koska sisäisessä tutkinnassa on toimittu laittomasti ja yritys olisi joutunut itse rikoksesta epäillyksi jatkaessaan prosessia.

Sekä Haastateltava C että D kuvailevat onnistunutta tutkintaryhmän kokoonpanoa monialaiseksi. Insider-epäilyjä varten ei tarvitse perustaa omaa tutkintaryhmää, vaan yrityksessä tulisi olla peruskokoonpano erilaisia tutkintoja varten. Kokoonpanolla tulisi olla vähintään johdon tuki sekä oikeudellinen, henkilöstöhallinnon ja turvallisuuden osaaminen.

Ratsulan tapaan myös haastateltavat mainitsevat sisäiseen tutkintaan liittyvän tietoturvallisuuden sekä epäillyn yksityisyyden että tutkinnan onnistumisen näkökulmasta. Haastateltava E korostaa erityisesti ulkopuolisten tutkijoiden käytön yhteydessä toimijoiden luotettavuuden varmistamista ja tietojen suojaamista. Tutkinta ja sen perusteella päätettävät toimenpiteet saattavat vaarantua, mikäli tutkinnan tietoja vuotaa kesken prosessin.

5.3.4 Työsuhteen päättymisvaihe

Yrityksellä on oltava suunniteltu ja henkilöstön tiedossa oleva kurinpitoprosessi, jonka perusteella toimitaan, mikäli työntekijä on syyllistynyt liikesalaisuuksiin kohdistuvaan insider-rikokseen tai muuhun yrityksen vastaiseen toimintaan.

Kurinpitoprosessia ei tule aloittaa, ennen kuin tutkinta on päättynyt ja on varmistettu, että tietoturvarikkomus on todistettavasti tapahtunut. Tahallisissa insider-tapauksissa turvallisuustoimenpiteet tulee kuitenkin aloittaa välittömästi teon paljastuttua vahinkojen rajaamiseksi. (ISO 27001 2013, A.7.2.3.) Mikäli työntekijä on oikeudettomasti hankkinut, ilmaissut tai käyttänyt liikesalaisuustietoa yritys voi ryhtyä epäillyn henkilön työsuhdetta koskeviin toimenpiteisiin.

Mahdollisen työsuhteen irtisanomisen tai purkamisen täytyy perustua esimerkiksi sisäisen tutkinnan perusteella kerättyihin todisteisiin ja niistä tehtyihin johtopäätöksiin. Tarvittaessa tutkintaa voidaan myös jatkaa tarvittavan näytön saamiseksi tai prosessi voidaan päättää tuloksetta.

Tutkintaprosessista johtuvia toimenpiteitä harkittaessa tulee noudattaa yhtenäistä linjaa henkilöstön yhdenvertaisen kohtelun toteutumiseksi. Ainakin seuraavat Ratsulan (2016 267-268) määrittelemät näkökulmat tulisi ottaa huomioon työsuhdetta koskevia toimenpiteitä harkittaessa:

- insider-teon vakavuus
- teon johdosta laiminlyödyt lait ja yrityksen toimintaohjeet
- tekoon liittyvät raskauttavat tai lieventävät seikat
- insiderin työhistoria, kuten aiemmat varoitukset
- irtisanomisen tai työsuhteen purun lailliset edellytykset
- (Työsopimuslaki 55/2001, 7-8. luku)

Työsuhdetta koskevia toimenpiteitä voivat olla suullinen tai kirjallinen varoitus tai työsopimuksen irtisanominen tai sen purkaminen (Työsopimuslaki 55/2001, 7-8. luku).

Mikäli insideria ei irtisanota vaan varoitetaan, tulee yrityksen päättää, miten asiaa seurataan siitä eteenpäin. Joka tapauksessa insider-riskien arviointi tulee toteuttaa uudelleen ja suunnitella, millä toimenpiteillä havaitunkaltaiset teot voidaan vastaisuudessa estää ja havaita ennen niiden tapahtumista. Arvioinnin vuoksi on tärkeää pystyä selvittämään teon mahdollistaneet juurisyyt, jotka liittyvät sekä yrityksen toimintaan että turvallisuuteen. (Ratsula 2016, 267-268.)

Työsopimuslain (55/2001, 7.luku 1 §) irtisanomisperusteita koskevan yleissäännöksen mukaan yritys voi irtisanoa toistaiseksi voimassaolevan työsopimuksen vain "asiallisesta ja painavasta syystä". Asiallisena ja painavana perusteena voi olla muun muassa työsopimuksen tai lain asettamien, työsuhteeseen olennaisesti vaikuttavien velvoitteiden vakava rikkominen tai laiminlyönti.

Työntekijää ei kuitenkaan saa irtisanoa, ennen kuin hänelle on annettu varoitus ja mahdollisuus korjata toimintansa. Yrityksen on myös selvitettävä onko työntekijä mahdollista sijoittaa muihin tehtäviin irtisanomisen sijasta. Mikäli irtisanomisperusteena on vakava työsuhteeseen liittyvä rikkomus, yrityksen ei tarvitse ensin antaa varoitusta tai selvittää muita soveltuvia tehtäviä ennen irtisanomista. (55/2001, 2§.) Yrityksen on kuitenkin irtisanottava työsopimus "kohtuullisen ajan kuluessa" siitä, kun epäilty insiderteko ja irtisanomisen perusteet ovat tulleet yrityksen tietoon (55/2001, 9.luku, 1§).

Yritys voi myös purkaa työsopimuksen päättyväksi heti, mutta vain erittäin painavasta syystä. Erittäin painava syy voi olla työsopimuksen tai lain asettamien, työsuhteeseen olennaisesti vaikuttavien velvoitteiden sen tasoinen vakava rikkominen tai laiminlyönti, että työsopimuksen jatkaminen edes irtisanomisajan loppuun ei tule kyseeseen. Yrityksen on kuitenkin purettava työsopimus 14 päivän kuluessa siitä, kun epäilty insiderteko ja purkamisperusteet ovat tulleet yrityksen tietoon. (55/2001, 8.luku 1 §.)

Ennen työsopimuksen irtisanomista tai purkamista epäillylle insiderille on varattava tilaisuus tulla kuulluksi työsopimuksen päättämisen syistä (55/2001, 9.luku, 2 §).

Työntekijän kuulemisesta huolimatta yrityksellä on direktio-oikeudesta johdettu tulkintaetuoikeus, joten se voi tehdä yksipuolisesti päätöksen työsuhteen päättämisestä. Yrityksen on tämän jälkeen toimitettava työsopimuksen päättämisilmoitus työntekijälle henkilökohtaisesti ja pyynnöstä ilmoitettava kirjallisesti sopimuksen päättymispäivämäärä ja irtisanomisen tai purkamisen syy (55/2001, 9.luku 4-5 §).

Insider-riskien hallinnan näkökulmasta erityistä huomiota tulee keskittää hetkeen, jolloin tehdään päätös työntekijän työsuhteen päättämisestä. Tällöin työntekijän valvontaa tulisi tehostaa ja pääsy- ja käyttöoikeuksia tulisi rajata mahdollisimman paljon tai poistaa kokonaan (Blackwell 2009, 59; Moore ym. 2014, 9).

Yrityksellä tulee olla laadittuna ohjeet ja toimintamalli, joka kattaa kaikki työsuhteen päättymiseen liittyvät toimenpiteet. Työsuhteen päättymiseen liittyvillä riskienhallintatoimenpiteillä on tilastollisesti suuri painoarvo, koska lähes kolmannes Cappellin ym. havaitsemista insidereista jatkoi tiedon varastamista organisaatiosta poissiirtymisen jälkeenkin (2012, 76).

Työsuhteen päättymiseen liittyvän prosessiohjeen tulisi sisältää tiedot siitä, kuka suorittaa eri työsuhteen päättymiseen liittyvät toimet, kuka vahvistaa toimenpiteiden suorittamisen ja milloin eri toimenpiteiden tulee olla tehtynä. Yksittäistä prosessia varten laadittu tarkistuslista tulisi palauttaa yrityksen määrittelemälle osastolle, kuten henkilöstöhallintoon ennen työntekijän lähtöä. (Collins ym.2016, 120-122.)

