Jere Mustonen

PROJEKTIEN TIETOTURVARISKIT – RISKIEN INDIKAATTORIT JA NIIDEN HYÖDYNTÄMINEN PROJEKTIEN TIETOTURVARISKIENHALLINNASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Mustonen, Jere
Projektien tietoturvariskit – tietoturvariskien indikaattorit ja niiden hyödyntämien projektiriskienhallinnassa
Jyväskylä: Jyväskylän yliopisto, 2020, 57+1 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Niemimaa, Marko

Tietoturvariskienhallinta on kokonaisvaltaista toimintaa, jossa pyritään ottamaan huomioon sekä inhimilliset että tekniset tekijät tavoiteltaessa mahdollisimman tehokkaita ja matalariskisiä prosesseja organisaation toiminnoissa. Tietoturvariskienhallintaa ovat ohjanneet tyypillisesti erilaiset ohjeistukset ja riskienhallintatyökalut, kuten ISO/IEC 27001 ja ISO/IEC 27005. Riskienhallintaan liittyvät ohjeistukset sisältävät lukuisia vaatimuksia siitä, mitkä asiat tulee huomioida riskienhallinnassa, mutta itse riskienhallinnan toteutuksesta ei anneta tarkkoja ohjeita. Yhtenä mahdollisena riskienarvioinnin ja seurannan välineenä voidaan mahdollisesti hyödyntää riski-indikaattoreita. Tutkimus toteutettiin toimeksiantona ja sen tarkoituksena oli analysoida tilaajaorganisaation aiempia projekteja ja löytää niistä realisoituneisiin tietoturvariskeihin viittaavia indikaattoreita. Tutkimuksessa pyrittiin luomaan indikaattoreita aiempien tutkimusten määrittämien indikaattorien luontiprosessien avulla ja analysoimalla aiemmissa projekteissa realisoituneita tietoturvariskejä. Tavoitteena oli tarjota tilaajaorganisaatiolle uutta tietoa ja mahdollisia apukeinoja tietoturvariskien hallintaan tulevissa projekteissa. Tutkimus toteutettiin laadullisena tapaustutkimuksena, jossa pääasiallinen tiedonkeräystapa oli laadullinen puolistrukturoitu haastattelu. Tutkimuksen tulokset osoittivat, että usein realisoituneen tietoturvariskin takana oli inhimilliset syyt, kuten huolimattomuusvirheet, puutteellinen osaaminen ja unohdukset.

Asiasanat: Riskienhallinta, indikaattori, tietoturvallisuus, inhimilliset virheet

ABSTRACT

Mustonen, Jere
Projects' information security risks – information security risk indicators and using indicators to project risk management
Jyväskylä: University of Jyväskylä, 2020, 57+1 pp.
Cyber Security, Master's Thesis
Supervisor(s): Niemimaa, Marko

Information security risk management is a holistic activity which goal is to consider both human and technical factors in order to achieve the most efficient and low-risk processes possible in the organization's operations. Information security risk management has typically been guided by various guidelines and risk management tools, such as ISO / IEC 27001 and ISO / IEC 27005. Risk management guidelines contain numerous requirements on what should be considered in risk management, but there aren't given precise instructions of the implementation of risk management itself. One possible tool for risk assessment and monitoring is the use of risk indicators. This study was carried out as an assignment and its purpose was to analyze the target organization's previous projects and find risk indicators which were related to realized information security risks. The aim of the study was to create indicators by using the process which was defined in previous studies and analyze the realized information security risks in previous projects. The purpose was to provide new information and possible tools for the target organization for managing information security risks in future projects. The study was conducted as a qualitative case study, where the main data collection method was a qualitative semi-structured interview. The results of the study showed that often realized security risk was due to human causes, such as negligence errors, lack of knowledge and forgetting.

Keywords: Risk management, indicator, information security, human error

KUVIOT

TAULUKOT

SISÄLLYS

1 Johdanto

Tieto- ja kyberturvallisuuden merkitys on kasvanut viime vuosikymmenien aikana valtioiden, yksityisten yritysten ja yksilöitten osalta. Yhä laajemmalle levittäytyvä digitalisaatio sekä palvelujen ja järjestelmien verkottuminen lisäävät tarvetta ylläpitää ja kehittää tieto- ja kyberturvallisuutta osana muita toimintoja. Erilaiset organisaatiot joutuvat ottamaan omassa toiminnassaan kokonaisvaltaisesti huomioon tietoturvariskit ja niihin liittyvät varautumistoimenpiteet. Suomen virallisen tilaston (2019) mukaan 18 % kyselyyn vastanneista yrityksistä oli kokenut tietoturvaongelmia, kuten palvelukatkoksia ja tietojen paljastumista. Näin ollen voidaan sanoa tietoturvariskienhallinnan olevan merkittävä osa organisaatioiden toimintaa. Tietoturvariskienhallinta on monimutkaista toimintaa, sillä tietoturvallisuuteen kuuluu lukuisia erilaisia teknisiä ja inhimillisiä elementtejä, jotka tulisi ottaa huomioon.

Tietoturvariskienhallinta pyrkii ensisijaisesti säilyttämään organisaatiolle merkityksellisen tiedon saatavuuden, luottamuksellisuuden ja eheyden. Tietoturvariskienhallintaan on olemassa erilaisia ohjeistuksia ja standardeja, mutta ne eivät välttämättä tarjoa selkeitä ohjeita siihen, mitä organisaation tulisi tehdä tietoturvallisuuden riskienhallinnan kannalta. Standardit ja ohjeistukset toimivat lähinnä dokumentaationa, joka esittää vaadittavat kriteerit hyväksyttävälle tietoturvariskienhallinnalle.

Yhtenä potentiaalisena keinona tietoturvariskienhallinnassa on riski-indikaattoreiden hyödyntäminen. Indikaattorilla tarkoitetaan varoitusmerkkiä, jonka käyttäytyminen seuraa indikaattoriin liitetyn riskin realisoitumisen mahdollisuutta. Indikaattorilla voidaan näin ollen seurata merkittävimpien riskien kehittymistä ja tarvittaessa reagoida niihin, mikäli indikaattorille määritetystä riskin raja-arvoista voidaan tulkita riskin realisoitumisen uhan kasvaneen. Valitun indikaattorin tulee täyttää tiettyjä ominaisuuksia, jotta se voi toimia luotettavana mittarina riskin suhteen. Indikaattorin tulisi olla helppokäyttöinen, mitattavissa ja kohdennettavissa selkeästi yksittäiseen riskiin.

