RISKIHENKILÖN KÄSITTELY ORGANISAATIOSSA

Riskienhallinnan näkökulma

Turvallisuusjohdon koulutusohjelma – TJK 13

Tutkielma

Pekka Turunen

Puolustusvoimat

Helsinki 21.4.2015

Aalto University Professional Development – Aalto PRO

Kurssi **Turvallisuusjohdon koulutusohjelma 13**	
Tekijä **Pekka Turunen, Puolustusvoimat**	
Tutkielman nimi **Riskihenkilön käsittely organisaatiossa**	
Oppiaine, johon työ liittyy **Turvallisuus**	Säilytyspaikka **Aalto Pro**
Aika **Huhtikuu 2015**	Tekstisivuja 26 Liitesivuja 6
Asiasanat **Riski, riskihenkilö, riskienhallintaprosessi, henkilöstöturvallisuus**	

Tiivistelmä

Tutkielman tavoitteena on tunnistaa riskihenkilön muodostamat riskit organisaatiolle ja määrittää vastatoimet, joiden avulla organisaatio pystyy hallitsemaan riskejä sekä pienentämään kriittisten toimintojen haavoittuvuutta. Tutkimus antaa perusteet riskihenkilökäsitteen käytölle sekä antaa mallin riskihenkilön käsittelylle organisaation riskienhallintaprosessissa.

Riskihenkilö uhkaa organisaation turvallisuutta sisältäpäin käyttäen väärin hänelle myönnettyjä pääsyoikeuksia tai pettää käyttäytymisellään hänelle osoitetun luottamuksen vahingoittaakseen organisaatiotaan.

Riskihenkilön tarkastelu pelkästään standardin mukaisessa riskienhallintaprosessissa tekee riskin käsittelystä kaavamaisen ja teknisen. Ongelma ei ole tekninen, vaan ihmiskeskeinen, joten sitä on käsiteltävä monelta eri osa-alueelta. Riskihenkilön aiheuttamia riskejä ennalta estetään ja torjutaan henkilöstöturvallisuuden keinoin, jossa on pystyttävä hyödyntämään myös käyttäytymistieteen tekniikoita.

Hallitakseen riskihenkilöihin liittyviä riskejä organisaatiolla on oltava hyvä riskihenkilön käsittelysuunnitelma. Suunnitelmassa keskitytään ilmiön ennalta ehkäisyyn, joka alkaa optimitilanteessa jo ennen kuin henkilö on aloittanut työskentelyn organisaatiossa. Riskin tunnistamisvaihe on riskihenkilön ennalta estämisen ja paljastamisen kannalta keskeinen.

Henkilöstöä on koulutettava havaitsemaan poikkeavaa toimintaa. Riskien syntymisen välttäminen tai poistaminen edellyttää henkilöstön tekemien toimenpiteiden valvontaa sekä hyödyntämällä monitasoisia turvajärjestelyjä. Usean henkilön yhtäaikainen läsnäolo kriittisissä toiminnoissa on kannatettavaa läpi koko työuran. Sillä vahvistetaan keskinäistä luottamusta ja kyetään paremmin havainnoimaan poikkeamia.

Ongelman jatkotutkimiseksi voi olla hyödyllistä kerätä organisaatioiden turvallisuus- ja henkilöstöjohdon mielipiteitä riskihenkilön käytännön käsittelystä ja edelleen pyrkiä maastouttamaan heiltä saatuja ajatuksia suomalaiseen organisaatiokontekstiin ja lainsäädäntöön.

Sisältö

1 Johdanto

1.1 Taustaa

"I believe that organizations that have good insider threat and data protection programs will be around in 10 years, and those that don't -- won't."[1]

Patrick Reidy,
CISO, FBI

Perinteisesti tarkasteltuna voiton ulkopuolisesta uhkasta saavuttaa se, jolla on numeerinen ylivoima, parempi välineistö tai ylivoimainen liikehtimiskyky. Mutta mitä tapahtuu, jos todellinen uhka tulee organisaation sisältä. Avoin hyökkäys voidaan torjua voimalla tai vastatoiminnalla, mutta vihamielinen hyökkäys organisaation sisältä voi tehdä pahojaan ennen minkäänlaisia puolustustoimia. Organisaatio ei voi koskaan olla varma siitä, että se on riittävän vahva ja nopea estämään sen, ettei yksi hyvin sijoitettu petturi voisi tuhota kaiken. Organisaatio on yleensä valmistautunut paljastamaan tai valvomaan ulkopuolisen henkilön yritystä päästä organisaation tietoon käsiksi ja on näin onnistunut pienentämään sen omaisuuteen kohdistuvaa anastusuhkaa. Varas, joka on vaikeampi tunnistaa ja joka voi aiheuttaa jopa vakavammat vauriot, on yrityksen sisällä oleva työntekijä valtuutetuilla pääsyoikeuksilla. Tämä sisäinen riskihenkilö voi varastaa pelkästään omaksi hyödykseen tai vakoilla yrityksen tietoja jonkun toisen organisaation tai valtion hyväksi.[2]

Keskustelu riskihenkilöiden muodostamasta sisäisestä uhkasta vilkastui sen jälkeen, kun Wikileaks-tapaus käynnistyi, ja viimeistään Snowden-tapaus

---

[1] http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection

[2] Nick Catrantzos, Managing the Insider Threat – No Dark Corners, CRC Press, New York, s. 3.
FBI, http://www.fbi.gov/

herätti organisaatiot ajattelemaan oman henkilökunnan aiheuttamaa riskiä organisaation merkittävälle tietopääomalle. Keskustelua käytiin erityisesti siitä, kuinka turvallisuusasiantuntijat kykenevät selvittämään potentiaaliset riskihenkilöt ennen kuin heidän organisaationsa joutuvat petoksen, merkittävän tai sensitiivisen tiedon menetyksen kohteeksi.[3]

Viimeisin riskihenkilökontekstiin liittyvä tapahtuma oli, kun Germanwingsin Airbus A320–lentokone (lento 4U9525) putosi Ranskan Alpeilla 24.3.2015. Perämies, 27-vuotias Andreas Lubitz oli yksin ohjaamossa ja ohjasi koneen tarkoituksellisesti vuorenseinämään. Hän käytti hyväkseen kapteenin poistumista ja lukitsi tämän ohjaamon ulkopuolelle. Lubitz oli hiljattain ennen lentoa hakenut netistä tietoa muun muassa itsemurhista ja lentokoneiden turvaovien toiminnasta. Lubitzin käyttämän internetselaimen historiatietoja ei ollut pyyhitty, joten hakutulokset olivat tallessa ennen turmalentoa olevalta ajanjaksolta. Lubitz oli hauissaan keskittynyt hoitomenetelmiin, itsemurhatapoihin, ja ainakin yhtenä päivänä hän oli hakenut tietoja ohjaamojen ovista ja niiden turvavarusteluista.[4]

Organisaatioiden sisältä syntyvä riski on todellinen ja merkittävä. Erään Yhdysvaltojen puolustusministeriön raportin[5] mukaan 87 % tunnistetuista tunkeutujista puolustusministeriön tietojärjestelmiin olivat joko omia työntekijöitä tai muita sisäisessä yhteydessä organisaatioon olevia[6].

1.2 Tutkimuksen tavoite, tutkimuskysymykset ja rajaukset

Tutkielman tavoitteena on tunnistaa riskihenkilön muodostamat riskit organisaatiolle ja määrittää vastatoimet, joiden avulla organisaatio pystyy hallit-

---

3 http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection

4 Helsingin sanomat, 24.3.2015, http://www.hs.fi/ulkomaat/a1305940962506. Saksan syyttäjänviraston lausunto Germanwings lento-onnettomuuteen, 2.4.2015, http://edition.cnn.com/2015/04/02/europe/france-germanwings-plane-crash-main/index.html

5 DoD Office of the Inspector General, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," Report No. PO 97-049, 25.9.1997.

6 DoD Insider Threat Mitigation, Final Report of the Insider Threat Integrated Process Team, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380. Lähteen mukaan riskihenkilön aiheuttamien turvallisuusongelmien peruslähteet ovat: 1) haitallisuus, 2) turvallisuustoiminnan väheksyntä, 3) huolimattomuus, ja 4) piittaamattomuus turvallisuusohjeistukseen, käytäntöihin ja tietojärjestelmien oikeaan käyttöön.

semaan riskejä sekä pienentämään kriittisten toimintojen haavoittuvuutta. Tutkimus antaa perusteet riskihenkilökäsitteen käytölle sekä antaa mallin riskihenkilön käsittelylle organisaation riskienhallintaprosessissa.

Tutkimuksen pääkysymys on: Millaisen riskin riskihenkilö muodostaa organisaatiolle ja miten riskiä voidaan hallita? Pääkysymys ratkaistaan selvittämällä alakysymykset: 1) Kuka on riskihenkilö ja miten hänet voidaan tunnistaa, 2) Kuinka riskihenkilöongelmaa voidaan käsitellä riskienhallintaprosessissa ja 3) Kuinka riskihenkilön muodostamia riskejä voidaan hallita työuran eri vaiheissa. Tutkimuksen ensimmäiseen ja toiseen alakysymykseen vastataan tutkielman toisessa luvussa, jossa aihetta käsitellään riskienhallintaprosessin ja -suunnittelun näkökulmasta. Kolmanteen alakysymykseen vastataan kolmannessa luvussa, jossa näkökulmaksi on valittu henkilön työura ja käytännön turvallisuustoimet aina rekrytointivaiheesta työsuhteen päättämiseen. Tutkielman pääkysymykseen vastataan neljännessä eli yhdistelmäluvussa, johon on myös koottu johtopäätökset.