Prosessissa voidaan ottaa huomioon muun muassa seuraavat toimenpiteet:

- Työntekijän kanssa tulisi pitää lähtökeskustelu, jonka yhteydessä on mahdollisuus tehdä viimeisiä havaintoja mahdollisista indikaattoritiedoista. Keskustelun yhteydessä on myös tärkeä muistuttaa työntekijää häntä sitovista salassapitovelvoitteista ja mahdollisesta kilpailukiellosta suullisesti tai kirjallisesti. Erityisesti tulisi korostaa kieltoa käyttää liikesalaisuustietoja uudessa työssä tai paljastaa niitä uudelle työnantajalle. Myös mahdollisesta sopimussakosta on hyvä mainita. Jos työsuhde on ollut pitkä, salassapito- ja kilpailukieltosopimuksista voi antaa kopion työntekijälle. Työntekijää voidaan pyytää muistuttamaan hänen salassapitovelvoitteestaan uudelle työnantajalle.
- Keskustelun tulisi pitää henkilöstöhallinto tai jokin muu taho, kuin työntekijän lähiesimies.
- Yrityksen tulisi irtisanomisaikana kontrolloida tarkasti liikesalaisuuksia sisältävien tietojen kopiointia tai tiedon siirtoa
- Työntekijän tulee palauttaa yritykselle kuuluva omaisuus, kuten: maksuaikakortit, avaimet, henkilökortit ja yrityksen tiedot ennen työsuhteen päättymistä
- Työntekijän pääsyoikeudet yrityksen tiloihin tulee poistaa
- Työntekijän tunnus murtohälytysjärjestelmiin tulee vaihtaa tai jos järjestelmissä käytetään yhteistä tunnusta, yhteistunnus tulee vaihtaa
- Työntekijöiden mahdolliset yhteiskäyttöiset tietojärjestelmätunnukset tulee vaihtaa
- Työntekijän käyttöoikeudet yrityksen tietojärjestelmiin tulee poistaa (sähköposti, verkkoyhteydet, pilvipalvelut, sovellukset, yrityksen omistamat sosiaalisen median tilit)

- Työntekijän lähtö tulee tiedottaa yrityksen muulle henkilöstölle. Jos yrityksen työntekijät eivät saa poislähtötietoa työntekijästä, he voivat tahattomasti paljastaa entiselle työntekijälle liikesalaisuuksia työsuhteen päättymisen jälkeen tai he ovat helpompia kohteita sosiaaliselle vaikuttamiselle. Lisäksi joissain tilanteissa voi olla hyödyllistä käydä avoin keskustelu muun henkilöstön kanssa insiderin työsuhteen päättymisestä
- Mikäli työntekijän uusi työnantaja on selvillä, yritys voi lähettää työntekijän uudelle työnantajalle kirjatun kirjeen, jossa ilmoitetaan neutraalisti lähtevän työntekijän salassapitovelvoitteista yritystä kohtaan.
- Työsuhteen päättymiseen liittyvät työntekijään kohdistuvat toimenpiteet tulee suorittaa asiallisesti ja työntekijään tulisi ottaa yhteyttä parin viikon kuluttua työsuhteen päättymisestä ja kysyä työntekijän kuulumisia. Tällä yksinkertaisella keinolla on mahdollista vahvistaa entisen työntekijän lojaliteettia yritystä ja sen liikesalaisuuksia kohtaan.

(ISO 27002 2017, 7.3.1 & 8.1.4; NITTF 2016, 9-10; Collins ym. 2016, 25 & 120-121; Ratsula 2016, 268-269; Vapaavuori 2016, 366-367; Cappelli ym. 2012, 75-76.)

Yrityksen tulee myös varautua siihen, että työntekijä irtisanoutuu, hänet irtisanotaan tai työsopimus puretaan riitatilanteessa.

Tällaisessa tapauksessa työsuhteen päättymisprosessin mukaiset pääsy- ja käyttöoikeuksien poistamiseen liittyvät toimenpiteet tulee suorittaa välittömästi. Työntekijä tulee saattaa työpisteelleen, jossa hän voi valvotusti kerätä henkilökohtaisen omaisuutensa ennen hänen saattamista pois yrityksen tiloista. Työntekijän tulee samalla palauttaa yritykselle kuuluva omaisuus, avaimet, henkilökortit ja yrityksen tiedot. (Valtiovarainministeriö 2008, 20.)

Mikäli todisteet tukevat epäilyä, yritys voi päättää käsitteleekö se tapausta riita- vai rikosasiana, koska liikesalaisuuksiin kohdistuvissa insider-teoissa on lähtökohtaisesti kyse asianomistajarikoksesta. Yritys voikin halutessaan tehdä syyttämispyynnön rikoksen tekopaikan syyttäjälle tai poliisille (689/1997, 1.luku 5 § & 4.luku 1§), jolloin syyteoikeuden vanhentumisaika on käytännössä viisi vuotta (39/1889, 8. luku 1 §).

Yrityksellä on tämän ohessa mahdollisuus hakea tuomioistumisesta turvaamistoimen määräämistä liikesalaisuustiedon oikeudettoman hankkimisen, ilmaisemisen tai käyttämisen estämiseksi (Työ- ja elinkeinoministeriö 2018, 64). Yritys voi lisäksi saada edelleen oikeudellista suojaa liikesalaisuudelleen, mikäli yritys pyrkii palauttamaan

paljastetun liikesalaisuustiedon takaisin salaiseksi ja ilmoittaa tiedon saaneita sen salassapidosta. Mikäli tieto on jo tullut laajasti julkiseen tietoon, voi yritys menettää tiedolle saadun liikesalaisuuden suojan edellä mainituista toimenpiteistä huolimatta. (Vapaavuori 2016, 69-70.)

Haastateltavat pitivät tärkeänä, että työsuhteen päättymismenettely on järjestelmällinen ja suunniteltu prosessi, jossa kirjallisuuskatsauksen tulosten mukaisesti varmistetaan, että kaikki toimenpiteet on suoritettu.

Muun muassa Haastateltava E viittaa Suomessa tapahtuneisiin Cappellin ym. (2012) tutkimuksissakin havaittuihin tekoihin, joissa tietoon kohdistuva varkaus on tapahtunut tai selvinnyt työsuhteen päättymisen yhteydessä. Tärkeimpänä yksittäisenä periaatteena pidettiin sitä, että pääsy- ja käyttöoikeudet liikesalaisuustietoihin katkaistaan välittömästi irtisanomistiedon kertomisen yhteydessä, jotta voidaan estää mahdolliset työsuhteen päättymisestä johtuvat tietovarkaudet.

Haastatteluissa tunnistettiin myös erilaisia työsuhteen päättymistilanteita, joihin tulee suhtautua tilanteen mukaisella tavalla. "99% menee ilman dramatiikkaa, mutta voi olla katkeria, jotka haluavat tahallaan viedä tietoja", jolla Haastateltava E viittaa itsenäisesti toimiviin insidereihin. Hän jatkaa, että "...jos lähtee ovet paukkuen, niin se vaati ihan oman prosessinsa. Irtisanomistieto annetaan samaan aikaan kun loppuvat oikeudet eri tietojärjestelmiin ym., tämäkin tulee tehdä prosessin mukaisesti ja hengeltään asiallisesti ilman turhaa dramatiikka ja muistutetaan liikesalaisuuden suojasta ja salassapitovelvoitteista."

Haastateltava D:n mukaan yrityksellä tulisi olla erillinen ohje tilanteisiin, joissa työntekijä lähtee riitaisasti tai hänet irtisanotaan riitaisassa tilanteessa.

Työsuhteen päättymisen jälkeen yrityksen tulee tehdä päätös mahdollisista jatkotoimenpiteistä.

Haastateltava C:n mukaan yrityksen tulisi käyttää kaikki lain sallimat keinot hyödyksi, mikäli on tapahtunut rikos. Myös Haastateltava D korostaa poliisin pakkokeinojen hyötyä joissakin tilanteissa, koska "henkilöllä voi olla kymmenet kopiot kotona, joten poliisi voi käyttää pakkokeinoja mm. takavarikkojen muodossa."

Haastateltava G:n mukaan näytön saaminen on paljon helpompaa, jos tapausta tutkitaan rikoksena, koska tällöin poliisilla on käytössä eri pakkokeinoja, kuten kotietsintä ja takavarikko, joiden avulla on usein saatu ratkaisevaa näyttöä rikoksen teosta. "Eihän tällaista (näytön saaminen) ikinä tapahtuisi, jos nämä eivät olisi rikosjuttuja", millä Haastateltava G viittaa Suomessa olemassa olevaan mahdollisuuteen käsitellä liikesalaisuustapauksia rikoksina.

Toisaalta Haastateltava E:n mukaan yritykset eivät ilmoita kaikkia tapauksia poliisille juuri takavarikoiden ja materiaalin käsittelyn vuoksi. Mikäli takavarikot kohdistuvat työntekijän välineiden lisäksi myös yrityksen muuhun materiaaliin, se voi haitata yrityksen liiketoimintaa. Toinen huolta herättänyt asia on liikesalaisuustietoja sisältävän materiaalin käsittely, jonka asianmukaiseen suojaamiseen poliisin suorittaman tutkinnan eri käsittelyvaiheissa ei välttämättä täysin luoteta. Myös maine- ja imagosyiden todettiin olevan usein syynä sille, että yritykset eivät halua viedä tapauksia viranomaisille.