Riski-indikaattoreita on käytetty yleisesti finanssialalla sekä lääketieteessä, mutta indikaattorien käyttö osana tietoturvallisuuden riskienhallintaa on ollut vähäistä. On epäselvää, miksi riski-indikaattoreita ei ole hyödynnetty enemmän

tietoturvallisuuden alalla. Indikaattoreiden käytöstä on näyttöä siitä, että niitä pystyttäisiin hyödyntämään myös tietoturva-alalla osana yleisesti käytettyjä riskienhallintatyökaluja (Özçakmak (2019).

1.1 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tämän tutkimuksen tarkoituksena on tarkastella, millaisia tietoturvariskeihin liittyviä indikaattoreita voidaan löytää tutkimuksen kohdeorganisaation edellisistä projekteista ja kuinka niitä voidaan hyödyntää jatkossa. Tutkimuskysymykset muotoutuivat seuraaviksi:

Mitä tietoturvariskien indikaattoreita projekteista voidaan tunnistaa?

Päätutkimuskysymyksen lisäksi laadittiin kaksi apututkimuskysymystä, joihin tutkimuksella pyrittiin vastaamaan. Apututkimuskysymykset muotoiltiin seuraavasti:

Miten havaittuja indikaattoreita voidaan hyödyntää projektien tietoturvariskien hallinnassa?

Mitkä käytännön työkalut tai menetelmät olivat haastateltavien mielestä toimivia tietoturvallisuuden riskienhallinnassa?

Tutkimukselle koettiin olevan tarve alkuvuodesta 2020, kun tutkimuksen kohdeorganisaatio pyrki päivittämään projektiriskienhallintaan liittyviä prosesseja. Tutkimuksen teoreettinen tausta keskittyy yleiseen riskienhallintaprosessiin sekä projektien että tietoturvallisuuden osalta. Tutkimus toteutetaan laadullisena tapaustutkimuksena, jossa tärkeimmän aineiston muodostavat organisaatiosta valikoitujen asiantuntijoiden puolistrukturoidut haastattelut. Tässä tutkimuksessa ei oteta kantaa positiivisiin riskeihin eikä määritetä havaituille indikaattoreille seurattavia raja-arvoja.

Tutkimuksessa ilmeni, että suurin osa aiemmissa projekteissa realisoituneista tietoturvariskeistä on kytköksissä inhimillisiin virheisiin. Tämä viittaa siihen, että henkilöstön koulutukseen ja perehdytykseen tulee panostaa enemmän, sillä erilaiset unohdukset ja virheet liittyvät usein puutteelliseen osaamiseen tai koulutukseen. Tutkimuksessa saavutettuja tuloksia voidaan hyödyntää tutkimuksen tilaajaorganisaation projektien tietoturvallisuuden parantamiseen.

1.2 Tutkimuksen rakenne

Tutkimuksen ensimmäisessä luvussa käsitellään tutkimuksen kannalta keskeisimmät käsitteet ja aiemmat aiheesta tehdyt tutkimukset. Tietoturvallisuuden

osalta käydään erikseen läpi tieto- ja kyberturvallisuuden käsitteet sekä tietoturvallisuuden riskienhallinnan tekijät. Samalla käsitellään lyhyesti tietoturvallisuuden riskienhallintaan kehitettyjä standardeja, tässä tapauksessa ISO/IEC 27001, ISO/IEC 27005 ja COBIT 5. Viimeisenä teoriaosassa käsitellään riskien indikaattorien käsitettä ja indikaattorien muodostamisen prosessia sekä laadullisten ja määrällisten indikaattoreiden eroavaisuuksia.

Tutkimuksen toisen luvun muodostaa menetelmäluku, jossa käsitellään tutkimuksen tekeminen, tutkimusmetodi, tutkimuskohde ja tutkimusaineiston kerääminen. Kolmannessa luvussa analysoidaan kerätty aineisto ja esitellään aineistosta tehdyt havainnot sekä muodostetut riski-indikaattorit. Tutkimuksen neljännessä luvussa esitellään yhteenveto tutkimuksesta, tutkimukseen kohdistuneet rajoitteet, tulosten pohdinta ja mahdolliset jatkotutkimusaiheet.

2 Riskienhallinta ja riski-indikaattorit

Tässä luvussa määritellään tutkimuksen kannalta keskeisimmät käsitteet ja esitellään aiempi aiheesta tehty tutkimus. Riskienhallinnan osalta olennaisia käsitteitä ovat tietoturvallisuus ja tietoturvallisuuden riskienhallinta, riski ja riskienhallinta, projektiriskienhallinta ja riski-indikaattori. Luvussa 2.1 määritellään tietoturvallisuus ja kyberturvallisuus, niiden väliset erot sekä niiden ylläpitämiseen tähtäävät toimenpiteet ja työkalut. Luvussa 2.2 määritellään riskin käsite ja luvussa 2.3 riskienhallinta. Luvussa 2.4 määritellään projekti ja projektiriskienhallinta. Viimeisenä määritellään riski-indikaattorit, niiden ominaisuudet ja määrittäminen luvussa 2.5.

2.1 Tietoturvallisuus ja kyberturvallisuus

Tietoturvallisuus määritellään Gordonin ja Loebin (2002) mukaan yleisesti toimenpiteinä, joiden tavoitteena on suojata tiedon saatavuus, luottamuksellisuus ja eheys. Kyseisistä elementeistä koostuva malli tunnetaan yleisesti CIA-mallina (CIA-lyhenne tulee englannin kielen sanoista *confidentiality, integrity* ja *availability*). Saatavuudella tarkoitetaan, että tieto on saatavilla tarvittaessa eikä tiedon saatavuutta pystytä häiritsemään. Luottamuksellisuudella tarkoitetaan, että tieto on käytössä vain niillä, jotka sitä tarvitsevat tai joilla on siihen oikeus eivätkä muut osapuolet pääse tietoon käsiksi. Tiedon eheydellä viitataan tiedon oikeellisuuteen, eli tiedon voidaan luottaa vastaavan todellisuutta eikä sitä ole päästy esimerkiksi manipuloimaan. Mikäli joku osa-alueista jätetään huomioimatta, on tietoturvallisuus vaarantunut (Gordon & Loeb, 2002).