Organisaation sisäisiä riskejä käsitellään moniulotteisesti henkilön aiheuttaman riskin ja riskienhallinnan näkökulmasta. Kehitettävän riskihenkilökäsittelymallin soveltamisen osalta tehtiin myös tiettyjä rajauksia. Riskihenkilö nähdään organisaation toiminnan kannalta uhkana, joten mahdollisuusnäkökulma on suljettu käsittelyn ulkopuolelle. Henkilöstöön kohdistuvien riskien käsittely ja ulkopuolelta tulevat henkilöriskit rajataan niin ikään tutkielman ulkopuolelle. Sen sijaan tutkimuksen tehtävänä on tarjota systemaattinen tapa riskihenkilöiden käsittelyyn vaikuttavien tekijöiden jäsentämiseksi. Tuloksiin perustuvien johtopäätösten tekeminen ja soveltaminen jäävät mallia käyttävän organisaation vastuulle.

Riskihenkilöä ja siitä muodostuvan ongelman käsittelymahdollisuuksia organisaatiossa kuvataan tutkielmassa yleisellä tasolla eikä kaikkia toimenpiteitä verrata Suomen lainsäädännön suomiin mahdollisuuksiin tai asettamiin rajoituksiin. Lainsäädäntö saattaa tehdä jotkin tutkielmassa esitetyt toimenpiteet vaikeiksi toteuttaa tai jopa mahdottomiksi.

Henkilötietojen keräämisessä ja käsittelyssä on otettava huomioon yksityisyyden suojasta säädetyt lait. Oikeus yksityisyyden suojaan on määritetty Suomen perustuslaissa, jossa todetaan erikseen säädettävät lait. Niitä ovat henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, laki yksityi-

syyden suojasta työelämässä, tietoyhteiskuntakaari. Henkilötietojen käsittelyä koskevia erillisiä vaatimuksia tulee osaltaan myös Euroopan unionin normeista sekä muista kansainvälisistä säännöksistä, normeista ja suosituksista. EU:n direktiiveistä on otettava huomioon henkilötietodirektiivi (46/1995/EY) ja sähköisen viestinnän tietosuojadirektiivi (58/2002/EY).[7]

1.3 Tutkimusmenetelmä ja lähdeaineisto

Tutkielma on tehty laadullisella tutkimusotteella. Tutkimuksen päämenetelmänä on käytetty teorialähtöistä sisällönanalyysia. Sisällönanalyysissä aineisto järjestetään tiiviiseen muotoon kadottamatta sen sisältämää informaatioita. Laadullisen aineiston analysoinnin tarkoituksena on informaatioarvon lisääminen luomalla hajanaisesta aineistosta selkeää ja yhtenäistä informaatioita. Aineiston laadullinen käsittely on tehty induktiivisella logiikalla; yksittäisistä havainnoista on tehty yleistyksiä.[8]

Tutkielmassa tarkastellaan riskihenkilön käsittelyä osana organisaation kokonaisvaltaista riskienhallintaa ja henkilöstöturvallisuustoimintaa. Teorian yhteydessä esitellään erilaisia kehittämis- ja toteutustapoja, joiden soveltuvuutta ei kuitenkaan tämän tutkimuksen puitteissa ole käytännössä kokeiltu, vaan niistä tehdyt johtopäätökset perustuvat pitkälti kirjallisuudessa ja internet-julkaisuissa esitettyihin näkemyksiin.

Riskihenkilöilmiötä käsitellään pääasiassa yhdysvaltalaisiin lähteisiin perustuen. Tutkimuksen tärkeimpinä lähteinä käytetään Nick Catrantzosin tutkimusta vuodelta 2012: Managing the Insider Threat, valtiovarainministeriön VAHTI –ohjetta vuodelta 2008 sekä FBI:n tutkimuksia ja julkaisuja. Suoraan aiheesta tehtyjä tutkimuksia ei Suomessa ole tehty, mutta tutkimuksia on paljon, jotka sivuavat ongelmaa. Niistä tärkeimpänä on hyödynnetty Kristiina Halosen väitöskirjaa vuodelta 2013: Pari askelta jäljessä. Riskienhallintaa käsitellään ISO 31000:2900 standardiin nojautuen.

---

[7] Suomen perustuslaki, 11.6.1999/731, 10§.
https://www.yksityisyydensuoja.fi/lains%C3%A4%C3%A4d%C3%A4nt%C3%B6

[8] Jouni Tuomi, Anneli Sarajärvi: Laadullinen tutkimus ja sisällönanalyysi, Tammi, 2002, s. 110.

1.4 Tutkimukseen liittyvien käsitteiden määrittely

Riski voidaan määritellä olosuhteeksi, jossa tapahtuman lopputulos poikkeaa toivotusta tai odotetusta lopputuloksesta. Riskit ovat kontekstisidonnaisia ja henkilöiden riskiarviot muuttuvat ajan ja paikan suhteen.[9] Yksinkertaistettuna riski voidaan nähdä epävarmuuden vaikutuksena tavoitteisiin, ja vaikutukset voivat olla odotuksiin nähden joko positiivisia tai negatiivisia[10].

Henkilöriski määritellään henkilöstöön kohdistuvaksi tai henkilöstöstä aiheutuvaksi riskiksi organisaation toiminnalle. Henkilöriskit voivat tulla joko organisaation sisältä tai sen ulkopuolelta. Henkilöriskillä voi olla sekä positiivisia että negatiivisia vaikutuksia. Henkilöriskin englanninkielisinä vastineina käytetään mm. personnel risk, people risk ja human resource (HR) risk.[11]

Kuva 1 Tutkittava ilmiö: Riskitaksonomia riskihenkilön näkökulmasta. [12]

[9] Kristiina Halonen: PARI ASKELTA JÄLJESSÄ – tuurilla mennään, Aalto-yliopisto, Tuotantotalouden laitos, väitöskirja, 2013, s 38-39. www.pk-rh.fi

[10] ISO 31000:2009, Risk management – Principles and guidelines, luku 2.1 määrittelee riskin: "Risk is the effect of uncertainty on objectives and an effect is a positive or negative deviation from what is expected."

[11] Kristiina Halonen, väitöskirja, 2013, s 38-39. http://www.pk-rh.fi/index.php?page=henkiloriskit

[12] Teuvo Uusitalo, VTT, luentomateriaali, TJK13, jakso 2, 2013, s. 31.

Tutkielman keskiössä on riskin muodostava henkilö, joka työskentelee tai on työskennellyt organisaation sisällä. Riskihenkilö käsitteenä on vielä vähän käytetty ja vakiintumaton suomalaisessa keskustelussa, tutkimuksissa ja kirjallisuudessa. Yleensä sitä käytetään terveydenhuollon terminologiassa. Tutkielman käsitemallissa riskihenkilö sijoittuu operatiivisiin riskeihin ja siellä henkilöriskien alueeseen, joka on osa organisaation sisäisiä riskejä.

Riskihenkilö uhkaa organisaation turvallisuutta sisältäpäin käyttäen väärin hänelle myönnettyjä pääsyoikeuksia tai pettää käyttäytymisellään hänelle osoitetun luottamuksen. Riskihenkilö käyttää pääsyoikeuttaan tahallisesti tai tahattomasti vahingoittaakseen organisaation intressejä luvattomien paljastusten, tiedon muuntelun, vakoilun, terrorismin tai kineettisin keinoin päättyen organisaation resurssien tai suorituskykyjen menettämiseen tai romahtamiseen. Riskihenkilön englanninkielisenä vastineena käytetään termiä insider threat.[13]

Useasti riskihenkilö yhdistetään tietoturvariskin aiheuttajaksi kyberturvallisuuden osana, jossa keskitytään käsittelemään hakkereita, tyytymättömiä työntekijöitä, entisiä työntekijöitä ja yrityksen toimintaan liittyviä muita henkilöitä, kuten konsultteja. Tietoturvariskien lisäksi tutkimuksessa tarkastellaan riskihenkilöä myös fyysisten ja maineriskien aiheuttajana, jossa otetaan huomioon henkilön taustat, henkilökohtaiset ominaisuudet ja käyttäytyminen.

VTT:n Helena Kortelainen on tiivistänyt riskienhallinnan määritelmän seuraavasti: *Riskienhallinta* on systemaattista ja jatkuvaa toimintaa, jonka avulla pyritään tunnistamaan riskit, arvioimaan niiden merkitystä sekä tarttumaan tarpeen tullen toimeen.[14] Valtionkonttori määrittelee internet-

---

http://www.pk-rh.fi/index.php?page=henkiloriskit

[13] FBI, National Insider Threat Task Force Mission Fact Sheet, http://www.fbi.gov/
http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection.
DoD Insider Threat Mitigation, Final Report of the Insider Threat Integrated Process Team, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380, s 4.
Department of Defense, Instruction 5240.26, May 4, 2012, Incorporating Change 1, Effective October 15, 2013, s. 13.
http://www.dtic.mil/whs/directives/corres/pdf/524026p.pdf

[14] Helena Kortelainen, VTT, luentomateriaali: Cost-Benefit tarkastelut riskitietoisen päätöksenteon pohjana, TJK13, jakso 2, 2013, s. 6.

sivuillaan riskienhallinnan Kortelaisen tavoin lisäten siihen todennäköisyyden arvioinnin merkityksen riskienhallinnassa.[15]

Henkilöriskejä torjutaan ***henkilöstöturvallisuuden*** keinoin, jolla tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa sekä tietoturvallisuuden alaterminä henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä.[16]