6 Johtopäätökset

Tässä luvussa esitetään tuloksiin perustuvat johtopäätökset sekä tutkimusprosessiin liittyvä pohdinta.

6.1 Liikesalaisuuksiin kohdistuvien insider-riskien hallinta Suomessa

Tutkimuskysymyksenä oli "miten liikesalaisuuksiin kohdistuvia insider-riskejä voidaan hallita Suomessa?"

Tähän kysymykseen pyrittiin löytämään vastaus purkamalla kysymys käsitteisiin ja jaottelemalla riskien hallintakeinot kolmeen vaiheeseen: työsuhteen alun riskienhallinta keinoihin, työsuhteen aikaisiin ja yleisiin riskien hallintakeinoihin sekä teon paljastamiseen liittyviin ja työsuhteen päättymisvaiheen riskien hallintakeinoihin.

Tutkimustulosten perusteella insider-riskien hallinnan merkittävimpiä haasteita ovat tieto- ja yksityisyydensuojaa koskevan lainsäädännön vaatimusten mukaisten riskien hallintakeinojen toteuttaminen sekä henkilöstön ymmärryksen kasvattaminen riskeistä ilman työhyvinvoinnin laskua ja uusien insider-riskien mahdollistamista.

Riskienhallinnassa tulee ottaa huomioon työelämän ja työntekotapojen muutos, jonka seurauksena perinteisillä riskien hallintakeinoilla ei välttämättä enää pystytä hallitsemaan riskejä. Insider-riskien hallinta edellyttää jatkuvaa toimintaympäristön arviointia ja rohkeutta hyväksyä jäännösriskit.

Tutkimuksen kokoava johtopäätös on, että suomalaiset yritykset voivat hallita liikesalaisuuksiin kohdistuvia insider-riskejä parhaiten systemaattisella lähestymistavalla, joka sisältää riskien hallintatoimenpiteitä työsuhteen kaikissa vaiheissa ja jossa korostuu johdon sitoutuminen, riskien hallintakeinojen toteuttamisen laillisuuden varmistaminen sekä huolellisesti suunniteltu henkilöstölle suunnattu viestintä.

Insider-riskien todennäköisyyden arvioiminen havaittujen tapausten lukumäärän perusteella on vaikeaa ilmiön piiloon jäävän luonteen vuoksi.

Ilmitulleiden rikosepäilyjen perusteella voidaan kuitenkin päätellä, että insider-riskit koskevat kaikkia toimialoja, tekijänä on huomattavasti todennäköisemmin mies kuin nainen ja teon tavoitteena on usein liikesalaisuustiedon hyödyntäminen oman tai toisen kilpailevan yrityksen toiminnassa. Riskien seurausten vakavuus on yrityskohtaista, mutta pahimmassa tapauksessa riski voi päättää liiketoiminnan kokonaan.

Yritysten tulisi harkita omaan riskienhallintaan sopivan insider-riskienhallintaohjelman käyttöönottoa, jonka johdosta riskejä on mahdollista hallita järjestelmällisesti pistemäisen lähestymistavan sijaan.

Rekrytointivaiheessa tulisi käyttää kaikkia lain mahdollistamia keinoja työnhakijan taustan ja soveltuvuuden arvioimiseen. Erilaisista lähteistä kerätyistä tiedoista tulisi yksittäisten arvioiden sijaan muodostaa yksi hallittu kokonaisuus, jonka perusteella arvioidaan hakijaan liittyvää insider-riskiä. Työhakijan taustaan liittyvillä selvityksillä sekä sopimuksilla pienennetään, mutta ei poisteta riskiä.

Riskienhallinta tarvitsee yritysten ylimmän johdon tuen, jotta insider-riskejä voidaan hallita tehokkaasti. Riskienhallinnalle annetun tuen tulee käydä ilmi annetuista ohjeista ja määräyksistä sekä johdon näyttämästä esimerkistä. Preventiivinen riskien hallinta insiderin työssäolovaiheen aikana perustuu mahdollisimman rajattuihin tiedonsaanti- ja käyttöoikeuksiin, minkä lisäksi tieto tai prosessi tulisi pyrkiä jakamaan useiden roolien kesken, jotta yksittäiselle henkilölle muodostuu liiketoimintaa haittaamatta mahdollisimman suppea kokonaistieto suojattavista liikesalaisuuksista.

Riskien hallinta vaatii kuitenkin tasapainoa turvallisuustoimenpiteiden ja henkilöstön hyvinvoinnin välillä, sillä työhyvinvoinnin ongelmat luovat niiden keston ajaksi selvän aikaikkunan sekä kolmannen osapuolen värväystoiminnalle että itsenäisesti toimivalle insiderille aktivoitua.

Tärkeä osa riskien hallintaa on insider-teon tai siihen viittaavan toiminnan mahdollisimman nopea havaitseminen ja havaintotiedon saaminen riskienhallinnan käyttöön. Henkilöstö tulee kouluttaa havaitsemaan insider-uhkia ja ilmoittamaan niistä eteenpäin. Koulutus ja muu insider-riskejä koskeva viestintä tulee suunnitella erittäin huolellisesti, jotta vältetään työhyvinvoinnin negatiivinen kehitys, työtyytymättömyyden kasvu ja uusien insider-uhkien luominen.Havaintoon reagoimiseksi yrityksillä tulisi olla suunniteltu toimintamalli insider-epäilyjen tutkintaa varten. Tutkinta antaa syötettä riskien hallintaprosessiin tulevien insider-tekojen ennaltaehkäisemiseksi ja mahdollistaa jo tapahtuneen teon selvittämisen ilman julkisuutta.

Työsuhteen päättymiseen liittyviä toimenpiteitä varten tulee olla suunniteltu prosessi ja työntekijän poistumiseen liittyvät toimenpiteet tulee suorittaa asiallisesti. Tarvittaessa rikos voidaan siirtää poliisin tutkittavaksi, jolloin todisteiden keräämiseksi voidaan käyttää pakkokeinoja.

Insider-riskien vakavuudesta huolimatta yritysten tulee myös pystyä hyväksymään jäännösriskit.

Sellaisten insider-riskien hallintakeinojen toteuttamista tulisikin välttää, joihin käytetty aika ja vaiva eivät ole oikeassa suhteessa niillä suojattavan liikesalaisuuden arvoon tai liiketoiminnan edellytysten heikentymiseen nähden esimerkiksi työtyytymättömyyden seurauksena.

Esitetyt johtopäätökset ovat samansuuntaisia kuin aihetta käsittelevissä anglosaksisissa tutkimuksissa. Tulokset eroavat ulkomaisista tutkimustuloksista kuitenkin erityisesti lainsäädäntöön liittyvissä kysymyksissä. Useat muissa maissa sallitut riskien hallintakeinot ja henkilöstön valvontaan liittyvät toimenpiteet ovat kokonaan kiellettyjä tai rajoitetummin käytettävissä Suomessa. Suomalainen organisaatiokulttuuri on myös erilainen, joten kaikkia anglosaksisissa maissa käytettyjä turvallisuustoimenpiteitä ei ole mahdollista toteuttaa yhtä suoraviivaisesti Suomessa.

Insider-riskien hallinta on silti perusperiaatteiltaan toteutettavissa samalla tavalla siten, että johdon ja henkilöstön antama tuki ja osallistuminen ovat riskien hallinnan onnistumisessa ratkaisevassa asemassa.

6.2 Diskussio

Opinnäytetyönä laadittu tutkimus toteutui suunnitelmien mukaisesti, vaikka sen näkökulmaa tarkennettiin prosessin edetessä. Alkuperäisenä suunnitelmana oli käsitellä insider-riskien hallintaa kriminologian alalla tunnetun peloteteorian (General Deterrence Theory) mukaisiin teemoihin jaoteltuna. Suunnitelmasta luovuttiin kirjallisuuskatsauksen tulosten perusteella, koska peloteteorian mukainen jaottelu olisi painottunut liian voimakkaasti ennaltaehkäiseviin riskienhallintakeinoihin.

Työn tuloksissa haluttiin saavuttaa laajempi perspektiivi, joten teemoittelu luotiin kirjallisuuskatsauksen tuloksista nyt esitetyn mallin mukaisesti. Vaikeimpia päätöksiä oli erilaisten kirjallisuuslähteistä ja haastatteluista saatujen ajatusten poissulkeminen.