Raggad (2010) kritisoi kyseistä kolmeen tekijään perustuvaa mallia, koska mainitut tavoitteet eivät ole riittäviä tietoturvallisuuden ylläpitämiseksi. Vaikka vaadittavaan kolmitasoiseen malliin lisätään tietoturvatavoitteet, laajennettukaan malli ei riitä turvallisuuden saavuttamiseen, jos turvallisuuden hallintaa ei sisällytetä turvallisuusmalliin. Vaihtoehtoinen tietoturvallisuuden riskienhallinnassa käytettävä viidestä elementistä koostuva malli (engl. Security Star) lisää aikaisempien elementtien lisäksi malliin autentikoinnin ja kiistämättömyyden. Autentikointi on prosessi, jossa tunnistetaan käyttäjä järjestelmään pääsyn yhteydessä. Kiistämättömyydellä tarkoitetaan sitä, että tietojärjestelmää käyttävä henkilö tunnistetaan ja hänestä tallennetaan tietoja luvattoman käytön ehkäisemiseksi ja tiedon alkuperän varmistamiseksi. Käsitteellä viitataan palveluun, joka todistaa tietojen alkuperän ja eheyden. Esimerkiksi digitaalista allekirjoitusta käytetään kiistämättömyyteen tähtäävänä pakotteena. Viidestä elementistä koostuva malli on riskiperusteinen eikä tavoiteperusteinen, kuten perinteinen kolmesta elementistä koostuva CIA-malli (Raggad, 2010).

Näiden mallien väliin asettuu Dhillonin & Backhousen (2000) tutkimuksessa esittelemä neljästä elementistä koostuva RITE-malli (engl. *responsibility, integrity, trust, ethicality)*. RITE-malli perustuu erityisesti työntekijöiden ja työyhteisön sisäiseen toimintaan ja ratkaisuihin, eikä se ota varsinaisesti kantaa tekniseen näkökulmaan tietoturvariskien ehkäisemisessä. Vastuullisuudella tarkoitetaan organisaation jäsenten kykyä ymmärtää oma roolinsa ja merkityksensä organisaation turvallisuuden kannalta sekä kykyä kantaa vastuu oman toiminnan turvallisuudesta ja kehittämisestä. Eheydellä tarkoitetaan tässä yhteydessä henkilön rehellisyyttä tai lojaalisuutta organisaatiolle ja kykyä käsitellä sensitiivistä tietoa niin, ettei tieto vuoda ulkopuolisille. Luottamuksella tarkoitetaan organisaation henkilöstön kykyä toimia ilman ulkoista valvontaa organisaation etua edistävällä tavalla. Eettisyydellä tarkoitetaan oletusta, jonka mukaan muut organisaation tai muun yhteisön jäsenet toimivat tiettyjen epävirallisten eettisten sääntöjen mukaan (Dhillon & Backhouse, 2000). Tietoturvallisuus voidaan ymmärtää erilaisten sitä tukevien tavoitteiden lisäksi myös olotilana, jossa tietoturvariskit ovat hallinnassa (Turvallisuuskomitea, 2018).

CIA-mallista on muitakin versioita, joissa siinä tunnistettuja puutteita pyritään täyttämään. Whitman ja Mattord (2009) ymmärtävät tietoturvallisuuden suojattavan tiedon ominaisuuksien kautta. He listaavat seuraavien ominaisuuksien olevan oleellisia ja tavoiteltavia suojattavalle tiedolle:

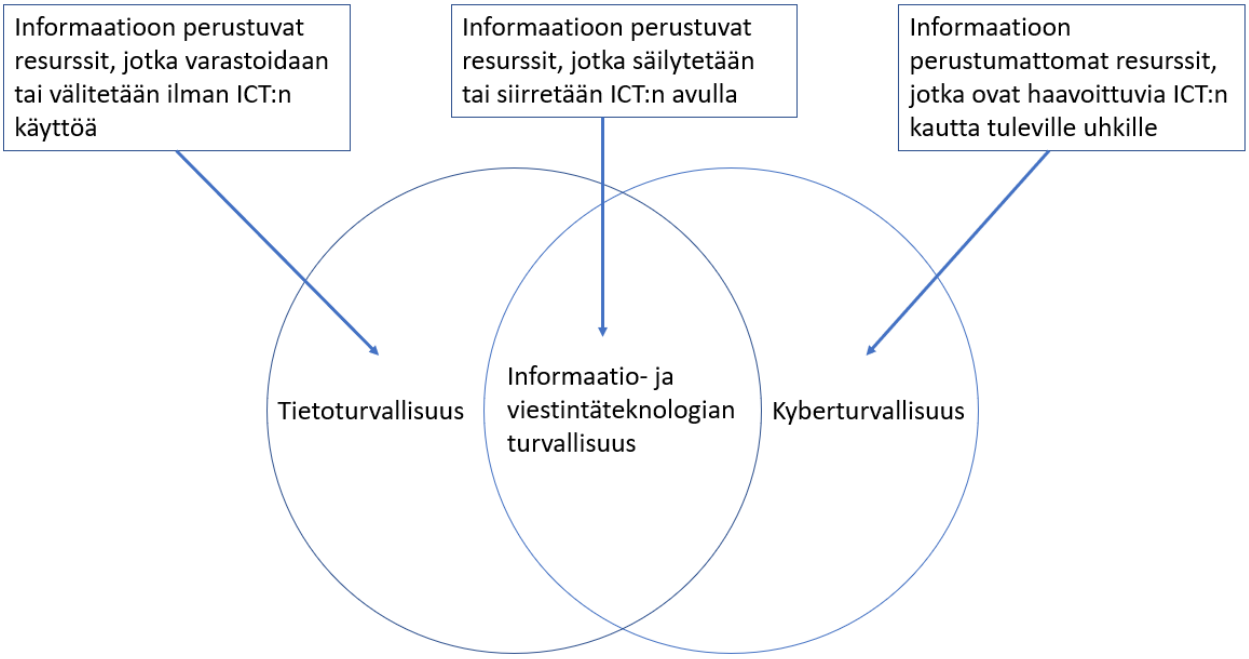
1. Tarkkuus (engl. accuracy): Informaatio on tarkkaa, kun se on virheetöntä ja sillä on käyttäjän odottama arvo tai sisältö.
2. Autenttisuus (engl. authencity): Informaation laadukkuuden tila, jossa informaatio on tilaltaan ja sisällöltään sama kuin luomishetkellä. Esimerkki autenttisuuden rikkomisesta ovat esimerkiksi kalasteluviestit.
3. Hyöty (engl. utility): Informaatiolla on arvo tai se on arvokasta silloin, kun se palvelee jotain tarkoitusta. Informaation tulee olla käyttäjälle mielekkäässä formaatissa.
4. Omistaminen (engl. possession): Informaation tila, kun se on jonkun yksittäisen osapuolen hallussa. Esimerkiksi kryptatun tiedon varastaminen loukkaa omistamista, muttei luottamuksellisuutta, sillä tietoa ei saada käytettäväksi ilman salauksenpurkua tiedon alkuperäisessä säilytysympäristössä.