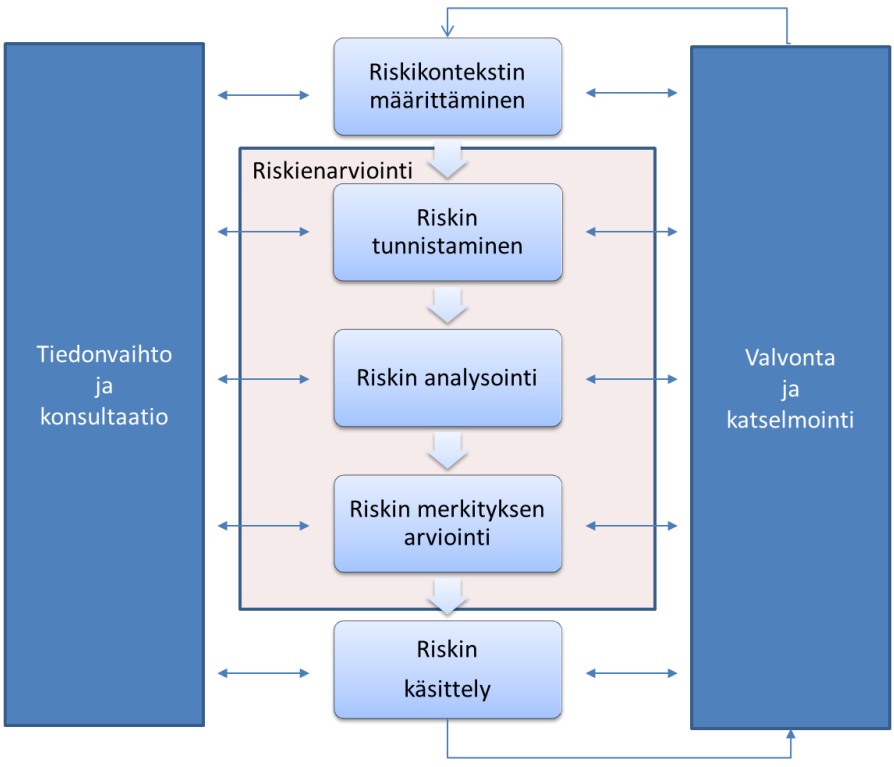
[15] Valtiokonttori, http://www.valtiokonttori.fi/download/noname/%7BEC6E11CB-4462-4390-8C21-E72F96EFAB7F%7D/84882. Organisaation riskienhallintapolitiikka: ”Riskienhallinta on systemaattista ja jatkuvaa toimintaa, jonka avulla pyritään tunnistamaan, arvioimaan ja hallitsemaan toimintaa uhkaavia riskejä, arvioimaan niiden todennäköisyyttä ja merkitystä sekä hallitsemaan niitä tehokkaasti.”

[16] Uusitalo, s. 31.
Valtiovarainministeriö, VAHTI-ohje 2/2008: Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta. ISBN 978-951-804-799-8 (pdf), s 11-12.

2 Riskihenkilön käsittely riskienhallintaprosessissa

2.1 Perusteita

Tässä luvussa riskihenkilön käsittely liitetään alla kuvattuun ISO 31000:2900 standardin mukaiseen riskienhallintaprosessiin. Prosessi kuvataan vaiheittain ja jokaiseen vaiheeseen lisätään riskihenkilön käsittelyn tarvitsemat erityispiirteet.



Kuva 2 Riskienhallintaprosessi.[17]

[17] Uusitalo, s. 40.
VTT: http://www2.vtt.fi/proj/riskianalyysit/riskianalyysit_maaritelmia.jsp

2.2 Riskikontekstin määrittäminen

Riskihenkilön käsittely riskienhallintaprosessissa aloitetaan kontekstin määrittämisestä. Osa-alue kuuluu operatiivisiin henkilöriskeihin ja se liitetään riskihenkilötapauksessa sisäiseen kontekstiin. Tässä yhteydessä sisäisten henkilöriskien merkittävyys arvioidaan organisaation muihin riskeihin verrattuna. Kriteerit määritetään siitä näkökulmasta, onko riski hyväksyttävissä tai hallittavissa. Kriteerit ovat linjassa organisaation arvojen, strategian ja tavoitteiden kanssa.[18]

2.3 Riskin tunnistaminen

Kontekstin määrittämisen jälkeen aloitetaan riskienarviointi, joka alkaa riskien tunnistamisella. Standardin mukaan riskin arviointiprosessissa määritetään riskien olennaisuus, joka voidaan laskea numeerisesti vaikuttavuuden ja todennäköisyyden tulona. Vaikuttavuutta ja todennäköisyyttä arvioidaan asteikolla 1-5. Vaikuttavuuden arviointikriteereinä ovat riskin realisoitumisen vaikutukset talouteen, terveyteen, maineeseen tai oikeudelliseen asemaan. Vaikuttavuuden arvioinnissa käytetään sitä arviointikriteeriä, jossa riskin vaikutukset ovat suurimmat.[19]

Riskihenkilön muodostaman riskin tunnistamisessa on pyrittävä hyödyntämään jatkuvaa oireanalyysia. Ihmiset ovat moniulotteisia, joten ongelmaa on käsiteltävä monelta eri osa-alueelta. Näin ollen ongelma ei ole tekninen, vaan ihmiskeskeinen.[20] Riskihenkilön tunnistamisen menetelmissä on kaksi erilaista osa-aluetta, jotka käsitellään erillisinä. Ensimmäiseksi on päätettävä kenestä on oltava huolissaan; toisinsanoin kenellä on kyky toteuttaa sellai-

---

[18] http://www.praxiom.com/iso-31000-terms.htm#2.22_Risk_criteria

[19] Valtiokonttori, organisaation riskienhallintapolitiikka, s. 4. http://www.valtiokonttori.fi/download/noname/%7BEC6E11CB-4462-4390-8C21-E72F96EFAB7F%7D/84882
Laskentaa tehtäessä on otettava huomioon, että pienen vaikutuksen ja suuren todennäköisyyden tulo johtaa samaan tulokseen kuin suuren vaikutuksen ja pienen todennäköisyyden tulo, vaikka riskit eivät olisi toisiinsa verrattavia. Tämä edellyttää lopuksi saatujen laskelmien herkkyysanalyysia, jossa verrataan saatujen tulojen merkittävyyttä organisaation toiminnalle.

[20] http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection

nen isku organisaatiotaan vastaan. Toiseksi on määritettävä kuka on todennäköinen henkilö, joka tekee iskun.[21]

Potentiaalisen riskikäyttäytymisen tunnistaminen edellyttää turvallisuusorganisaation tiedonhankintaa monista eri lähteistä. Yksi indikaattori voi kertoa liian vähän, mutta kun se yhdistetään muiden indikaattoreiden antamiin tietoihin, niin häiriöt käyttäytymismalleissa voivat nousta esiin ja ne voivat yhdistyä henkilöön, joka voi muodostaa riskin organisaation kriittiselle toiminnalle. Oleellista on arvioida monista eri lähteistä saatua relevanttia tietoa, jos työntekijän käyttäytyminen edellyttää lähempää tarkastelua tai asia pitää ottaa virallisempaan tutkintaan. Saattaa olla mahdollista, että henkilö ei toimi vahingoittamistarkoituksessa, mutta on avun tarpeessa. Molemmissa tapauksissa henkilö voi muodostaa riskin organisaation turvallisuudelle ja tilanne vaatii jatkotutkimuksia.[22]

Riskin tunnistamisen ensimmäisenä vaiheena on riskilähteiden tunnistaminen, joka sisältää mahdollisten riskihenkilöiden identifioinnin.[23] Tässä yhteydessä kartoitetaan riskihenkilön henkilökohtaiset ominaisuudet ja käyttäytymiseen liittyvät indikaattorit, jossa voi hyödyntää liitteessä 1 esitettyjä taulukoita. Riskienhallintaprosessissa tapauksille annetaan riskikriteeriluku[24]. Tunnistamalla riskit ja kuvaamalla niiden merkittävyys, syyt ja seuraukset yhtenäisellä ja vertailtavalla tavalla mahdollistetaan tehokkaat riskienhallintatoimenpiteet. Indikaattoreita voidaan käyttää organisaation painotuksia noudattaen ja riskikriteeriluvun voi jokainen organisaatio laatia itse.

Riskihenkilömäärittely tehdään ensisijaisesti tapauksissa, joissa harkitaan yksittäisen henkilön rekisteröintiä. Se voidaan tehdä myös taannehtivasti esimerkiksi turvallisuusselvitysmenettelyyn tai taustaselvityksiin liittyvissä tapauksissa, joissa arvioidaan organisaation henkilöstötietoihin vuosien mittaan tallennettujen tietojen oikeellisuutta ja merkityksellisyyttä.

---

[21] Matt Bishop, Sophie Engle, Deborah A. Frincke, Carrie Gates, Frank L. Greitzer, Sean Peisert, and Sean Whalen: A Risk Management Approach to the “Insider Threat”,s, 3-4. http://web.cs.ucdavis.edu/~peisert/research/insiderthreat-chapter-final-prepress.pdf.

[22] FBI, National Insider Threat Task Force Mission Fact Sheet, http://www.fbi.gov/

[23] Uusitalo, s. 42.
http://www.pk-rh.fi/index.php?page=henkiloriskit

[24] Uusitalo, s. 41.

Liitteen 1 indikaattoritaulukkoa voidaan hyödyntää esimerkiksi seuraavalla tavalla: Riskin tunnistaminen edellyttää vähintään neljän kohdan täyttymistä, kun henkilöä arvioidaan pelkästään henkilökohtaisia ominaisuuksia käyttäen tai pelkästään käyttäytymiseen liittyviä indikaattoreita käyttäen. Kun arviointi tehdään sekä henkilökohtaisia ominaisuuksia että käyttäytymiseen liittyviä indikaattoreita käyttäen, riskin tunnistaminen edellyttää kummastakin ryhmästä vähintään kolmen kohdan täyttymistä.

Seuraavasta esimerkkitapauksesta on löydettävissä henkilökohtaisiin ominaisuuksiin ja käyttäytymiseen liittyviä indikaattoreita. Indikaattoreiden ilmeneminen ja yhtäaikainen vaikutus pitäisi herättää turvallisuusorganisaation arvioimaan, että onko kyseessä riskihenkilötapaus ja aloittaa riskin pienentämistoimenpiteet.