Työn paisumisen vuoksi rajauksesta oli välttämätöntä pitää kiinni, mutta tässä työssä hyödyntämättömiä ajatuksia on kuitenkin mahdollista käyttää osana jatkotutkimusta ja insider-riskienhallinnan jatkokehittämistä työelämässä. Työn merkittävin rajaus liittyy tietojärjestelmiin liittyvien insider-uhkien ja -riskien hallintakeinojen poisjättämiseen. Rajaus oli välttämätön edellä mainittuun paisumiseen viitaten, vaikkakin se esti kokonaiskuvan muodostamisen ilmiöstä.

Opinnäytetyössä analysoidut tulokset vastasivat odotuksia. Haastatteluiden asiantuntijakommentit olivat jopa odotettua monipuolisempia, mikä mahdollisti joidenkin teemojen kriittisenkin käsittelyn. Tämä oli toivottua, koska suunnitteluvaiheessa yhtenä riskinä tunnistettiin haastatteluvastausten homogeenisuus. Riski ei kuitenkaan toteutunut ja haastattelujen koettiin tutkimussuunnitelman mukaisesti syventävän kirjallisuuskatsauksen tuloksia ja tuovan suomalaisen näkökulman käsiteltäviin teemoihin.

Työn tulokset tarjoavat uutta tietoa Suomessa tapahtuvan liikesalaisuuksiin kohdistuvan insider-rikollisuuden erityispiirteistä.

Tulosten hyöty perustuu rikosten laadullisen sisällön tarkasteluun ja siitä tehtyihin suuntaa-antaviin yleistyksiin, jotka tuottivat aiemmin tutkimatonta faktoihin perustuvaa tietoa insidereista ja tekotavoista Suomessa. Viranomaisten tietoon tulleiden rikostapausten vähäisen lukumäärän vuoksi riskien todennäköisyydestä ei kuitenkaan voitu tehdä päätelmiä. Riskien hallinnan tulokset tuottivat tietoa insider-riskien hallintakeinojen parhaiden käytänteiden eri piirteistä ja soveltuvuudesta suomalaisen elinkeinoelämän käyttöön. Parhaat käytänteet on tunnistettu jo aiemmin eri tutkimuksissa, mutta niihin liittyviä yksityiskohtia ja näkökulmia on esitetty paljon.

Erityisesti suomalaisasiantuntijoiden tutkimukseen tuomat argumentit tuottivat viitekehyksessä uutta tietoa aiheesta. Työ on myös ajankohtainen, koska uusi liikesalaisuuslaki on hyväksytty tutkimuksen julkaisuhetkellä ja keskeisinä referensseinä käytetyt riskienhallintaa ja tietoturvallisuutta käsittelevät standardit on tutkimusprosessin aikana päivitetty.

Laurea-ammattikorkeakoulun (2017, 3) mukaan opinnäytetyön tulee kehittää työelämää ja sen tavoitteena voi olla esimerkiksi työkulttuurin kehittäminen.

Tulosten ja johtopäätösten perusteella voidaan väittää, että opinnäytetyö on saavuttanut sille asetetut tavoitteet. Tutkimuksen tuloksia on mahdollista hyödyntää yritysten liikesalaisuuksiin kohdistuvien insider-riskien hallinnassa ja organisaatiokulttuurin kehittämisessä. Insider-uhkaa ja Suomen tilannekuvaa koskevien tulosten hyödynnettävyys korostuu erityisesti yritysten mahdolliseen riskienhallintaan kuuluvassa uhkakartoitusprosessissa, jossa tarvitaan tietoa muun muassa uhkien todennäköisyydestä sekä insiderin motivaatiotekijöistä ja kyvystä. Insider-riskien hallintaa koskevia tuloksia voidaan hyödyntää best practices-tyyppisesti poimimalla parhaita käytänteitä ja yksityiskohtia koskevia ajatuksia osaksi yrityksen riskien hallintaa ja mahdollisen insider-riskienhallintaohjelman muodostamista.

Tutkimustuloksia voidaan lisäksi marginaalisin muutoksin hyödyntää myös julkishallinnon insider-riskien hallinnassa. Useat tutkimuksessa käsitellyt riskien hallintakeinot soveltuvat myös tahattomista insider-uhkista johtuvien riskien hallintaan. Tästä syystä tutkimustulosten osittainenkin soveltaminen on perusteltua, vaikka yritys ei syystä tai toisesta tunnista tahallisia insider-riskejä.

Opinnäytetyön eri vaiheissa syntyi ajatuksia jatkotutkimuksille. Tutkimuksen ulkopuolelle rajattiin riskien hallinta, joka kohdistuu erityisesti tietojärjestelmiä hyväksikäyttäviin insider-tekoihin. Työelämän digitalisoituminen ja riippuvaisuus tietotekniikasta luovat jatkuvasti uusia haavoittuvuuksia, joita voi hyödyntää insider-teossa. Jatkotutkimus voisi kohdistua muun muassa insider-riskien kyberulottuvuuteen ja tietojärjestelmissä toteutettaviin riskien hallintakeinoihin. Toinen ajankohtainen aihe jatkotutkimukselle olisi opinnäytetyön julkaisuhetkellä sovellettavaksi tuleva EU:n yleinen tietosuoja-asetus ja sitä täsmentämään annettava tietosuojalaki.

Tämän tutkimuksen johtopäätöksenä todettiin, että yritysten tulee kiinnittää erityistä huomiota suunniteltujen insider-riskien hallintakeinojen laillisuuden tarkasteluun. Yleinen tietosuoja-asetus määrää henkilötietojen käsittelystä yrityksissä, joten jatkotutkimuksessa olisi mahdollista tarkastella tietosuoja-asetuksen asettamia rajoituksia ja mahdollisuuksia insider-riskien hallinnan toteuttamisessa. Tulosten hyödynnettävyys ei myöskään rajautuisi pelkästään Suomeen, sillä asetus velvoittaa sellaisenaan kaikkia unionin jäsenmaita.

Opinnäytetyöprosessin olennainen osa on tutkimustulosten toistettavuuden ja pätevyyden arvioiminen. Seuraavassa on pohdittu työn reliaabeliutta ja validiutta.

Laadullisten tutkimusten reliabiliteetin arvioinnin yhteydessä viitataan usein saturaatiokäsitteeseen, jolla tarkoitetaan tutkimusaineiston kylläänytymistä. Kylläänytymisen merkkinä pidetään havaintoa, jonka mukaan aineistossa alkavat toistua samat vastaukset. Hirsjärven ym. mukaan saturaation avulla voidaan määrittää aineiston määrä, jolla on

saavutettu teoreettisesti merkittävä tulos. (Hirsjärvi 2010, 182.) Tutkielman kirjallisuuskatsausta koskevan aineiston saturaatio oli havaittavissa ja perusteena työn ja tulosten teemoittelulle.

Reliaabeliutta, eli tutkimustulosten toistettavuutta horjuttaa kuitenkin tutkimuksen tekijän tekemät valinnat ja poissuljennat lukemattomista lähdevaihtoehdoista ja haastateltavista. Toisaalta tutkija voidaan nähdä yhtenä tutkimuksen instrumenteista, jonka kuuluukin vaikuttaa tutkimusvalintoihin ja jonka osallistuminen tutkimuksen tekoon tulisi olla yksi reliabiliteettia vahvistava tekijä tutkimuksen toistettavuuden takaajana. Tutkimusvalintoihin liittyvää heikkoutta pyrittiin vahvistamaan tutkimusstrategian ja analysointiprosessin tarkalla kuvauksella.

Myös tutkimuksen validiteetti voidaan kyseenalaistaa eräiden kirjallisuuskatsauksessa käytettyjen lähteiden vuoksi, koska niiden tieteellistä perustaa ei voitu tutkimuksen teon yhteydessä aukottomasti todentaa. Näihin lähteisiin luetaan teokset, jotka eivät olleet osa tieteellisiä julkaisuja tai viranomaisjulkaisuja, eikä niiden sisällöstä välttämättä käynyt ilmi esitettyjen väitteiden taustalla oleva tutkimusaineisto. Tällaisia lähteitä tarkasteltiin tapauskohtaisesti ja huomiota kiinnitettiin kirjoittajan akateemiseen taustaan sekä luotettavissa lähteissä tehtyihin viittauksiin kyseiseen kirjoittajaan. Edellä mainitun arvion perusteella teoksista poimittuja tutkimuksessa esitettyjä väitteitä voidaan pitää riittävän luotettavina.