Kyberturvallisuudella tarkoitetaan Turvallisuuskomitean (2018) mukaan digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Samalla kyberturvallisuuden todetaan olevan tavoitetila, jossa kybertoimintaympäristöön (yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö) voidaan luottaa ja jossa sen toiminta on turvattu (Turvallisuuskomitea, 2018).

Myös Committee on National Security Systems (2015) käsittää kyberturvallisuuden erilaisten sähköisten järjestelmien turvallisuudeksi määrittelemällä kyberturvallisuuden tietokoneiden, sähköisten kommunikaatiojärjestelmien ja -

palveluiden sekä niihin sisältyvien tietojen saatavuuden, eheyden, luottamuksellisuuden, autentikoinnin ja kiistämättömyyden turvaaviksi toimiksi.

Aiempien määritelmien perusteella voidaan huomata, että tieto- ja kyberturvallisuudella on selkeitä yhtymäkohtia, mutta ne eivät tarkoita täysin samaa asiaa. Kyberturvallisuus määritteenä sisältää samoja elementtejä kuin tietoturvallisuus, mutta kyberturvallisuus sisältää myös laajan toimijoiden verkoston (organisaatiot, yksittäiset käyttäjät) tekemät ratkaisut ja toiminnan. Von Solms & van Nierkerk (2013) toteavat kyberturvallisuuden ulottuvan tietoturvallisuuden sisältämien asioiden ulkopuolelle. Lisäksi todetaan informaatio- ja viestintäteknologian turvallisuuden muodostuvan tieto- ja kyberturvallisuudesta. Kuvio 1 havainnollistaa tieto- ja kyberturvallisuuden välistä suhdetta (kuvio 1).



Kuvio 1 Informaatio - ja viestintäteknologian turvallisuuden, tietoturvallisuuden ja kyberturvallisuuden suhde (Von Solms & van Nierkerk, 2013 mukaan)

Tietoturvallisuus käsittää suojattavat tietoresurssit, jotka eivät ole digitaalisessa muodossa. Käsitteiden leikkauskohta sisältää digitaalisessa muodossa olevan tiedon, jota pyritään suojaamaan tieto– ja kyberturvallisuudessa. Kyberturvallisuuteen kuuluvat informaatioon perustumattomat resurssit, jotka ovat haavoittuvia ICT:n kautta tuleville uhkille. Esimerkiksi terveydenhuollon käyttämiin informaatiojärjestelmiin voi kohdistua haittaohjelma, joka pysäyttää terveydenhuollon normaalit toiminnot. Tällöin yksilön ja yhteiskunnan hyvinvointi ovat vaarantuneet (Von Solms & van Nierkerk, 2013).

2.1.1 Organisaation ja johtamisen rooli tietoturvallisuuden edistämisessä

Von Solms & Von Solms (2004) tunnistavat kymmenen tyypillistä virhettä tietoturvallisuuden johtamisessa:

1. Organisaation johto ei ymmärrä, että tietoturvallisuus on heidän vastuullaan.
2. Ei ymmärretä, että tietoturvallisuus on liiketoimintaongelma eikä pelkästään tekninen ongelma.
3. Ei ymmärretä, että tietoturvallisuuden johtaminen on moniulotteinen kokonaisuus, johon ei ole valmista ratkaisua.
4. Ei ymmärretä, että tietoturvallisuussuunnitelma tulee perustua tunnistettuihin riskeihin.
5. Ei tiedetä tai ei hyödynnetä kansainvälisesti määritettyjen parhaiden käytäntöjen merkitystä tietoturvallisuuden johtamisessa.
6. Ei ymmärretä organisaation tietoturvapolitiikan olennaisuutta.
7. Ei ymmärretä, että tietoturvallisuuden noudattamisen valvonta ja seuranta ovat välttämättömiä.
8. Ei ymmärretä kunnollisen tietoturvallisuuden johtamisen rakenteen tärkeyttä.
9. Ei ymmärretä käyttäjien tietoturvallisuustietoisuuden keskeistä merkitystä.
10. Tietoturvajohtajia ei tueta infrastruktuurilla, työkaluilla tai muilla tukevilla mekanismeilla, jotta he voisivat suorittaa tehtävänsä tehokkaasti.