> ***Henkilökohtaiset ominaisuudet****: Tiedetään, että henkilö on eronnut aviopuolisostaan edellisenä vuonna ja hänen päihteiden käyttö on lisääntynyt, jolla on ollut vaikutuksia työsuorituksiin. Tapahtumien myötä henkilölle on syntynyt rahahuolia ja velkaantumista työkavereille. Hän on yrittänyt paikata tilannetta lisääntyneellä uhkapelaamisella.*
>
> ***Käyttäytyminen****: Työntekijän suoritukset ovat romahtaneet, hänelle sattuu usein huolimattomuusvirheitä ja hän usein myös ylittää asetetut aikamäärät. Hänen on havaittu kopioivan tarpeettomasti materiaalia eikä noudata tietoturvaohjeistuksia. Sairauslomat ovat lisääntyneet, joiden aikana hän käyttää yhtiön tietojärjestelmiä etäyhteydellä.*

Rekisteröinnin yhteydessä on aina kirjoitettava auki, miten indikaattorien nähdään ilmenneen kyseisessä tapauksessa. Indikaattoreita on käytettävä aina tapauskohtaisesti huolellista kokonaisharkintaa noudattaen. Tähän sisältyy erityisesti lähteiden luotettavuuden arviointi.

2.4 Riskin analysointi

Tunnistamisvaiheen jälkeen siirrytään riskin analysointiin. Siinä punnitaan riskin aiheuttajaa ja syytä, niiden seurauksia sekä seurausten todennäköisyyttä. Riskihenkilön käsittelyn näkökulmasta arviointiin otetaan tässä vaiheessa myös organisaation tapahtumat, mihin mahdolliset toteutuvat riskit voivat organisaatiossa vaikuttaa. On myös arvioitava, mitkä tekijät voivat

edesauttaa riskin toteutumista ja mitkä ovat toteutumisen potentiaaliset seuraukset.[25]

Riskimahdollisuuksien löytämiseksi on keskeistä ymmärtää yrityksen vahvuudet ja tunnistaa organisaation kruununjalokivet. Analysointi voidaan aloittaa listaamalla pahimmat skenaariot, niin voimavarojen kuin henkilöidenkin näkökulmasta, jotka voivat tehdä tuhoa yritykselle. Tässä yhteydessä voidaan kysyä, mitkä ovat tärkeimmät järjestelmät, jotka sisältävät sensitiivisemmät tiedot. Niissä järjestelmissä on seurattava käyttäjätietoja, logeja ja dokumenttien liikkeitä. FBI:n tutkimusten mukaan kriittisimmissä järjestelmissä 80 % tiedon siirrosta tekevät vain alle 2 % työvoimasta.[26] Analysointivaiheessa on kyettävä identifioimaan organisaation vastustajat (kilpailijat), oma henkilöstö ja suojattavat tiedot. Silloin on kysyttävä: Kuka on kiinnostunut organisaatiostasi ja kenet he voisivat yrityksestäsi maalittaa hyödyntääkseen häntä omien tavoitteidensa saavuttamiseksi?[27]

Alla olevaan taulukkoon on koottu organisatoriset faktorit, jotka tukevat arviointia.

Taulukko 1 Organisatoriset faktorit[28]

Organisatoriset faktorit		
Faktorit	Kuvaus	Riskiluku
Henkilöstöllä on liian laajat oikeudet.	Yksityisen, luokitellun tai muun suojatun materiaalin hankinta on helppoa ja se on saatavilla. Pääsyoikeudet annetaan henkilöille,	

[25] ISO 31000:2900 standardi.
Uusitalo, s. 42.

[26] http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection

[27] http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection. FBI tarkastelee kyperin, kontekstiin liittyvän (esim taloudellinen tilanne, matkustelu, raportointi) ja psykologisen tiedon keräämisen kombinaatiota. Yritysten turvallisuushenkilöstön on työskenneltävä lakiasiantuntijoiden kanssa määrittääkseen tiedot, jotka voidaan laillisesti kerätä.

[28] Catrantzos, s. 18.
FBI, The Insider Threat: An introduction to detecting and deterring an insider spy. http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure

Organisatoriset faktorit		
Faktorit	Kuvaus	Riskiluku
	jotka eivät niitä tarvitse.	
Suojaustasomerkintöjä ei hallita.	Yksityinen tai luokiteltu tieto ei ole merkitty/leimattu tarkoituksenmukaisesti tai se on tehty väärin.	
Materiaalin ja tiedon kuljettamista ei kontrolloida.	Yksityisen, luokitellun tiedon ja muun suojatun materiaalin ulosviennin organisaation tiloista tai tietojärjestelmistä on helppoa.	
Etätyöskentely on huolimatonta.	Henkilöstölle ei ole annettu selkeitä ohjeita etätyöskentelyyn sensitiivisten tai yksityisluonteisten aineiston käsittelyyn.	
Turvallisuuskulttuuri on leväperäistä.	Käsitys siitä, että turvallisuus on väljä ja varkauden seuraukset ovat minimaaliset tai niitä ei ole ollenkaan.	
Aikapaine aiheuttaa virheitä turvallisuustoiminnassa.	Työntekijät voivat liiallisessa kiireessä suojata vaillinaisesti yksityiset tai suojatuksi tarkoitetut materiaalit, tai eivät harkitse loppuun toimintansa seurauksia.	
Salassa pidettävän tiedon suojaamista ei hallita.	Työntekijöitä ei ole koulutettu kuinka salassa pidettävä tieto suojataan kunnolla.	

2.5 Riskin merkityksen arviointi

Riskienarviointivaihe päätetään merkityksen arviointiin niiden riskien osalta, jotka löydettiin riskien analysointivaiheessa. Merkityksen arvioinnissa otetaan huomioon myös kontekstisarvioinnin yhteydessä annetut riskikriteerit. [29]

[29] ISO 31000:2900 standardi.
Uusitalo, s. 42.

Tässä vaiheessa tehdään päätökset riskien siedettävyydestä riskianalyysin perusteella ottamalla huomioon sellaiset tekijät, kuten sosio-ekonomiset ja ympäristölliset näkökohdat.[30] Organisaatio voi luoda riskien merkitysten arviointiasteikon omista lähtökohdistaan, joka helpottaa vertailua. Asteikko sisältää numeeriset arvot ja jokaisen tason määritelmän esimerkiksi seuraavasti häiriökäyttäytymisen osalta:

- Riskitaso 0 – Kiusanhenki: Henkilö käyttää työnantajan suomia työkaluja ja työaikaa silloin tällöin omiin henkilökohtaisiin tarkoituksiin.
- Riskitaso 1 – Kasvava kiusa: Henkilö käyttää järjestelmällisesti työnantajan suomia työkaluja ja työaikaa silloin tällöin omiin henkilökohtaisiin tarkoituksiin ja häiritsee samalla muiden työrauhaa.
- Riskitaso 2 – Krooninen häiriö: Henkilö käyttää järjestelmällisesti kollegoiden työkaluja omiin henkilökohtaisiin hämäräperäisiin tarkoituksiinsa ja aiheuttaa harmia koko työyhteisölle ja turvallisuudelle. Näin hän suojelee itseään organisaation valvonnalta sekä samalla asettaa toiset varaan ja epäilyksen alaiseksi.
- Riskitaso 3 – Ei hyväksyttävä, hallitsematon häiriö: Henkilöllä on niin työasiat kuin henkilökohtaisetkin asiat hallitsemattomassa tilassa. Henkilö ei noudata ohjeita tai lakeja seurauksista piittaamatta.

2.6 Riskinkäsittely

Riskienarvioinnista siirrytään riskinkäsittelyyn, jossa valittuja riskejä voi säätää. Riskille valitaan yksi tai useampi käsittelyvaihtoehto, joita ovat: Vältetään riskin syntyminen, minimoidaan, siirretään tai poistetaan riskin aiheuttaja. Käsittelyprosessissa riskin todennäköisyyttä voidaan vielä muuttaa ja riskistä aiheutuvia seurauksia voidaan vaihtaa. Riski voidaan jakaa toisen osapuolen kanssa (esim. vakuuttaminen) tai säilyttää ennallaan tai jopa korottaa uusien mahdollisuuksien löytämiseksi. [31]

Riskihenkilön käsittelyn näkökulmasta riskin syntymisen välttäminen toteutuu tausta- ja turvallisuusselvitysten avulla erityisesti väärien rekrytointien

[30] VTT, http://www2.vtt.fi/proj/riskianalyysit/riskianalyysit_maaritelmia.jsp

[31] ISO 31000:2900 standardi.
Uusitalo, s. 48.
http://www.pk-rh.fi/index.php?page=henkiloriskit
http://www.praxiom.com/iso-31000-terms.htm#2.25_risk_treatment

välttämisenä ja työsuhteen aikana oikealla turvallisuusvalvonnalla. Riskin siirtäminen ja aiheuttajan minimointi riskihenkilötapauksissa voidaan toteuttaa mm. työtehtävien muuttamisena tai rajoittamisena siten, että henkilö ei pääse kiinni organisaatiolle kriittiseen tietoon ja näin aiheuta riskiä sen toiminnalle. Kontrollitoimina voidaan käyttää myös pääsyoikeuksien rajoittamista. Riskin poistaminen voi käytännössä tarkoittaa jopa riskihenkilön työsuhteen irtisanomista. Siinä tapauksessa se merkitsee jo riskihenkilölle asetetun riskin toteutumista, jotta työsopimuslain mukaiset irtisanomisperusteet täyttyvät[32]. Riskihenkilötapauksessa riskin korottaminen ei tule kyseeseen, koska riskillä on vain negatiiviset seuraukset.