Lähteiden valinnan yleisenä suuntaviivana käytettiin julkaisuajankohtaa, millä pyrittiin mahdollisuuksien mukaan käyttämään uusinta tietoa tutkimuksen tekemisessä. Poikkeuksen tekivät julkaisut, joihin oli viitattu säännöllisesti tuoreemmissa julkaisuissa sekä organisaatioturvallisuuden periaatteita koskevat klassikot, joiden edelleen voimassaolevat teoriat on luotu vuosikymmeniä sitten.

Ilmiötä tarkastelevan suomalaisen tutkimustiedon ja julkaisujen puute heikentää kuitenkin työn validiteettia.

Tätä pyrittiin kompensoimaan suomalaisasiantuntijoiden haastatteluilla, jotka kohdistuivat anglosaksisissa tutkimuksissa esitettyihin väitteisiin sekä suomalaisen insiderrikosten tilannekuvan luomisella, joka sitoi aiheen Suomeen. Validiutta on tarkennettu myös käyttämällä tutkimustavoitteen saavuttamiseen menetelmätriangulaatiota.

Haastateltavien valinnassa pyrittiin löytämään aihepiirin tuntevia eri näkökulmasta tutkimuskysymystä tarkastelevia korkeasti koulutettuja asiantuntijoita.

Vaikka haastateltavien valinnassa pyrittiin monipuolisuuteen, haastateltavien yhdistävänä tekijänä ollut aihepiiri oli samalla validiteetin kannalta heikkous. Haastateltaviksi ei aihepiirin tuntemusta korostaneen valinnan vuoksi valikoitunut henkilöitä, jotka olisivat katsoneet tutkimuskysymystä täysin eri näkökulmasta kuin muut haastateltavat. Tämä kuitenkin tiedostettiin ja hyväksyttiin suunnitelmavaiheessa, koska haastattelujen päätarkoituksena oli tuoda asiantuntijanäkökulma tutkimuksen teemoihin, joiden pohdinta suhteessa tutkimuskysymykseen vaatii tietämystä turvallisuusalalta.

Reliaabeliuden ja validiuden pohdinnan lisäksi Hirsjärven ym. mukaan tutkijan vastuulla on tuntea tutkimusetiikan yleisperiaatteet ja ottaa niiden asettamat vaatimukset huomioon tutkimusta tehdessään (2010, 23).

Opinnäytetyö pyrittiin toteuttamaan Tutkimuseettisen neuvottelukunnan määrittelemän hyvän tieteellisen käytännön mukaisesti (Varantola, Launis, Helin, Spoof & Jäppinen 2013, 8). Neuvottelukunnan antaman ohjeistuksen mukaan keskeisiä lähtökohtia ovat tiivistettynä rehellisyyden noudattaminen, eettisesti kestävien tiedonhankintamenetelmien käyttäminen, asianmukaisten lähdeviittausten merkitseminen, tutkimuslupien hakeminen, tutkimusryhmän vastuunjaosta sopiminen ja sidonnaisuuksista ilmoittaminen.

Tutkimuksen tiedonhankintaan käytettiin kirjallisuuslähteitä, poliisiasiain tietojärjestelmää ja asiantuntijoita. Hyvän tieteellisen käytännön mukaisesti insider-rikostilannekuvaa varten haettiin tutkimuslupa poliisiasiain tietojärjestelmän rekisterinpitäjältä Poliisihallituksesta.

Tilannekuvan analysoinnin edetessä rekisterinpitäjältä pyydettiin lisäksi alkuperäiseen tutkimuslupaan liittyvää muutosta tilannekuvan esitysmuotoon. Tilannekuvan kokoamisessa, tiedon käsittelyssä ja julkaistavan tiedon arvioinnissa noudatettiin tutkimuslupahakemuksessa määriteltyjä ja rekisterinpitäjän asettamia vaatimuksia. Merkittävin tutkimuseettinen pohdinta liittyi joihinkin rikosnimikkeisiin liittyvien otosten pieneen kokoon ja niistä tehtäviin yhteenvetoihin. Pienestä otoksesta tehtävät yhteenvedot olisivat saattaneet mahdollistaa joidenkin rikoksesta epäiltyjen, asianomistajien tai muussa asemassa olevien henkilöiden tunnistamisen. Tällaisissa tapauksissa yhteenvetotiedot päätettiin olla julkaisematta ja päätöksestä tehtiin maininta käsiteltävän rikosnimikkeen yhteyteen.

Tutkimuksen yhtenä tietolähteenä toimineille asiantuntijahaastateltaville annettiin ennen haastatteluun suostumista tietoa aiheesta ja heidän annettiin itse päättää tutkimukseen osallistumisesta, jotta varmistettiin tutkimuskohteiden itsemääräämisoikeuden toteutuminen. Haastateltaville lähetettiin ennen haastatteluajankohtaa kirjallisesti tarkemmat tiedot tutkimusongelmasta, haastatteluteemoista, haastattelun tallentamisesta ja tallenteiden käsittelystä. Haastattelun nauhoittamislupaa pyydettiin sekä etukäteen lähetettävässä viestissä että uudelleen haastattelun alkaessa.

Koska opinnäytetyön tutkimuskohteena ja haastattelujen aiheena olivat suojautumiskeinot rikosilmiöltä, jolla on kytkös kaikkein vakavimpiin tiedon luottamuksellisuuteen kohdistuviin uhkiin, päätettiin tasapuolisesti kaikkien haastateltavien henkilöllisyys suojata heidän itsensä ja edustamiensa organisaatioiden suojaamiseksi.

Merkittävin tutkimuksen tekoon liittyvä eettinen pohdinta tapahtui kuitenkin jo aiheen valinnan yhteydessä, koska tutkimus tarkastelee yrityksen omia työntekijöitä uhkana.

Aihe on mielenkiintoinen, mutta se voi herättää kielteisiä tunteita, sillä ihmisen perusluonteeseen kuuluu toisiin ihmisiin ja heidän hyviin tarkoitusperiinsä luottaminen. Vaikka omien työntekijöiden aiheuttamat insider-riskit ovat vakavia ja todellisia, perustuu kaikkien yritysten toiminta aina myös luottamukseen työnantajan ja työntekijöiden välillä. Omien työntekijöiden jahtaamisesta voi tulla taakka, joka heijastuu intohimoisesti insider-riskejä metsästävän ihmisen henkilökohtaiseen elämään.

If you never trust anyone, from a personal standpoint
you will never fully get to enjoy what life has to offer

– Eric Cole & Sandra Ring

Lähteet

Painetut

ACFE 2018. 2018 Global Study On Occupational Fraud And Abuse. Association of Certified Fraud Examiners.

Anttila, P. 2006. Tutkiva toiminta ja ilmaisu, teos, tekeminen. Hamina: Akatiimi.

Blackwell, C. 2009. The Insider Threat. Combatting the Enemy Within. IT Governance Publishing.

Blankenship, J. 2016. Hunting Insider Threats: Forrester`s Model For Establishing An Insider Threat Team. Forrester Research Inc.

Burkett, R. 2013. Rethinking an Old Approach. An Alternative Framework for Agent Recruitment: From MICE to RASCLS. Studies in Intelligence Vol. 57, No. 1.

Cappelli, D. Moore, A., Trzeciak, R. 2012. The CERT Guide to Insider Threats. How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Software Engineering Institute. Carnegie Mellon University.

Charney, D., L. 2010. True Psychology of the Insider Spy. Intelligencer: Journal of U.S. Intelligence Studies.

Charney, D., L. 2014. NOIR: A White Paper.

Crowd Research Partners 2016. Insider Threat – Spotlight Report.

Clarke, R.A., Morell, M.J., Stone, G.R., Sunstein, C.R., Swire, P. 2014. The NSA Report: Liberty and Security in a Changing World. President`s Review Group on Intelligence and Communications Technologies. Princeton US: Princeton University Press.

Cole, E., Ring, S. 2005. Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft. Rockland, US: Syngress.

Collins, M., Theis, M., Trzeciak, R., Strozer, J., Clark, J., Costa, D., Cassidy, T., Albrethsen, M., Moore, A. 2016. Common Sense Guide to Mitigating Insider Threats, Fifth Edition. The CERT Insider Threat Center. Software Engineering Institute, Carnegie Mellon University.

Colwill, C. 2009. Human factors in information security: The insider threat - Who can you trust these days?. Information Security Technical Report 14 (2009) 186-196. Elsevier: UK.

Contos, B. 2006. Enemy at the Water Cooler. Real-Life Stories of Insider Threats and Enterprise Security Management Countermeasures. Rockland, US: Syngress.

Cooper, H. 1989. Integrating Research: A Guide for Literature Reviews (Applied Social Research Methods) 2nd Edition. Sage Publications, Inc.