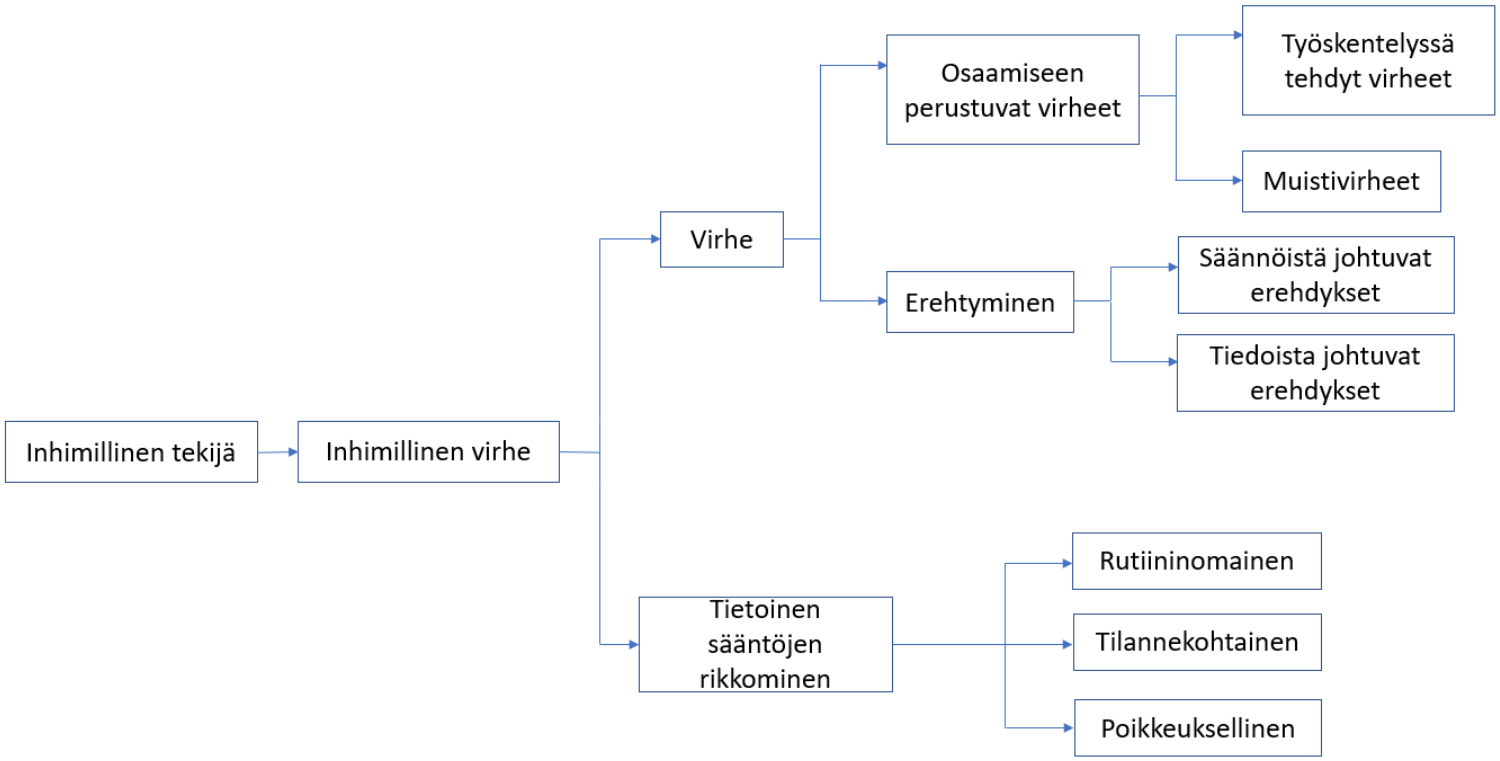
On hyvä huomata, että kaikki edellä mainitut seikat vaikeuttavat tehokasta tietoturvallisuustoimenpiteiden jalkauttamista osaksi organisaation normaalia toimintaa, mikä on itsessään yksi merkittävä ongelma riskienhallinnan osalta. Tietoturvallisuustoimenpiteistä ei saada hyötyä organisaatiolle, mikäli se jää elämään pelkkänä tehtynä dokumenttina eikä osana päivittäisiä rutiineja. Merete Hagen, Albrechtsen & Hovden (2008) toteavat, että yksi tehokkaimmista keinoista lisätä organisaation tietoturvallisuutta on lisätä henkilöstön tietoisuutta asiasta. Heidän mukaansa tietoisuuden lisääminen kuitenkin kuuluu organisaatioiden vähiten toteutettuihin toimenpiteisiin. Vastaavasti teknis-hallinnolliset toimenpiteet (tietoturvapolitiikka, valvonta) ovat käytetyimpiä toimenpiteitä organisaation tietoturvallisuuden lisäämiseksi, mutta niiden tehokkuus on huomattavasti alhaisempi verrattuna tietoturvatietoisuuden lisäämiseen. Näin ollen voidaan sanoa, että tietoturvatoimenpiteiden toteuttamisen ja niiden tehokkuuden arvioinnin välillä vallitsee käänteinen suhde (Merete Hagen ym., 2008).

Organisaation henkilöstön tietoisuuden lisääminen tietoturvallisuuden kannalta on oleellista myös siksi, että suurin osa tietoturvarikkomuksista johtuu inhimillisistä virheistä. Kraemer, Carayon & Clem (2009) tunnistivat tutkimuksessaan useita inhimillisiä ja organisatorisia tekijöitä, joilla on yhteys teknisten laitteiden ja tietoturvallisuuden haavoittuvuuksiin. Tunnistetut tekijät luokiteltiin yhdeksään eri kategoriaan:

- ulkoiset vaikutukset (engl. external influences)
- inhimilliset virheet (engl. human error)
- johtaminen (engl. management)

- laitteista ja tietoturvasta vastaava organisaatio (engl. organization of CIS, Computer and Information Security)
- suorituskykyjen hallinta (engl. performance management)
- politiikka (engl. policy)
- resurssien hallinta (engl. resource management)
- teknologia (engl. technology)
- harjoittelu (engl. training)

Inhimilliset virheet voidaan jaotella edelleen kategorioihin, jotka määrittävät virheen aiheutumisen syyt ja virheeseen vaikuttaneet asiat. Hughes & Ferret (2007) jakavat virheet tai erehdykset tahallisiin ja tahottomiin (kuvio 2). Tahalliset virheet perustuvat tietoiseen sääntöjen vastaiseen toimintaan, jonka juurisyynä voi toimia rutiini, jolloin sääntöjen rikkominen normaali tapa toimia organisaatiossa. Myös tilannesidonnaisuus nähdään tietoisena sääntöjen rikkomisen tekijänä, esimerkiksi työn kiireellisyys pakottaa rikkomaan sääntöjä tavoitteisiin



Kuvio 2 Inhimillisten virheiden kategorisointi (Hughes & Ferret, 2007 mukaan)

pääsemiseksi. Poikkeustilanne vaikuttaa myös tietoisiin rikkomuksiin, tyypillisesti sääntöjen vastainen toiminta ilmenee hätätilanteissa tai käytettäessä uusia toimintatapoja työn suorittamiseen (Hughes & Ferret, 2007).