2.7 Tiedonvaihto ja konsultointi

Aktiivisella ja oikea-aikaisella viestinnällä on keskeinen rooli riskienhallinnassa. Tiedonvaihto ja konsultointi toteutetaan erityisesti organisaation henkilöstöhallinnon, turvallisuuden ja johdon välillä kaikissa riskihenkilöön liittyvässä riskienhallintaprosessin vaiheissa. Tietoa on vaihdettava itse riskistä, sen syistä ja seurauksista sekä tehdyistä toimenpiteistä. Tiedonvaihdolla varmistutaan, että johto ymmärtää päätösten perusteet ja syyt, miksi tiettyjä toimenpiteitä täytyy tehdä. [33]

Riskienhallinta perustuu eri riskien yhtenäiseen tunnistamiseen, arviointiin ja raportointiin. Onnistunut riskihenkilönkäsittelyohjelma edellyttää työyhteisössä läpinäkyvyyttä. Johto on keskeisessä roolissa organisaation salaisuuksien menettämisen estäjänä. Johto edesauttaa oikean toimintakulttuurin luomisessa, jossa työntekijöiden epärehellisyys tai organisaation horjuttaminen sisältä päin ei ole missään tapauksessa hyväksyttävää.[34]

---

[32] Työsopimuslaki 26.1.2001/55, 7 luku, 1. ja 2.§. Työnantaja saa irtisanoa toistaiseksi voimassa olevan työsopimuksen vain asiallisesta ja painavasta syystä. Työntekijästä johtuvana tai hänen henkilöönsä liittyvänä asiallisena ja painavana irtisanomisperusteena voidaan pitää työsopimuksesta tai laista johtuvien, työsuhteeseen olennaisesti vaikuttavien velvoitteiden vakavaa rikkomista tai laiminlyöntiä. https://www.finlex.fi/fi/laki/ajantasa/2001/20010055#L7

[33] ISO 31000:2900 standardi.
Uusitalo, s. 49.
http://www.pk-rh.fi/index.php?page=henkiloriskit

[34] Catrantzos, Managing the Insider Threat , s. 47.

2.8 Valvonta- ja katselmointi

Riskienhallinnan valvonta- ja katselmointiprosessilla varmistetaan, että toiminta on tehokasta. Sillä kerätään tietoa myös tulevaisuuden riskienarviointia varten ja opitaan, trendi-muutoksista, onnistumisista ja epäonnistumisista. Valvontamekanismeilla havaitaan muutokset riskikontekstissa ja tunnistetaan hälyttävät riskit. [35]

Toimiva ja tehokas sisäinen valvonta ja riskienhallinta tukevat turvallisuuden suunnittelua ja päätöksentekoa. Arvioinnissa syntyvässä analyysissä voidaan tarkastella ja kehittää mm. seuraavia asioita: turvallisuuskulttuuri, turvallisuusjohtaminen, henkilöturvallisuus, fyysinen turvallisuus, tietoturvallisuus ja lainmukaisuus.

[35] ISO 31000:2900 standardi.
Uusitalo, s. 50.
http://www.pk-rh.fi/index.php?page=henkiloriskit

3 Riskihenkilön hallinta henkilöstöturvallisuuden keinoin

3.1 Perusteita

Tutkimusten mukaan riskihenkilö pettää organisaation luottamuksen yleensä laskelmoinnin, ei hetkellisen mielijohteen perusteella.[36] Riskihenkilöstä voidaan löytää kolme avainominaisuutta: 1) Pääsyoikeus: Riskihenkilö tarvitsee tiettyyn tasoon saakka pääsyoikeuden resursseihin. 2) Tieto: Riskihenkilö tarvitsee tiedon niistä resursseista, jotka ovat sen saatavilla. 3) Luottamus: Riskihenkilöllä on oikeuksia, joita se voi käyttää ylittääkseen asetetut rajoitukset, mutta henkilöön luotetaan, ettei hän käytä niitä.[37]

Riskihenkilö sijoittuu tutkielmassa henkilöriskien alueeseen. Henkilöriskejä torjutaan henkilöstöturvallisuuden keinoin. Siinä on keskeistä suunnitelmallinen ja järjestelmällinen henkilöstön kehittämien, johtaminen ja henkilöstöasioiden hallinto. Henkilöstöturvallisuustyöllä vähennetään oman henkilöstön aiheuttamaa tuottamuksellista uhkaa muun muassa ohjeistamalla, kouluttamalla, kehittämällä työmenetelmiä ja vaikuttamalla asenteisiin[38].

Henkilöstöturvallisuuden vastuut kirjataan henkilöiden toimenkuviin. Esimiehillä on vastuu seurata turvallisuuden toteutumista omassa yksikössään ja alaistensa toiminnassa. Puolet kaikista tietoturvarikkomuksista liittyy organisaation menettelytapoihin.[39] Henkilöstöturvallisuuden osalta tietotur-

---

[36] Catrantzos, s. 7. Allen ja Polmar ovat julkaisseet tutkimuksen, jossa tutkittiin yli 70 sisäisen petturin tapausta. 80-luvun petturit olivat kasvottomia, vaatimattomia ja tavallisia ihmisiä.

[37] Matt Bishop ja muut, s. 8. http://web.cs.ucdavis.edu/~peisert/research/insiderthreat-chapter-final-prepress.pdf.

[38] Valtiovarainministeriö, VAHTI-ohje 2/2008, s 19.

[39] Valtiovarainministeriö, VAHTI-ohje 2/2008, s 14.

vatason arviointi vaatiikin siten arvioijalta ihmistuntemusta ja näkemystä kyseisestä osa-alueesta.

Seuraavissa alaluvuissa käsitellään mahdollisia riskihenkilön aiheuttamia riskejä ja niiden käytännön hallintakeinoja työuran näkökulmasta.

3.2 Rekrytointi

Riskihenkilön torjunta alkaa jo ennen kuin henkilö on aloittanut työskentelyn organisaatiossa. Turvallisuusorganisaation ja henkilöstöhallinnon yhteistyöllä on luotava prosessi henkilön rekrytoinnista alkaen pahimman riskihenkilövaihtoehdon mukaan, joka on suunnitelmallinen organisaatioon tunkeutuminen vahingoittamis- tai vakoilutarkoituksessa. Hyvän riskihenkilön käsittelyohjelman tavoitteena on ennalta ehkäistä, tunnistaa ja keskeyttää riskihenkilön toiminta. Ohjelman toteuttajien on kyberturvallisuuden ohella tunnistettava henkilöstö ja salassa pidettävä tieto.[40]

Henkilöstöturvallisuudesta huolehtiminen alkaa rekrytoinnin yhteydessä tehtävistä taustatarkistuksista ja turvallisuusselvityksistä, joihin mahdollinen tunkeutuja ensimmäisenä törmää organisaatioon pyrkiessään. Tarkistusten tavoitteena on varmistaa, että henkilö on sopiva erityistä luotettavuutta edellyttävään tehtävään. Taustatarkastukset kannattaa tehdä useammasta toisistaan riippumattomista lähteistä, jossa hyödynnetään asiaan objektiivisesti suhtautuvia ammattilaisia.

Henkilöturvallisuusselvitystä voi hakea määrätyiltä turvallisuusviranomaisilta: poliisilta, suojelupoliisilta tai pääesikunnalta. Turvallisuusselvitys on valtion virkamiehelle edellytys virkaan nimittämiselle. Muiden tehtävien osalta hakuoikeudet suppean, perusmuotoisen tai laajan turvallisuusselvityksen osalta on selvitetty seikkaperäisesti turvallisuusselvityslaissa.[41] Organisaation kannattaa hyödyntää tämäkin mahdollisuus mahdollisen riskihenkilön torjunnassa.

---

[40] http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection.

[41] Turvallisuusselvityslaki 726/2014, 15§ - 22§: Valtion virkamiehestä haetaan turvallisuusselvitystä, jos henkilö hoitaa sellaisia tehtäviä, joissa hän salassa pidettäviä tietoja paljastamalla tai muulla lainvastaisella teolla voi merkittävällä tavalla vaarantaa valtion turvallisuutta, maanpuolustusta, kansainvälisiä suhteita, poikkeusoloihin varautumista, väestönsuojelua tai yhteiskunnan elintärkeitä toimintoja taikka mainittujen etujen suojaamiseksi toteutettuja turvallisuusjärjestelyjä. http://www.finlex.fi/fi/laki/alkup/2014/20140726#Pidp4076896

Työhaastattelu on vaihe, jolloin on hyvä mahdollisuus tehdä henkilökohtaisia havaintoja hakijasta. Haastattelijoina käytetään useampaa henkilöä samanaikaisesti, jolloin eri henkilöt pystyvät havainnoimaan haastateltavassa eri asioita. Riskihenkilön torjunnan näkökulmasta luotettavuuden arviointi on tärkein ja sen selvittämisessä kehonkieli on oleellisessa asemassa. Psykologin arvio henkilöstä on kullan arvoinen[42].

3.3 Koeaika

Henkilön valinnan jälkeen hänet otetaan koeajalle. Se on riskihenkilön torjunnan kannalta merkittävä vaihe, joka kannattaa ottaa vakavasti. Sen ajaksi uudelle työntekijälle määrätään valvoja, joka on hänen kanssa läheisessä tekemisessä koko koeajan. Koeajan ajaksi uudelle työntekijälle määritetään myös rajoitetut pääsyoikeudet organisaation tietoon, koska koeaika voi päättyä myös työsuhteen purkamiseen eikä organisaatio halua menettää sensitiivistä tietoaan[43].