CPNI 2013. CPNI Insider Data Collection Study. Report of Main Findings. Centre for the Protection of National Infrastructure.

CSO Magazine, U.S. Secret Service, Software Engineering Institute. 2011. Cyber Security Watch Survey 2011. CERT Program at Carnegie Mellon University and Deloitte

Department of Defence. 2011. DoD Directive 5240.06: Counterintelligence awareness and reporting (CIAR). Washington, D.C.: Department of Defence.

Earnest, P. & Karinch, M. 2010. Business Confidential: Lessons for Corporate Success from Inside the CIA. AMACOM: Washington D.C.

Eriksson, P. & Kovalainen, A. 2008. Qualitative Methods in Business Research. Lontoo: Sage Publications.

EU/2016/943. Euroopan parlamentin ja neuvoston direktiivi (2016/943), julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta.

EU 2013. 2013/488/EU. Neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä. Euroopan unionin virallinen lehti. 15.10.2013.

EUR-Lex 2016. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance).

Flinkman, M. & Salanterä S. 2007. Integroitu katsaus – eri metodeilla tehdyn tutkimuksen yhdistäminen katsauksessa. Teoksessa Johansson, K., Axelin, A., Stolt, M. & Ääri, R-L. (toim.) Systemaattinen kirjallisuuskatsaus ja sen tekeminen. Turun yliopisto. Hoitotieteen laitoksen julkaisuja. Turku: Digipaino.

Gelles, M., G. 2016. Insider Threat. Prevention, Detection, Mitigation, and Deterrence. Elsevier: Oxford.

HaVM 5/2017. Valiokunnan mietintö HaVM 5/2017 vp–VNS 5/2016 vp. Hallintovaliokunta Valtioneuvoston selonteko sisäisestä turvallisuudesta.

Helsingin seudun kauppakamari 2016. Yrityksiin kohdistuvat kyberuhat 2016. Helsingin seudun kauppakamari.

Herzberg, F. 1968. One more time: How do you motivate employees? Not by improving work conditions, raising salaries, or shuffling tasks. Harvard Business Review: January-February 1968.

Herbig, K. L. 2008. Changes in espionage by Americans: 1947-2007. Monterey, CA: Defence Personnel Security Research Center.

Hirsjärvi, S., Remes, P & Sajavaara P. 2010. Tutki ja kirjoita. 15.-16. painos. Hämeenlinna: Kariston Kirjapaino.

Hirsjärvi, S., Remes, P & Sajavaara P. 2013. Tutki ja kirjoita. 18. painos. Hämeenlinna: Kariston Kirjapaino.

Hirsjärvi, S. & Hurme, H. 2000. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hollinger, R. 1986. Acts Against the Workplace: Social Bonding and Employee Deviance. Deviant Behavior 7:53-75. Hemisphere Publishing Corporation.

Huhtamäki, H., A. 2014. Kilpailukielto ja salassapito sopimussuhteissa. Helsingin kauppakamari. Meedia Zone OU:Viro.

Humphreys, E. 2008. Information security management standards: Compliance, governance and risk management. Information Security Technical Report. Volume 13, Issue 4, November 2008, Pages 247-255. Elsevier.

IAEA. 2008. Preventive and Protective Measures Against Insider Threats. IAEA Nuclear Security Series No. 8.

Jackson, G.M. 2012. Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security. Hoboken, US: Wiley.

Kananen, J. 2008. Kvali. Kvalitatiivisen tutkimuksen teoria ja käytänteet. Jyväskylän ammattikorkeakoulun julkaisuja-sarja. Jyväskylä: Jyväskylän yliopistopaino.

Kauppi, V. 2017. Maksuhäiriöt keskittyvät samoille kuluttajille. Luottolista 1/2017. Suomen Asiakastieto Oy.

Keskuskauppakamari & Helsingin seudun kauppakamari 2012. Yritysten rikosturvallisuus 2012. Riskit ja niiden hallinta. Keskuskauppakamari.

KKO:2013:17. Yrityssalaisuuden väärinkäyttö, Tahallisuus – Olosuhdetahallisuus.

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., Osula, A-M. 2015. Insider Threat Detection Study. NATO Cooperative Cyber Defence Centre of Excellence.

Kowalski, E., Cappelli, D., Moore, A. 2008. Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector. U.S. Secret Service and CERT/SEI. Carnegie Mellon University, Software Engineering Institute.

Laurea-ammattikorkeakoulu 2017. Laurean opinnäytetyöohje. Hyväksytty 15.8.2017.

Liiten, M. 2017. Yrityksistä karkaa tiedostoja vääriin käsiin. Helsingin Sanomat 5.1.2017.

Lee, J. & Lee, Y. 2002. A holistic model of computer abuse within organizations. Information Management & Computer Security 10/2 [2002] 57-63. University of Colorado at Boulder. Colorado, USA.

McAfee. 2015. Grand Theft Data: Data exfiltration study: Actors, tactics, and detection. Report.

McGuiness, T. 2001. Defence In Depth. Version 1.2E. SANS Institute InfoSec Reading Room.

Metsämuuronen, J. 2006. Laadullisen tutkimuksen käsikirja. Jyväskylä: Gummerus Kirjapaino.

Mehan, J. E. 2016. Insider Threat: A Guide to Understanding, Detecting, and Defending Against the Enemy from Within. IT Governance.

Millett, L.I. 2000. Summary of Discussions at a Planning Meeting on Cyber-Security and the Insider Threat to Classified Information. Washington, US: National Academies Press.

Miner, J.B. 2005. Organizational Behavior 1. Essential Theories of Motivation and Leadership. London: M.E.Sharp.

Moore, A., Cappelli, D., Caron, T. C., Shaw, E., Spooner, D., Trzeciak, R. 2011. A Preliminary Model of Insider Theft of Intellectual Property. Software Engineering Institute. Carnegie Mellon University.

Moore, A., P., Collins, M., L., Mundie, D., A., Ruefle, R.,M. & McIntire, D., M. 2014. Pattern-Based Design of Insider Threat Programs. Software Engineering Institute. Carnegie Mellon University.

Cressey, D. R. 1953. Other People`s Money, A Study in the Social Psychology of Embezzlement: Patterson Smith.

Nato 2017. AAP-06. Edition 2017. Nato Glossary Of Terms And Definitions (English And French). North Atlantic Treaty Organization Nato Standardization Office (Nso) 2017.

NetDiligence 2017. 2017 Cyber Claims Study.

NITTF. 2016. Protect Your Organization from the Inside Out: Government Best Practices. National Insider Threat Task Force.

Nykänen, K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. A 581. Oulun yliopisto, Luonnontieteellinen tiedekunta, Tietojenkäsittelytieteiden laitos.

Parker, T., Shaw, E., Stroz, E., Devost, M.G., Sachs, M.H. 2004. Cyber Adversary Characterization: Auditing the Hacker Mind. Rockland US: Syngress.

Pelastusopisto 2017. Pelastustoimen taskutilasto 2012-2016. Pelastusopiston julkaisu D-sarja: Muut 1/2017.

Poliisihallitus 2017. Epäiltyjen tietojärjestelmän tietosuojaseloste. POL-2016-15046. ID-176297.

Ponemon Institute. 2016. 2016 Cost of Insider Threats Benchmark Study of Organizations in the United States. Ponemon Institute LLC.

Puhakainen, P. & Siponen, M. 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly Vol. 34 No. 4 pp. 757-778/ December 2010.

Punch, M. 1998. Politics and Ethics in Qualitative Research. Handbook of Qualitative Research, Thousand Oaks: Sage Publications.

Ratsula, N. 2016. Compliance - Eettinen ja vastuullinen liiketoiminta. Helsinki: Talentum.

Ratsula, N. 2016a. Yrityksen sisäinen valvonta. Kerava: Edita.

Saario, K. & Vesterinen, P. 2017. Yritysten rikosturvallisuus 2017. Riskit ja niiden hallinta. Keskuskauppakamari.

Saathoff, G.B., Nold, T. & Holstege, C.P. 2013. We Have Met the Enemy and They Are Us: Insider Threat and Its Challenge to National Security. Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies. Edited by: Akhgar, B. & Yates, S. Elsevier: Oxford.

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja. Vaasa: Vaasan yliopisto

Saltzer, J., H. & Schroeder, M., D. 1975. The Protection of Information in Computer Systems. Proceedings of the IEEE 63(9).

Scott, J. & Spaniel, D. 2017. In 2017, The Insider Threat Epidemic Begins. Institute for Critical Infrastructure Technology. CyberSecurity Think Tank.