2.1.2 Tieto– ja kyberturvallisuuden riskienhallinnan malleja ja työkaluja

Tieto- ja kyberturvallisuuden riskienhallintaan on olemassa useita eri malleja ja standardeja, joita voidaan käyttää apuna tietoturvariskien tunnistamisessa. Tunnetuimpia malleja on ISO/IEC 27001-standardi, joka sisältää ohjeistuksen tietoturvallisuuden hallintajärjestelmästä. Tavoitteena on rakentaa johtamisjärjestelmä, jolla suojataan organisaation tieto-omaisuus ja kyberympäristö. Standardi pyrkii ohjeistamaan organisaatiota ennakoimaan riskejä ja varautumaan niihin tehokkailla prosesseilla. Standardin mukaan tietoturvallisuuden hallintajärjestelmä suunnitellaan, toteutetaan, arvioidaan sekä viimeiseksi kehitetään ja ylläpidetään. Järjestelmän elinkaari tekee jatkuvaa kiertoa, jolla pyritään hallintajärjestelmän ajantasaisuuteen (ISO 27001, 2013).

Samaan standardiperheeseen täydennystä tuo ISO/IEC 27005-standardi, joka sisältää ohjeita tietoturvallisuuden riskienhallintaan. Standardi sisältää mm. tietoturvariskien hallintaprosessin ja siihen sisältyvien toimintojen kuvauksen. ISO/IEC 27005 tarkoituksena on tukea tietoturvallisuuden jalkauttamista osaksi organisaation toimintaan (ISO 27005, 2018). ISO/IEC 27005 listaa useita mahdollisia uhkia ja niistä aiheutuvia seurauksia. Kyseistä liitettä käytetään apuna myöhemmin kartoitettaessa tietoturvariski-indikaattoreita projekteista. ISO/IEC-standardit määrittävät toimeenpantavat turvallisuuskontrollit, mutta ne eivät ota kantaa siihen, miten turvallisuuskontrollit käytännössä toteutetaan.

Tietoturvallisuuden riskienhallinnan mallit eivät sisällä mainintaa riski-indikaattoreiden käyttämisestä, mutta menetelmänä indikaattoreita on mahdollista käyttää osana tietoturvallisuuden riskienhallintaa. Riskienhallinnan malleista ainoastaan COBIT 5-viitekehys sisältää maininnan riski-indikaattoreiden hyödyntämisestä osana tietoturvallisuuden riskienhallinnan prosessia. Prosessissa indikaattoreita pyritään hyödyntämään skenaariopohjaisen riskienhallinnan metodeilla. Al-Ahmad ja Mohammed (2015) avaavat artikkelissaan COBIT 5:n sisältämän riskienhallintaprosessin vaiheita tarkemmin, mukaan lukien riski-indikaattoreiden muodostamisen. Artikkelissa kehotetaan hyödyntämään aikaisemmin muodostettua tietoturvariskiprofiilia ja tunnistamaan siitä riskitrendejä. Näiden tietojen perusteella muodostetaan mittarit ja hälytysrajat riskeille, jotka vaativat tietoturvariskienhallinnan huomiota. Samalla tulee määrittää raportointikäytännöt riski-indikaattoreiden ja poikkeamien havainnointiin, jaksottaiset tarkastusajankohdat ja tarvittavien päivitysten tekeminen riski-indikaattoreille. Kaikki määriteltyjen indikaattoreiden tulee olla riskeistä vastaavan henkilön hyväksymiä (Al-Ahmad & Mohammed, 2015).

Aikaisempaa tutkimusta indikaattorien hyödyntämisestä löytyy sangen rajallisesti. Luvussa 2.5 viitataan Salujan ja Idrisin (2014) tekemän tutkimuksen lisäksi Özçakmakiin (2019), joka tutki tietoturvallisuuden malleja ja niiden yhtäläisyyksiä avainriskien indikaattoreihin. Tutkimuksessaan hän loi mallin ISO/IEC 27001-standardin riskienhallintaprosessin pohjalta, johon on liitetty mukaan tietoturvariskeistä kertovien indikaattoreiden muodostaminen ja hyödyntäminen tietoturvariskienhallinnassa. Tutkimuksessa todettiin, että riski-in-

dikaattorien jalkauttaminen osaksi tietoturvariskienhallinnan standardeja on toteutettavissa kohtuullisen helposti. Tutkimuskohteena olevan organisaation palautteen perusteella resurssien kohdentaminen muuttui tehokkaammaksi sekä riskien tunnistaminen ja havainnointi parantui (Özçakmak, 2019).

Sabău-Popa, Bradea, Boloş & Delcea (2015) ovat tutkineet tietoturvallisuuden indikaattorien toimivuutta terveydenhuollon puolella, jossa sairaalan tavoitteena oli ottaa käyttöön tietoturvaloukkauksista varoittava järjestelmä. Tutkimuksessa analysoitiin luotujen indikaattoreiden perusteella sairaalaan kohdistuvaa riskiä tiedon luottamuksellisuuden ja kyberturvallisuusriskien osalta. Indikaattoreita seurattiin vuosina 2011–2013 ja indikaattorien arvojen kehitystä seurattiin vuosittain. Tutkimuksessa todettiin kyseisen sairaalan olevan altistunut tietoturvaloukkauksille ja sairaalalle esitettiin suosituksia tietoturvallisuuden parantamiseen (Sabău-Popa ym. 2015).

2.2 Riski

Riskillä voidaan tarkoittaa negatiivisesti tai positiivisesti projektin tai hankkeen lopputulokseen vaikuttavaa tekijää. Riskin mielletään tyypillisesti koostuvan todennäköisyydestä ja vaikutuksesta, joista saadaan riskin vakavuus (Project Management Institute, 2008). Positiivinen riski voidaan ymmärtää mahdollisuudeksi, joka pystyy auttamaan organisaation toimintaa. Tässä tutkimuksessa keskitytään pelkkiin negatiivisiin riskeihin ja niistä aiheutuviin vaikutuksiin.