Koeaika päättyy, kun työntekijä osoittautuu henkilöksi, joka kannattaa pitää. Tämän arvion ei anna pelkästään määrätty valvoja, vaan koko työtiimi, joka on päivittäin läheisessä tekemisessä uuden henkilön kanssa. Jatkuva yhteydenpito työkavereiden kesken ja tiimin sisäinen valvonta vähentävät koeajalla olevan mahdollisuuksia salailevaan toimintaan tai organisaation sabotointiin. Usean henkilön yhtäaikainen läsnäolo kriittisissä toiminnoissa on kannatettava tekniikka läpi koko työuran eikä pelkästään koeaikana[44]. Se

---

42 Laki yksityisyyden suojasta työelämässä, 13.8.2004/759, 13§. Työntekijää voidaan hänen suostumuksellaan testata henkilö- ja soveltuvuusarvioinnein työtehtävien hoidon edellytysten tai koulutus- ja muun ammatillisen kehittämisen tarpeen selvittämiseksi. http://www.finlex.fi/fi/laki/ajantasa/2004/20040759#L4P13

43 Työsopimuslaki 26.1.2001/55, 4§. Työnantaja ja työntekijä voivat sopia työnteon aloittamisesta alkavasta, enintään neljän kuukauden pituisesta koeajasta. Koeajan kuluessa työsopimus voidaan molemmin puolin purkaa.
https://www.finlex.fi/fi/laki/ajantasa/2001/20010055#L1P4

44 Catrantzos, s. 25-27.
European Aviation Safety Agency, EASA, SIB 2015-04 turvallisuustiedote, 27.3.2015, http://ad.easa.europa.eu/ad/2015-04. Euroopan lentoturvallisuusviranomainen EASA ohjeisti lentoyhtiöitä vastaavaan toimintatapaan Germanwingsin lennon 4U9525 dramaattisten tapahtumien jälkeen. EASA toivoo lentoyhtiöiden arvioivan uudelleen turvallisuusriskejä, jotka liittyvät lentäjien poistumiseen ohjaamosta operatiivisista tai fysiologista tarpeista johtuen lennon ei kriittisissä vaiheissa. EASA antoi lentoyhtiöille väliaikaisen suosituksen varmistamaan, että ohjaamossa olisi aina yhden lentäjän lisäksi myös toinen miehistön jäsen eli ns. kaksi henkeä ohjaamossa –sääntö.

lisää työyhteisön sisäistä luottamusta, turvallisuuden tunnetta ja läpinäkyvyyttä.

3.4 Työsuhde

Riskihenkilöiden tunnistamiseksi ja paljastamiseksi on analysoitava tietojärjestelmätietoja ja niiden yhteyksiä, joita ei ole aikaisemmin havaittu (data mining)[45] sekä käytettävä käyttäytymiseen perustuvia tekniikoita. Toiminnassa keskitytään diagnostiikkaan ja käyttäytymiseen liittyvien indikaattoreiden havainnointiin. Psykologiset riskitekijät voivat vaihdella tyytymättömistä työntekijöistä, elämäntilanteesta johtuvaan korkeaan stressiin (esim avioero tai taloudelliset ongelmat), haavoittuviin ja egoistisiin henkilöihin. Näissä tapauksissa nousee tärkeään rooliin tiedonvaihto henkilöstöhallinnon kanssa.[46]

Taustatarkistuksia tehdään myös työsuhteen aikana satunnaisesti[47] ja toimenkuvien muuttuessa. Henkilöstöhallinnolla on oltava riittävä asiantuntemus tarkistuksia ja testauksia koskevasta lainsäädännöstä sekä niissä käytettävistä menetelmistä. Tarkistustiedot tallennetaan organisaation henkilöstörekisteriin[48]. Henkilön mahdollisesti aiheuttamien riskien arvioinnissa on arvioitava henkilön luotettavuutta, lojaaliutta, vastuullisuutta ja osaamista. Erilaiset vaitiolo- ja salassapitosopimukset sekä niiden ajantasaisuudesta huolehtiminen kuuluvat tietoturvavastuiden hallinnointiin. Niistä on tehtävä kirjausmerkintä henkilöstörekisteriin.[49]

Mikäli esimerkiksi tiedot turvaselvityksistä on viety organisaation henkilöstörekisteriin ja toisaalta tiedetään, keistä selvitykset tulisi tehdä, saadaan helposti kokonaiskuva tilanteesta. Erilaisen ohjeistuksen olemassaolosta tai teknisistä järjestelyistä, kuten todentamisen toteuttamisesta tietojärjestelmissä, voidaan tehdä tarkistuslistoja, jotka kuvaavat organisaation henkilöstö-

---

45 http://searchsqlserver.techtarget.com/definition/data-mining

46 FBI, National Insider Threat Task Force Mission Fact Sheet, http://www.fbi.gov/

47 Catrantzos, s. 39-40. Lähde painottaa työntekijöiden auditoinnin satunnaisuutta.

48 Henkilötietolaki, 22.4.1999/523, 8§.

49 Valtiovarainministeriö, VAHTI-ohje 2/2008, s 21.

turvallisuuteen panostamisen astetta. Näitä asioita pyritään mittaamaan henkilöstöturvallisuuden arviointilomakkeilla.[50]

Työuran aikana riskihenkilön aiheuttamaa riskiä voidaan pienentää suunnitelmallisella henkilöstön työtehtävien kierrolla. Sillä edistetään sitoutumista, työhyvinvointia ja mielenkiinnon säilymistä työtehtäviin ja samalla vähennetään riskiä leipääntymiseltä ja henkilön omien ”työtä helpottavien menetelmien” muodostumiselta vastoin organisaation virallista toimintatapaa.

Turvallisuushenkilöstön kierrättäminen organisaation eri osissa on suositeltavaa, erityisesti siellä, missä organisaation ydintoiminta tapahtuu. Samoin organisaation sisältä voidaan siirtää henkilöstöä turvallisuustoimialalle, jolloin luottamus ja osaaminen organisaation eri toimintoihin kasvavat. Toinen taktiikka perustuu turvallisuusorganisaation ja käyttäjien välisen yhteistoiminnan tiivistämiseen. Eräs metodi on luoda turvallisuusorganisaatio ulkoistamalla se ulkoiselle ryhmälle, joka ei houkuta riskihenkilöitä toimimaan uhkaavalla tavalla.[51]

Työntekijöitä voidaan valvoa teknisin järjestelmin ja apuvälinein. Pohja riskihenkilöiden aikeiden paljastuksille luodaan tietojärjestelmäkäyttäytymisen seurannalla (aineiston määrä, toiminnan tiheys ja toistuvuus) ja siihen liitettävillä taktiikoilla, kuinka uhkaava käyttäytyminen saadaan esiin.[52]

Työntekijöiden valvonnan järjestelyissä on otettava huomioon laki yksityisyyden suojasta työelämässä. Sen mukaisesti työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella. Teknisin keinoin toteutetun valvonnan säännöt ja menettelyt sekä sähköpos-

[50] Valtiovarainministeriö, VAHTI-ohje 2/2008, s 14.

[51] Catrantzos s. 45-46.
http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection
http://searchcio.techtarget.com/definition/crowdsourcing

[52] FBI, National Insider Threat Task Force Mission Fact Sheet, http://www.fbi.gov/

tin ja tietoverkkojen käyttösäännöt on käytävä yhteistoiminta- tai kuulemismenettelyssä työpaikalla.[53]

Teknisillä järjestelmillä voidaan työntekijää myös ohjata oikeaan turvallisuuskäyttäytymiseen. Esimerkiksi näyttöpäätteelle ilmestyvät varoitukset aina, kun käyttäjä yrittää ladata sensitiivistä tietoa järjestelmistä ulkoiseen muistiin. Se osoittaa työntekijöille, että joku valvoo heidän tekemisiään. Eräs keino on antaa työkaluja ja mahdollisuuksia suoraan käyttäjille suojaamaan, kryptaamaan ja luokittelemaan käyttämänsä tieto. Tällä tavoin vastuuta tietoturvallisuudesta siirretään tavallisille käyttäjille ja hyödynnetään sosiaalisen manipuloinnin keinoja (social engineering) turvallisuustietoisuuden nostamiseksi.[54]

Riskihenkilön muodostamia riskejä pienennetään organisatorisilla henkilöstöturvallisuuskeinoilla. Turvallisen toiminnan perusperiaatteena on, että tietoja saa vain työtehtävään ja lähtökohtaisesti vain vähimmäistarpeeseen. Tärkeimpänä on määriteltävä pääsyoikeudet tietoon ja tiloihin eli kenellä tai millä ryhmillä ja millä periaatteilla on oikeus päästä tiloihin sekä saada tietoja haltuunsa ja käsitellä tietoja. Sitten määritellään kenellä on pääsy organisaation materiaaliin ja järjestelmiin eli ketkä saavat käsitellä organisaation toiminnalle kriittisimpiä välineitä, kuten ohjelmistoja, tietokantoja, salausavaimia, palomuureja, reitittimiä tai palvelimia.[55]

Organisaatioiden on myös määriteltävä henkilöstönsä osaamisprofiilit sekä määriteltävä, kuka on avainhenkilö, jolla on oltava sijaisia, ja kuka on kykenevä toimimaan sijaisena. Hyvään turvallisuuspolitiikkaan kuuluu myös määritellä kuka ylläpitää pääsy-, valtuus- ja hallintatietoja ja kenellä on siihen tietoon pääsyoikeus. Samoin on määriteltävä, miten järjestelmän ylläpi-

---

53 Laki yksityisyyden suojasta työelämässä, 13.8.2004/759, 3-4§ ja 21§. Työnantajan on kerättävä työntekijää koskevat henkilötiedot ensi sijassa työntekijältä itseltään. Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, työntekijältä on hankittava suostumus tietojen keräämiseen. Lain perustelujen mukaan työnantajalla on oikeus työn johto ja valvontaoikeutensa perusteella päättää valvontatavoista, jos ne muutoin ovat sallittuja. Työnjohto ja valvontaoikeutta rajoittavat tietyt perusoikeudet, työlainsäädäntö ja työntekijöihin ja virkamiehiin ja heidän työnantajiinsa sovellettava muu lainsäädäntö.