SFS-EN ISO 27001. 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. 2.painos. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-EN ISO 27002. 2017. Information technology. Security techniques. Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015). Helsinki: Suomen Standardisoimisliitto SFS.

SFS-EN ISO 27005. 2013. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. 2.painos. Helsinki: Suomen Standardisoimisliitto SFS.

Shaw., E.D., Ruby, K.G., Post, J.M. 1998. The Insider Threat to Information Systems. Security Awareness Bulletin, Number 2-98. Monterey: Security Research Center of the Defence Security Service.

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., J., Flynn, L. 2012. Common Sense Guide to Mitigating Insider Threats, 4th Edition. The CERT Insider Threat Center. Software Engineering Institute, Carnegie Mellon University.

Silverman, D. 2005. Doing Qualitative Research: A Practical Handbook. SAGE Publications.

Sisäasiainministeriö 2012. Liiketoimintaa turvallisesti – kansallinen strategia yritystoiminnan turvallisuuden parantamiseksi. Sisäasiainministeriön julkaisusarja 30/2012.

Software Engineering Institute. 2016. Common Sense Guide to Mitigating Insider Threats, Fifth Edition. The Cert Insider Threat Center. CMU/ SEI-2015-TR-010. Carnegie Mellon University.

Stolt, M. & Routasalo P. 2007. Tutkimusartikkelien valinta ja käsittely. Teoksessa Johansson, K., Axelin, A., Stolt, M. & Ääri, R-L. (toim.) Systemaattinen kirjallisuuskatsaus ja sen tekeminen. Turun yliopisto. Hoitotieteen laitoksen julkaisuja. Turku: Digipaino.

Straub, D., Welke, R. 1998. Coping with systems risk: security planning models for management decision making. MIS Quarterly 4/1998. Management Information Systems Research Center, University of Minnesota.

Suojelupoliisi 2017. Suojelupoliisin vuosikertomus 2016. Ratakatu 12, 00120 Helsinki, Suomi.

Suojelupoliisi 2018. Suojelupoliisin vuosikertomus 2017. Ratakatu 12, 00120 Helsinki, Suomi.

Suvorov, V. 1984. Chapter 4. Inside Soviet Military Intelligence. London: MacMillan Publishing Company.

Taylor, S. A., Snow, D. 1997. Cold war spies. Why they spied and how they got caught. Intelligence and National Security, Vol. 12, 2/1997. London: Frank Cass.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. 2005. The insider threat to information systems and the effectiveness of ISO17799. Computer & Security. Volume 24, Issue 6, September 2005. Elsevier.

Tuomi, J & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Vantaa: Hansaprint.

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. Tammi.

TSV 2010. Työelämän tietosuoja ns. whistleblowing ilmiantojärjestelmissä. Tietosuojavaltuutetun toimisto.

Työ- ja elinkeinoministeriö 2018. Liikesalaisuusdirektiivin kansallista täytäntöönpanoa valmistelleen työryhmän mietintö. Työ- ja elinkeinoministeriön julkaisuja 2/2018.

Tilastokeskus. 2014. Naiset ja miehet Suomessa 2014. Helsinki: Edita Publishing Oy.

Valtiovarainministeriö 2008. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Valtionhallinnon tietoturvallisuuden johtoryhmä. VAHTI 2/2008.

Vapaavuori, T. 2016. Yrityssalaisuudet, liikesalaisuudet ja salassapitosopimukset. 2. painos. Alma Talent Oy.

Varantola, K., Launis, V., Helin, M., Spoof, S. & Jäppinen, S. 2013. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Helsinki: Tutkimuseettinen neuvottelukunta.

Verizon 2016. 2016 Data Breach Investigations Report.

Verizon 2017. 2017 Data Breach Investigations Report 10th Edition.

Viega, J. McGraw, G. 2002. Building Secure Software: How to Avoid Security Problems the Right Way. Boston, MA: Addison-Wesley.

Viskari, S. 2009. Tieteellisen kirjoittamisen perusteet. Opas kirjoittamiseen ja seminaarityöskentelyyn. Tampere: Tampereen yliopistopaino

Wajsman, N. & Garcia-Valero, F. 2017. Protecting Innovation Through Trade Secrets and Patents: Determinants for European Union Firms. European Union Intellectual Property Office. European Observatory on Infringements of Intellectual Property Rights.

Weiland, R., M., Moore, A., P., Cappelli, D., M., Trzeciak, R., F. & Spooner, D. 2010. Spotlight On: Insider Threat from Trusted Business partners. Joint CyLab (CMU) and CERT (SEI) Report.

World Trade Organization 1994. Agreement on Trade-Related Aspects of Intellectual Property Rights. Annex 1C.

Sähköiset lähteet

Akava 2017. Salassapitoehdot työsopimuksissa, Akavan selvitys 2017. Viitattu 21.11.2017. https://www.akava.fi/files/22416/Salassapitoehdot_tyosopimuksissa_2017.pdf

Allianz 2018. Allianz Risk Barometer. Top Business Risks For 2018. Viitattu 16.4.2018. http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf

Beaulieu-Hains, D. 2013. ISAF, NATO employ tactics against 'insider threats'. Viitattu 5.8.2017. https://www.army.mil/article/95102/ISAF__NATO_employ_tactics_against__insider_threats_

CDSE. 2017. Need-to-Know. Center for Development of Security Excellence. U.S. Defence Security Service. Viitattu 27.12.2017. https://www.cdse.edu/multimedia/need-to-know/need_to_know.pdf

Council of Europe 2014. Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers. Viitattu 2.2.2018. https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec%282014%297&Language=lanEnglish&Ver= original&Site=CM&BackColorInternet=C3C3C3& BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true

Department of Defence. 2013. Report on Progress Toward Security and Stability in Afghanistan. Viitattu 5.8.2017. https://www.defense.gov/Portals/1/Documents/pubs/Section_1230_Report_July_2013.pdf

DHRA. 2017. Need-to-Know. The Defense Personnel and Security Research Center. Defense Human Resources Activity. U.S. Department of Defence. Viitattu 1.9.2017. http://dhra.mil/perserec/osg/s1class/need.htm

Fischer, L., F. 1998. Espionage by the Numbers: A Statistical Data Base. DSS/Security Research Center. Viitattu 11.8.2017. http://www.iwar.org.uk/ecoespionage/resources/security-guide/Treason/Numbers.htm

Gray, D.D. & Faiez, R. 2012. Afghan violence falls; insider attacks rise. Viitattu 5.8.2017. http://www.washingtontimes.com/news/2012/dec/30/afghan-violence-falls-insider-attacks-rise/

Ikävalko, K. 2018. Maksuhäiriömerkinnät yhä yleisempiä – Asiakastieto: luotonantajat jakamaan luottotietoja kattavammin. Viitattu 30.4.2018. https://yle.fi/uutiset/3-10147628

Matson-Mäkelä, K. 2013. "Totta hemmetissä pelottaa". Viitattu 2.1.2018. https://yle.fi/uutiset/3-6915369

NITTF. National Insider Threat Task Force Mission Fact Sheet. Office of the Director of National Intelligence. Viitattu 5.8.2017. https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf

NITTF. 2017. Any Given Day. Office of the Director of National Intelligence. Viitattu 6.8.2017. https://www.youtube.com/watch?v=nkWc7ZVyN9Q&feature=youtu.be

Poliisi 2018. Yrityssalaisuuksia sisältänyt postipaketti palautui ja johti esitutkintaan. Itä-Uudenmaan poliisilaitoksen tiedote 20.04.2018. Viitattu 20.04.2018. https://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/yrityssalaisuuksia_sisaltanyt_postipaketti_palautui_ja_johti_esitutkintaan_69783

Reuters. 2016. Suspected Islamist who worked for German domestic spy agency arrested. Viitattu 5.8.2017. http://www.reuters.com/article/us-germany-security-idUSKBN13O2LJ

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. Aineisto- ja teorialähtöisyys. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 18.2.2018. http://www.fsd.uta.fi/menetelmaopetus/kvali/L2_3_2_3.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006a. Teemoittelu. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 18.2.2018. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_4.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006b. Kvantifiointi. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 18.2.2018. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_3.html

Saukkonen, P. 2018. Teoreettinen viitekehys. Viitattu 17.2.2018. http://www.mv.helsinki.fi/home/psaukkon/tutkielma/Teoreettinen_viitekehys.html

Schiowitz, E. 2016. Insider Threat Awareness. Viitattu 6.4.2018. https://www.slideshare.net/EricSchiowitz/expert-fso-insider-threat-awareness