Myös Bannermanin (2008) mukaan riski voidaan esittää koostuvan kahdesta oleellisesta tekijästä, todennäköisyydestä ja vaikutuksesta. Todennäköisyys määrittää, kuinka suuri mahdollisuus riskin esiintymiselle on ja vaikutus määrittää riskin eskaloitumisesta seuraavat muutokset. Näin ollen riski voidaan esittää seuraavana yksinkertaisena matemaattisena kaavana: $\mathbf{R} = \mathbf{P} \times \mathbf{I}$, missä R tarkoittaa riskiä, P on riskin todennäköisyys ja I riskin vaikutusta sen realisoituessa. Riskin vaikutus määritellään usein esimerkiksi siitä aiheutuvien taloudellisten menetysten perusteella, siihen kuluneena aikana tai riskin vaikutuksen laajuutena (Bannerman, 2008).

ISO (International Organization of Standardization, 2018) määrittelee riskin haluttuun tavoitteeseen vaikuttavaksi epävarmuustekijäksi. Riskiä käsitellään tyypillisesti sen aiheuttamien seurauksien ja sen esiintymisen todennäköisyyden perusteella tai edellisten yhdistelmänä (ISO Guide, 2018).

Edellä mainittu tapa käsitellä riskiä määrällisesti on tyypillinen tapa riskien määrittelyssä. Ohessa esitelty yksinkertainen matemaattinen malli on laajalti käytetty erilaisissa riskityökaluissa. Coxin (2008) mukaan kyseiseen malliin perustuvat riskimatriisit eivät ole luotettavia ja niitä tulisi käyttää varoen vain silloin, kun riskit on selitetty huolellisesti useiden riskiarvioiden yhteenvetona. Cox (2008) luokittelee seuraavia rajoitteita riskimatriiseihin liittyen:

1. Heikko resoluutio: Tyypillinen riskimatriisi kykenee vertailemaan luotettavasti ja yksiselitteisesti vain alle kymmenesosaa tunnistetuista uhkapareista. Matriisit voivat antaa samanlaiset luokitukset määrällisesti hyvin erilaisille riskeille.
2. Virheet: Riskimatriisit voivat virheellisesti antaa korkeamman laadullisen luokituksen riskille, joka on määrällisesti pienempi. Erityisesti sellaisten riskien osalta, joiden esiintyvyys ja vaikutus korreloivat negatiivisesti, riskimatriisi voi antaa jopa huonompia tuloksia kuin täysin satunnaisesti tehty analyysi.
3. Mahdollisimman optimaalisen resurssien kohdentaminen: Resurssien tehokas kohdentaminen riskiä vähentäviin toimenpiteisiin ei voi perustua riskimatriisissa määritettyihin kategorioihin.
4. Monitulkintaiset lähtötiedot ja tulokset: Riskin vakavuusluokituksia ei voida tehdä objektiivisesti epävarmojen seurausten vuoksi. Riskimatriiseihin annetut lähtöarvot (todennäköisyys ja vaikutus) ja näiden perusteella tuotettu riskin vakavuus vaativat subjektiivista tulkintaa, minkä vuoksi eri henkilöt voivat saada vastakkaisia luokituksia samoista määrällisistä riskeistä.

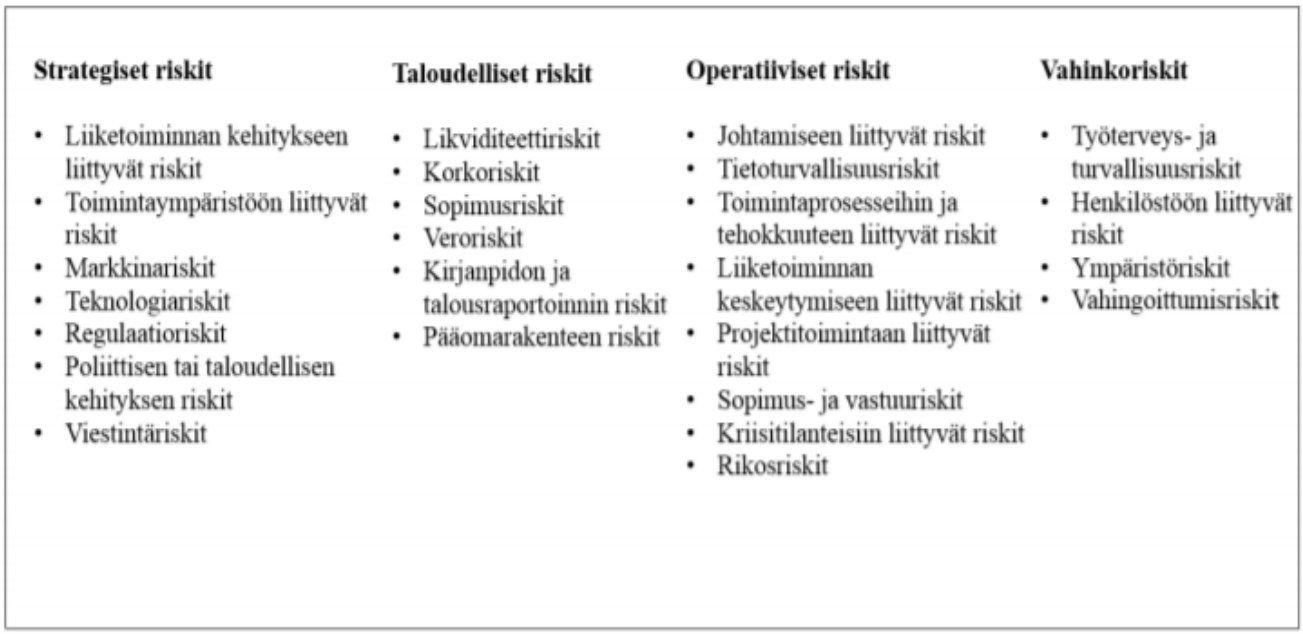
Myös tietoturvariski voidaan määritellä erikseen, vaikka määritelmä sisältääkin paljon samoja elementtejä aiemmista määritelmistä. Sanastokeskuksen (2004) mukaan tietoturvariski voidaan ymmärtää tietoturvauhan toteutumisen todennäköisyydeksi ja siitä aiheutuvan haitan suuruudeksi. Tietoturvauhat jaetaan sisäisiin ja ulkoisiin. Sisäisiin uhkiin luetaan organisaation työntekijöiden toiminta ja ulkoisiin organisaation ulkopuolelta tulevat uhat, kuten haittaohjelmat ja kalasteluyritykset. Tietoturvariskien suuruus määritetään siitä aiheutuvan haitan ja riskin realisoitumisen todennäköisyyden perusteella. (Sanastokeskus, 2004)

Valtiovarainministeriö (2008) määrittelee tietoturvasanastossaan tietoturvariskin tietoon, tietoliikenteeseen tai tietojärjestelmään kohdistuvana vahingon vaarana, mutta se ei ota erikseen kantaa sisäisiin tai ulkoisiin riskeihin. Valtiovarainministeriön määritelmä nivoutuu selkeämmin tiedonkäsittelyn sähköiseen ympäristöön liittyviin riskeihin.