54 http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection
http://searchcio.techtarget.com/definition/crowdsourcing

55 Valtiovarainministeriö, VAHTI-ohje 2/2008, s 27.

täjiä valvotaan ja estetään tekemästä virheitä tai rikkomuksia. Toiminnassa on vältettävä sisäisiä riskejä lisääviä työyhdistelmiä sekä ehkäistä virheiden ja väärinkäytösten mahdollisuutta. Yksikään henkilö ei voi olla turvatussa käsittelyketjussa vastuussa enempää kuin yhdestä käsittelyketjun suorituksesta, esimerkiksi valtuuttamisesta, hallussapidosta tai kirjanpidosta.[56]

3.5 Työsuhteen päättyminen

Organisaatiolla on oltava selkeät ohjeet niistä toimenpiteistä, jotka on tehtävä työsuhteen päättyessä. Henkilöltä poistetaan käyttö- ja kulkuoikeudet. Henkilö velvoitetaan palauttamaan organisaation materiaali ja muu omaisuus. Huomattava, että työtehtäviin liittyvät sähköpostit ja tietoaineistot eivät lähde työntekijän mukaan, vaan ne siirretään seuraajalle tai tuhotaan tarpeettomina. Lähtijää on muistutettava salassapitovelvoitteista ja arvioitava, mitä tietotaitoa hän vie mennessään ja kuinka kriittistä sen on organisaation ydintoiminnalle. Työsuhteen päättymisestä on tiedotettava organisaation henkilöstölle, jotta katkaistaan organisaatiolle kriittisen tiedon vuotamisesta entiselle työntekijälle ja mahdolliselle kilpailijalle.[57]

Riitatilanteen seurauksena purkautuneen työsuhteen päättymiseen on myös varauduttava. Tällöin eronneen tai erotetun työntekijän pääsy organisaation tietojärjestelmiin on estettävä välittömästi eroilmoituksen jälkeen sekä huolehdittava järjestelmien lokien tarkistamisesta järjestelmien tavanomaisesta poikkeavan käytön selvittämiseksi. Tulehtuneessa tilanteessa on työntekijä saatettava työpisteelleen, josta hän valvotusti kerää henkilökohtaisen omaisuutensa, minkä jälkeen hänet saatetaan ulos toimitiloista. Samalla on huolehdittava työntekijälle luovutettujen käyttäjätunnusten, kulkulupien, avainten ja muiden pääsyoikeuksien peruuttamisesta ja pois ottamisesta.[58]

[56] Valtiovarainministeriö, VAHTI-ohje 2/2008, s 27.

[57] Sama, s 42.

[58] Sama, s 20.

4 Yhdistelmä

Tutkimuksen pääkysymyksenä on selvittää millaisen riskin riskihenkilö muodostaa organisaatiolle ja miten riskiä voidaan hallita. Riskihenkilö uhkaa organisaation turvallisuutta sisältäpäin. Tästä muodostuvat riskit ovat organisaation sisäisiä operatiivisia henkilöriskejä. Riskihenkilöksi luetaan henkilö, jonka voidaan perustellusti arvioida aiheuttavan riskejä organisaatiolle tai vaarantaa sen toimintaa. Riskihenkilö tarvitsee pääsyoikeuden organisaation resursseihin, joita hän voi käyttää vahingoittaakseen organisaation etuja. Riskihenkilö pettää organisaation luottamuksen yleensä laskelmoinnin perusteella käyttäen väärin hänelle myönnettyjä pääsyoikeuksia.

Riskihenkilön tarkastelu pelkästään standardin mukaisessa riskienhallintaprosessissa tekee riskin käsittelystä kaavamaisen ja teknisen. Riskienhallintaprosessin mukaisessa ongelmankäsittelyssä painottuvat riskin tunnistamis- ja riskin analysointivaiheet. On kuitenkin muistettava, että ongelma ei ole tekninen, vaan ihmiskeskeinen. Ihmiset ovat moniulotteisia, joten ongelmaa on käsiteltävä monelta eri osa-alueelta. Henkilötietojen keräämisessä ja käsittelyssä on otettava huomioon yksityisyyden suojasta säädetyt lait. Tästä näkökulmasta tarkasteltuna ongelman käsittelyssä varmin tie on ensin laittaa organisatoriset, henkilöriippumattomat riskienhallintamenetelmät kuntoon ja sen jälkeen edetään henkilöriippuvaisten menetelmien hyödyntämiseen.

Ongelma ei ole myöskään pelkästään turvallisuusorganisaation ratkaistavissa; sen hallintaan tarvitaan koko organisaation yhteistoimintaa. Hallitakseen riskihenkilöihin liittyviä riskejä organisaatiolla on oltava hyvä riskihenkilön käsittelysuunnitelma. Suunnitelmassa keskitytään ilmiön ennalta ehkäisyyn, ei niinkään paljastamiseen. Ennalta ehkäisy alkaa jo ennen kuin henkilö on aloittanut työskentelyn organisaatiossa. Tunnistamisvaihe on riskihenkilön ennalta estämisen ja paljastamisen kannalta keskeinen. Organisaatioon on luotava järjestelmällinen toimintamalli, jossa henkilöstön taustoja tarkastellaan rekrytoinnista alkaen ja jatkaen satunnaisesti koko työuran ajan. Tarkis-

tusten tavoitteena on varmistaa, että henkilö on sopiva tehtävään eikä muodosta riskiä organisaation ydintoiminnalle. Uuden työntekijän koeaika on riskihenkilön torjunnan kannalta merkittävä vaihe, jonka aikana työntekijän motivaatio, luotettavuus toimintatavat arvioidaan. Usean henkilön yhtäaikainen läsnäolo kriittisissä toiminnoissa on kannatettavaa läpi koko työuran eikä pelkästään koeaikana. Sillä vahvistetaan keskinäistä luottamusta ja kyetään paremmin havainnoimaan poikkeamia.

Toimiva ja tehokas sisäinen valvonta ja riskienhallinta tukevat turvallisuuden suunnittelua ja päätöksentekoa ja parantavat siten organisaation tuloksia ja tavoitteiden saavuttamisen mahdollisuuksia. Riskihenkilön aiheuttamia riskejä ennalta estetään ja torjutaan henkilöstöturvallisuuden keinoin, johon sisältyvät suunnitelmallinen henkilöstön kehittämien, johtaminen ja henkilöstöasioiden hallinto. Henkilöstöturvallisuuden arvioinnin yhteydessä havaittuja tyypillisiä korjattavia kohteita ovat: Taustaselvityksen puutteet, riittämättömät tai sopimattomat henkilöt, henkilöstön käytettävyyden arviointi, varahenkilöjärjestelyt, tietoturvaohjeistuksen, sääntöjen tiedottamisen ja valvonnan sekä koulutuksen puutteet. Riskien syntymisen välttäminen tai poistaminen edellyttää henkilöstön tekemien toimenpiteiden valvontaa ristiin- ja kaksoistarkistuksin sekä hyödyntämällä monitasoisia turvajärjestelyjä, jossa pääsy- ja käyttöoikeudet on lokeroitu luokittain ja henkilöryhmittäin riittävän pieniin osiin kokonaisuuden suojaamiseksi.

Hyvän turvallisuuskulttuurin omaavan organisaation ominaispiirteitä ovat keskinäiseen luottamukseen perustuva viestintä, yhteinen käsitys turvallisuuden merkityksestä ja luottamus ennalta ehkäisevien toimien tehokkuuteen. Henkilöstöä on koulutettava havaitsemaan poikkeavaa toimintaa. Esimerkiksi varojen käyttöön liittyvät väärinkäytökset paljastuvat tilintarkastajien ja tietojärjestelmien väärinkäytökset IT-organisaation toimenpitein. Kun taas henkilökohtaiset ja käyttäytymiseen liittyvät ongelmat näyttäytyvät ensin työkavereille ja henkilöstöhallinnolle.

Riskihenkilöä ja siitä muodostuvan ongelman käsittelymahdollisuuksia organisaatiossa kuvataan tutkielmassa yleisellä tasolla eikä kaikkia toimenpiteitä verrata Suomen lainsäädännön suomiin mahdollisuuksiin tai asettamiin rajoituksiin. Joissakin tutkielmassa esitetyissä toimenpiteissä lainsäädäntö saattaa tehdä jotkin tutkielmassa esitetyt toimenpiteet vaikeiksi toteuttaa tai jopa mahdottomiksi.

Riskihenkilöiden paljastamisen ja ennalta ehkäisyn tietämys Suomessa on alkuvaiheessa ja toiminnassa on pystyttävä hyödyntämään käyttäytymistieteen tekniikoita. Ongelman jatkotutkimiseksi voi olla hyödyllistä kerätä organisaatioiden turvallisuus- ja henkilöstöjohdon mielipiteitä riskihenkilön käytännön käsittelystä ja edelleen pyrkiä maastouttamaan heiltä saatuja ajatuksia suomalaiseen organisaatiokontekstiin ja lainsäädäntöön.

LÄHTEET

LAIT

Henkilötietolaki, 22.4.1999/523.

Laki yksityisyyden suojasta työelämässä, 13.8.2004/759.

Suomen perustuslaki, 11.6.1999/731.

Turvallisuusselvityslaki 726/2014.

Työsopimuslaki 26.1.2001/55.

OHJEET JA STANDARDIT

ISO 31000:2009, Risk management – Principles and guidelines, 15.11.2009.

Valtiovarainministeriö, VAHTI-ohje 2/2008, ISBN 978-951-804-799-8: Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta.

KIRJALLISUUS

Catrantzos Nick: Managing the Insider Threat – No Dark Corners, CRC Press, New York, 2012.

Halonen Kristiina: PARI ASKELTA JÄLJESSÄ – tuurilla mennään, Aalto-yliopisto, Tuotantotalouden laitos, väitöskirja, 2013.

Department of Defense Office of the Inspector General, USA: "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," Report No. PO 97-049, 25.9.1997.

Tuomi, Jouni, Sarajärvi, Anneli: Laadullinen tutkimus ja sisällönanalyysi, Tammi, 2002.

INTERNET-ARTIKKELIT

Bishop Matt, Engle Sophie, Frincke Deborah A., Gates Carrie, Greitzer Frank L., Peisert Sean, and Whalen Sean: A Risk Management Approach to the "Insider Threat". http://web.cs.ucdavis.edu/~peisert/research/insiderthreat-chapter-final-prepress.pdf

CNN, 2.4.2015, http://edition.cnn.com/2015/04/02/europe/france-germanwings-plane-crash-main/index.html

Department of Defense, USA
DoD Insider Threat Mitigation, Final Report of the Insider Threat Integrated Process Team, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380

Department of Defense, Instruction 5240.26, May 4, 2012, Incorporating Change 1, Effective October 15, 2013. http://www.dtic.mil/whs/directives/corres/pdf/524026p.pdf

European Aviation Safety Agency, EASA, SIB 2015-04 turvallisuustiedote, 27.3.2015, http://ad.easa.europa.eu/ad/2015-04.