SFS 2018. Riskit hallintaan – SFS-ISO 31000. Suomen Standardisoimisliitto SFS. Viitattu 18.4.2018. https://www.sfs.fi/files/8496/31000_riskienhallinta_esite_A4_pitkaselitys.pdf

Suojelupoliisi 2017. Turvallisuusselvitysrekisteri. Viitattu 30.12.2017. http://www.supo.fi/turvallisuusselvitykset/turvallisuusselvitysrekisteri

Tilastokeskus 2015. Palkansaajien kuolemaan johtaneet työpaikkatapaturmat 1975–2014. Viitattu 28.4.2018. http://www.stat.fi/til/ttap/2015/ttap_2015_2017-11-30_tau_001_fi.html

Tilastokeskus 2017. Piilorikollisuus. Viitattu 24.9.2017. http://www.stat.fi/meta/kas/piilorikollisuu.html

Tilastokeskus 2017a. Eräiden rikostyyppien kehitys 2012–2016. Viitattu 28.4.2018. https://www.stat.fi/til/rpk/2016/13/rpk_2016_13_2017-03-23_tau_001_fi.html

Väkevä, L. 1999. Hermeneutiikka tieteellisenä lähestymistapana. Viitattu 18.2.2018. http://www.edu.oulu.fi/muko/lvakeva/lisuri/hermeneu.htm

Lait ja asetukset

Esitutkintalaki 805/2011

HE 9/2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

HE 53/2002. Hallituksen esitys Eduskunnalle eräiden rikoslain talousrikossäännösten ja eräiden niihin liittyvien lakien muuttamiseksi.

HE 66/1988. Hallituksen esitys eduskunnalle rikoslainsäädännön kokonaisuudistuksen ensimmäisen vaiheen käsittäväksi rikoslain ja eräiden muiden lakien muutoksiksi.

HE 105/2016. Hallituksen esitys Eduskunnalle laeiksi työsopimuslain, merityösopimuslain sekä julkisesta työvoima- ja yrityspalvelusta annetun lain muuttamisesta

HE 157/2000. Hallituksen esitys eduskunnalle työsopimuslaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 49/2018. Hallituksen esitys eduskunnalle liikesalaisuuslaiksi ja eräiksi siihen liittyviksi laeiksi.

Henkilötietolaki 523/1999

Julkisuuslaki 621/1999

Laki sopimattomasta menettelystä elinkeinotoiminnassa 1061/1978

Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995

Laki poliisin henkilörekisteristä 509/1995

Laki turvallisuusselvityksistä 177/2002

Laki oikeudenkäynnistä rikosasioissa 689/1997

Laki velan vanhentumisesta 728/2003

Laki yksityisyyden suojasta työelämässä 759/2004

Laki yhteistoiminnasta yrityksissä 334/2007

Liikesalaisuuslaki 2018

Rikoslaki 39/1889

Tietoyhteiskuntakaari 917/2014

Työsopimuslaki 55/2001

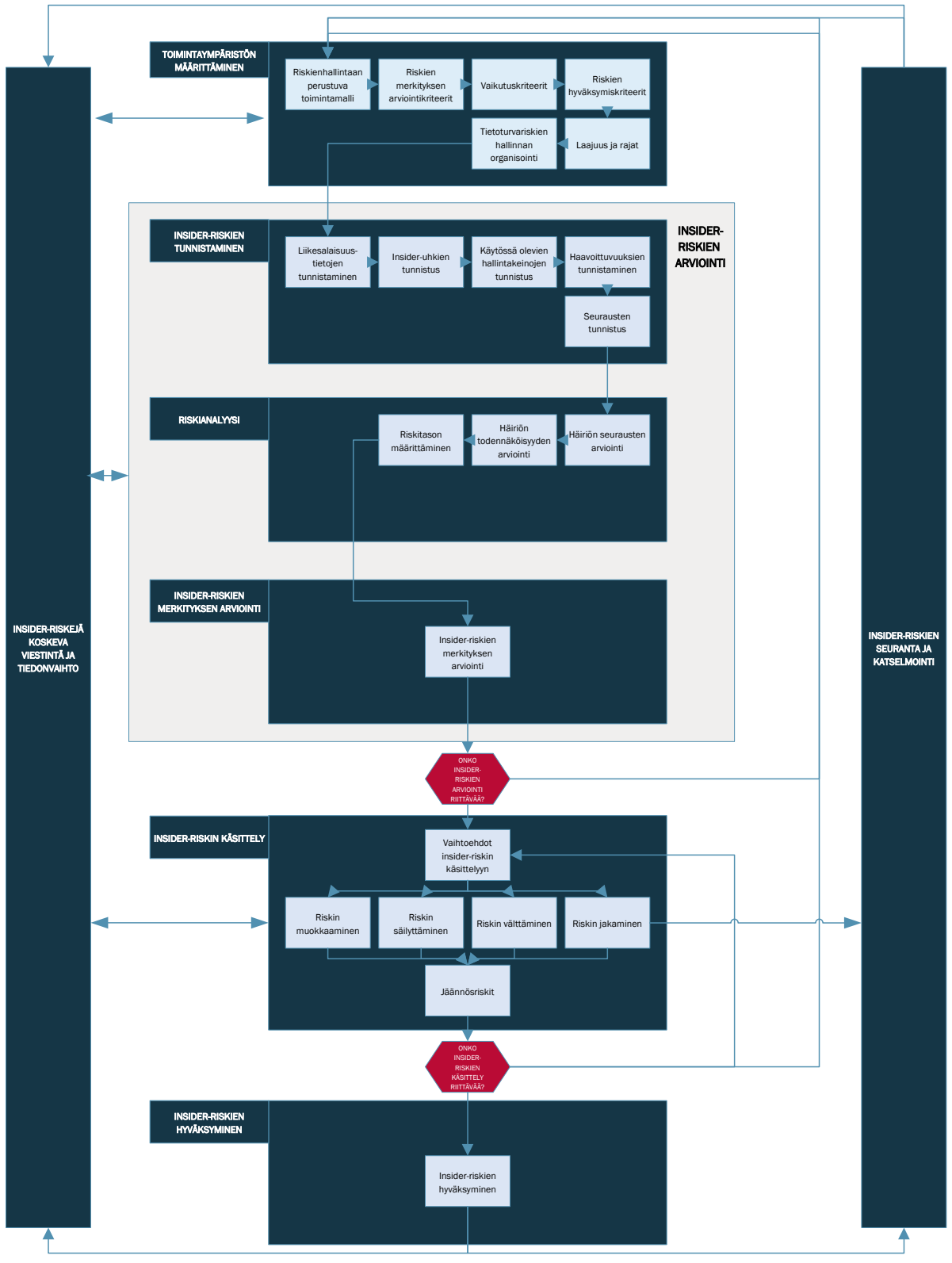
Ydinenergialaki 990/1987

Haastattelut

Haastateltavat A-G keväällä 2018.

Liitteet

Liite 1: Insider-riskienhallintaprosessi (mukaillen ISO 27005 2013, 7.1 - 12.2)


TOIMINTAYMPÄRISTÖN MÄÄRITTÄMINEN
Riskienhallintaan perustuva toimintamalli
Riskien merkityksen arviointikriteerit
Vaikutuskriteerit
Riskien hyväksymiskriteerit
Laajuus ja rajat
Tietoturvariskien hallinnan organisointi
INSIDER-RISKIEN TUNNISTAMINEN
Liikesalaisuus-tietojen tunnistaminen
Insider-uhkien tunnistus
Käytössä olevien hallintakeinojen tunnistus
Haavoittuvuuksien tunnistaminen
Seurausten tunnistus
INSIDER-RISKIEN ARVIOINTI
RISKIANALYYSI
Riskitason määrittäminen
Häiriön todennäköisyyden arviointi
Häiriön seurausten arviointi
INSIDER-RISKIEN MERKITYKSEN ARVIOINTI
Insider-riskien merkityksen arviointi
ONKO INSIDER-RISKIEN ARVIOINTI RIITTÄVÄÄ?
INSIDER-RISKIN KÄSITTELY
Vaihtoehdot insider-riskin käsittelyyn
Riskin muokkaaminen
Riskin säilyttäminen
Riskin välttäminen
Riskin jakaminen
Jäännösriskit
ONKO INSIDER-RISKIEN KÄSITTELY RIITTÄVÄÄ?
INSIDER-RISKIEN HYVÄKSYMINEN
Insider-riskien hyväksyminen
INSIDER-RISKEJÄ KOSKEVA VIESTINTÄ JA TIEDONVAIHTO
INSIDER-RISKIEN SEURANTA JA KATSELMOINTI

SUOJELUPOLIISI
SKYDDSPOLISEN
FINNISH SECURITY INTELLIGENCE SERVICE