Federal Bureau of Investigation
http://www.fbi.gov/

http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection.

FBI: National Insider Threat Task Force Mission Fact Sheet, http://www.fbi.gov/.

FBI: The Insider Threat, An introduction to detecting and deterring an insider spy. http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.

Helsingin sanomat, 24.3.2015: http://www.hs.fi/ulkomaat/a1305940962506.

http://searchcio.techtarget.com/definition/.

http://www.praxiom.com/iso-31000-terms.htm#2.22_Risk_criteria.

https://www.yksityisyydensuoja.fi/lains%C3%A4%C3%A4d%C3%A4nt%C3%B6.

Suomen Riskienhallintayhdistys, http://www.pk-rh.fi/index.php?page=henkiloriskit.

Valtiokonttori, luonnos asiakirja organisaation riskienhallintapolitiikasta: http://www.valtiokonttori.fi/download/noname/%7BEC6E11CB-4462-4390-8C21-E72F96EFAB7F%7D/84882.

VTT: http://www2.vtt.fi/proj/riskianalyysit/riskianalyysit_maaritelmia.jsp.

MUUT LÄHTEET

Kortelainen Helena, VTT, luentomateriaali: Cost-Benefit tarkastelut riskitietoisen päätöksenteon pohjana, TJK13, jakso 2, 2013.

Uusitalo, Teuvo, VTT: luentomateriaali, TJK13, jakso 2, 2013.

Väisänen, Lassi: ennakkolukumateriaali TJK13:lle, käsittelee ISO 31000:2900 standardia, 24.5.2012.

LIITTEET

Liite 1, Riskihenkilöindikaattorit, henkilökohtaiset ominaisuudet[59]

Henkilökohtaiset ominaisuudet		
Indikaattorit	Kuvaus	Riskiluku
Ahneus tai taloudelliset vaikeudet	Usko, että raha korjaa kaiken. Mahdolliset kohtuuttomat velat tai suunnattomat kulut. Eläminen yli varojen. Velkaantuminen muille kuin virallisille tahoille.	
Selittämättömät vihanpuuskat ja koston halu	Tyytymättömyys, joka aiheuttaa halun kostaa organisaatiolle tai muille henkilöille.	
Ongelmat työssä	Arvostuksen puute, erimielisyydet vertaisten tai esimiesten kanssa, tyytymättömyys työhön, odotettavissa oleva lomautus.	
Ideologia	Halu auttaa altavastaajaa, poliittiset näkemykset tai muu erityinen syy	
Jakautunut lojaalisuus	Uskollisuus toisille ihmisille tai yritykselle, tai muulle valtiolle kuin Suomelle	

59 Nick Catrantzos, Managing the Insider Threat – No Dark Corners, CRC Press, New York, s. 18-170.
FBI, The Insider Threat, An introduction to detecting and deterring an insider spy. http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure

Henkilökohtaiset ominaisuudet		
Indikaattorit	Kuvaus	Riskiluku
Seikkailun tunne ja jännitys	Halu lisätä jännitystä elämään, kaikenlaiset salaiset toimet ja menetelmät kiinnostavat.	
Mahdollisuus joutua kiristyksen kohteeksi	Avioliiton ulkopuoliset suhteet, peitelty sukupuolinen suuntautuminen[60], uhkapelaaminen, petos.	
Sairaus[61]	Mielenterveyden järkkymiseen viittaava syy, kuten itsetuhoisuus tai harhakuvitelmat ja olemattomien asioiden havainnointi, jotka kohdistuvat itseensä tai lähiympäristöön. Alkoholismin tai muiden riippuvuutta aiheuttavien aineiden käytön seurauksesta johtuva toiminta.	
Ego ja minäkuva, ylimielisyys	”Minä olen sääntöjen yläpuolella” –asenne, narsismi tai halu korjata itseluottamukselle tapahtuneet kolaukset. Henkilöä on helppo imarrella ja lupailla hänelle parempi työpaikka.	
Miellyttämisen halu	Halu miellyttää tai saavuttaa jonkun hyväksyntä, joka hyötyy sisäpiiritiedosta, liitettynä odotukseen saatavasta vastapalveluksesta.	
Empatiakyvyn puute	Ei kykene asettumaan toisten ihmisten/organisaation asemaan eikä kykene näkemään tekojensa seurauksia.	

[60] Henkilötietolaki, 22.4.1999/523, 11§: Huomattava, että Suomen henkilötietolaki ei salli rekisteröintiä henkilön seksuaalista suuntautumista tai käyttäytymistä. https://www.finlex.fi/fi/laki/ajantasa/1999/19990523?search[type]=pika&search[pika]=henkil%C3%B6rekisteri#L3P11

[61] Henkilötietolaki, 22.4.1999/523, 11§: Huomattava, että Suomen henkilötietolaki ei salli rekisteröintiä, jotka kuvaavat henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia.

Henkilökohtaiset ominaisuudet		
Indikaattorit	Kuvaus	Riskiluku
Voimakas kiinnostus tai sympatisointi	Järjestäytynyt rikollisuus, poliittiset, aatteelliset tai uskonnolliset ääriliikkeet.	
Pakonomainen ja turmiollinen käytös	Huumeiden tai alkoholin väärinkäyttö, tai muuhun riippuvuuteen liittyvä käytös	
Perheongelmat	Avioliitto-ongelmat tai erossa oleminen rakkaista ihmisistä tai avioeron jälkeiset ongelmat (esim. lasten elatus/huoltajuus, tulehtuneet välit ex -aviopuolisoon).	
Kohtuuton salailu	Pyrkii salaamaan kaikkea, missä on osallisena; asuminen, liikkuminen, työ, vapaa-aika.	

Liite 2, Riskihenkilöindikaattorit, käyttäytymiseen liittyvät indikaattorit[62]

Käyttäytymiseen liittyvät indikaattorit		
Indikaattorit	Kuvaus	Riskiluku
Omaisuuden tai tiedon luvaton käyttö	Ilman lupaa tai tarvetta, vie kotiinsa organisaation omaisuutta tai muuta materiaalia asiakirjoina, muistitikuilla, kovalevyillä tai sähköpostitse.	
Korostunut uteliaisuus	Etsii tai saa käyttöönsä sopimattomasti turvaluokiteltua tai muuta materiaalia asioista, jotka eivät liity hänen työtehtäviinsä	
Kiinnostus ulkopuolisiin toimijoihin	On kiinnostunut tehtäviensä ulkopuolisista asioista, jotka liittyvät erityisesti ulkomaisiin toimijoihin tai kilpaileviin yrityksiin.	
Tarpeeton kopiointi	Kopioi tarpeettomasti materiaalia, jos se on jonkun muun omaisuutta tai turvaluokiteltua.	
Tietojärjestelmien etäkäyttö	Käyttää etänä tietojärjestelmiä ollessaan lomalla, sairauslomalla tai vapaa-aikanaan.	
Välinpitämättömyys tietoturvaan	Ei noudata tietoturvaohjeistuksia, jotka liittyvät omien ohjelmistojen tai komponenttien asentamiseen, pääsyyn rajoitetuille internetsivuille, luvattomien hakujen suorittamiseen tai luottamuksellisen tiedon lataamiseen.	

[62] Nick Catrantzos, Managing the Insider Threat – No Dark Corners, CRC Press, New York, s. 18-170.
FBI, The Insider Threat, An introduction to detecting and deterring an insider spy. http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure

Käyttäytymiseen liittyvät indikaattorit		
Indikaattorit	Kuvaus	Riskiluku
Oudot työajat	Työskentelee outoina aikoina, omaa huomattava halua tehdä ylitöitä, tai halua työskennellä viikonloppuisin tai muuten epätavallisina aikoina, jolloin mahdollisuus tehdä asioita peitellysti	
Ulkomaan kontaktien ja –matkojen salaaminen	Raportoimattomia ulkomaalaiskontakteja (erityisesti ulkomaisten hallitusten edustajat) tai raportoimattomia ulkomaanmatkoja. Selittämättömiä tai oudoista syistä tehtyjä lyhyitä ulkomaanmatkoja.	
Äkkirikastuminen	Selittämätön vauraus: ostaa asioita, joihin kotitalouden tulot eivät riitä	
Epäilyttävät yhteydet	Omaa epäilyttäviä henkilökontakteja, kuten kilpailevien yritysten edustajat, liikekumppanit tai muut epäilyttävät henkilöt.	
Pettymykset	On henkilökohtaisten kriisien tai uraan liittyvien pettymysten musertama	
Epätavallinen kiinnostus kollegojen elämään	Osoittaa epätavallista kiinnostusta työtovereittensa henkilökohtaiseen elämään, kyselee esim. asiattomia kysymyksiä liittyen taloudelliseen tilanteeseen tai parisuhteeseen	
Valvonnan paljastaminen	On huolissaan, että on tutkinnan kohteena; jättää kotiinsa tai työpaikalleen ansoja paljastaakseen mahdolliset kotietsinnät; etsii mikrofoneja ja kameroita. Epäilee, että häntä tarkkaillaan.	

Käyttäytymiseen liittyvät indikaattorit		
Indikaattorit	Kuvaus	Riskiluku
Piittaamattomuus yhteiskunnan säännöistä	Epäillään toistuvasti syyllistyneen rikoksiin tai on muuten tekemisissä poliisin kanssa: juopumuspidätykset tai poikkeuksellisen suuri määrä tekoja joissa on asianomistaja-asemassa.	
Omat julkitulot ja paljastukset	Tekee irtiottoja organisaation ulkoisesta ja sisäisestä tiedotuslinjasta. Pyrkii syyllistämään muita henkilöitä ja heidän tekemisiä.	
Suoritusten romahtaminen	Työntekijän suoritukset ovat järjestään heikompia (huolimattomuus, aikamäärien ylittäminen, piittaamattomuus) aikaisempaan suoritustasoon verrattuna.	