NIST (National Institute of Standards and Technology, 2011) määrittelee tietoturvariskin edellisestä poiketen riskiksi organisaation toiminnoille (tehtävät, toiminnot, imago, maine). Lisäksi riski on uhka omaisuudelle, yksilöille, muille organisaatioille tai kansakunnalle, sillä tietoja tai tietojärjestelmiä voidaan käyttää luvattomasti, paljastaa, muokata tai tuhota. Straub & Welke (1998) tulkitsevat järjestelmäriskin hyvin vastaavalla tavalla, mutta määritelmässä riski on epävarmuustekijä käytettäessä tietokonepohjaisia järjestelmiä tiedon toimittamiseen.

Suominen (2003) luokittelee teoksessaan myös tietoriskin käsitteen. Tietoriskillä tarkoitetaan tietoihin ja niiden käyttöön kohdistuvien tapahtumien uhkaa. todetaan tietoriskien johtuvan riippuvuudesta tietojärjestelmiin ja niistä saataviin palveluihin. Lisäksi julkisten ja yksityisten verkkojen yhdistämisen, hajautetun tiedonkäsittelyn yleistymisen ja palveluiden ulkoistamisen todetaan heikentäneen organisaatioiden mahdollisuuksia valvoa tehokkaasti omaa tietoturvallisuuttaan (Suominen, 2003).

Riskit voidaan luokitella Ilmosen, Kallion, Kosken & Rajamäen (2013) mukaan erilaisiin kategorioihin, jotka ovat strategiset, taloudelliset, operatiiviset ja vahinkoriskit. Jokaisella riskikategorialla riski voi olla joko ulkoinen tai sisäinen. Ulkoinen riski voi olla esimerkiksi asiakkaasta tai lainsäädännöstä johtuva riski, sisäinen riski voi liittyä organisaation omiin valintoihin strategian tai liiketoimintojen suhteen (kuvio 3).



Kuvio 3 Riskien kategorisointi (Ilmonen ym. 2013 mukaan)

Ulkoisiin riskeihin varautuminen on haastavampaa kuin sisäisiin riskeihin, sillä ne ovat usein organisaatiosta riippumattomia. Vaikka organisaatio ei voi vaikuttaa ulkoisen riskin syntymiseen, siihen voidaan varautua samoja keinoja käyttäen kuin sisäisiin riskeihin varautumiseen. Sisäisiin riskeihin organisaation on helpompi vaikuttaa, sillä organisaatiolla on usein dokumentaatiota sisäisistä riskeistä, jolloin niihin voidaan vaikuttaa esimerkiksi henkilöstön perehdyttämisellä ja kouluttamisella. Riskidokumentaatiota päivitetään sitä mukaa, kun uusia riskejä havaitaan ja sitä myötä organisaation kyky varautua sisäisiin riskeihin hiljalleen paranee.

Kuviosta voidaan havaita tietoturvallisuusriskien kuuluvan operatiivisten riskien kategoriaan. Ilmonen, Kallio, Koski & Rajamäki (2013) toteavat operatiivisten riskien liittyvän organisaation sisäisiin prosesseihin, työntekijöihin, järjestelmiin sekä ulkoisiin tapahtumiin, joista voi seurata välittömiä tai välillisiä vahinkoja. Operatiivisilla riskeillä on myös yhteys strategisen tason riskeihin. Operatiivisella tasolla huomioidaan informaatioteknologiaan ja tietoturvallisuuteen liittyvät riskit. Esimerkkejä riskeistä ovat järjestelmien väliset integraatiot, huonosti organisaation toimintaan soveltuvat järjestelmät tai järjestelmien heikko muunneltavuus tarpeiden muuttuessa (Ilmonen ym. 2013).

2.3 Riskienhallinta

Riskienhallinta käsitteenä ei ole yksiselitteinen, johtuen riskien moninaisuudesta, organisaation toimintaympäristöstä tai riskejä käsittelevien osapuolien taustoista. Riskienhallinta on oleellista organisaatioiden toiminnalle, sillä onnistuessaan se parantaa organisaation toimintaa ja kilpailukykyä, kun taas riskienhallinnan epäonnistuessa seurauksena voi olla pahimmillaan organisaation toiminnan loppuminen realisoituneiden haittojen vuoksi.

Riskienhallinta voidaan käsittää projektin tai hankkeen johdon määrittäminä toimenpiteinä, jotka estävät riskejä toteutumasta tai pienentävät riskin merkittävyyttä (Wallace & Keil, 2004). Toisaalta riskienhallinta voidaan esittää myös siihen kuuluvina vaiheina. Tällöin riskienhallinnan voidaan sanoa olevan riskien tunnistamista, analysointia ja kontrolloimista (Thun & Hoenig, 2011). Kansainvälinen riskienhallinnan standardi ISO/IEC 31000 ymmärtää riskienhallinnan samankaltaisesti kuvatessaan riskienhallintaa organisaation toimiksi, joilla voidaan tehokkaasti tunnistaa, arvioida ja käsitellä riskien vaikutusta organisaation tavoitteiden saavuttamiseen (SFS, ISO 31000:2018).

Malménin ja Wessbergin (2004) käsitys riskienhallinnasta yhdistelee edellä mainittuja piirteitä kokonaisvaltaisemmin. Heidän mukaansa riskienhallinta on työtä, jolla turvataan organisaation toiminnan jatkuvuus, henkilöstön hyvinvointi ja ympäristön kestävä käyttö. Riskienhallinta pitää sisällään kaikki toimet yritystä kohtaavien vaarojen ja ongelmien tai näihin liittyvien riskien sekä aiheutuvien vahinkojen välttämiseksi ja pienentämiseksi. Riskienhallinnassa korostetaan sen suunnitelmallista ja järjestelmällistä toteuttamista (Malmén & Wessberg, 2004).

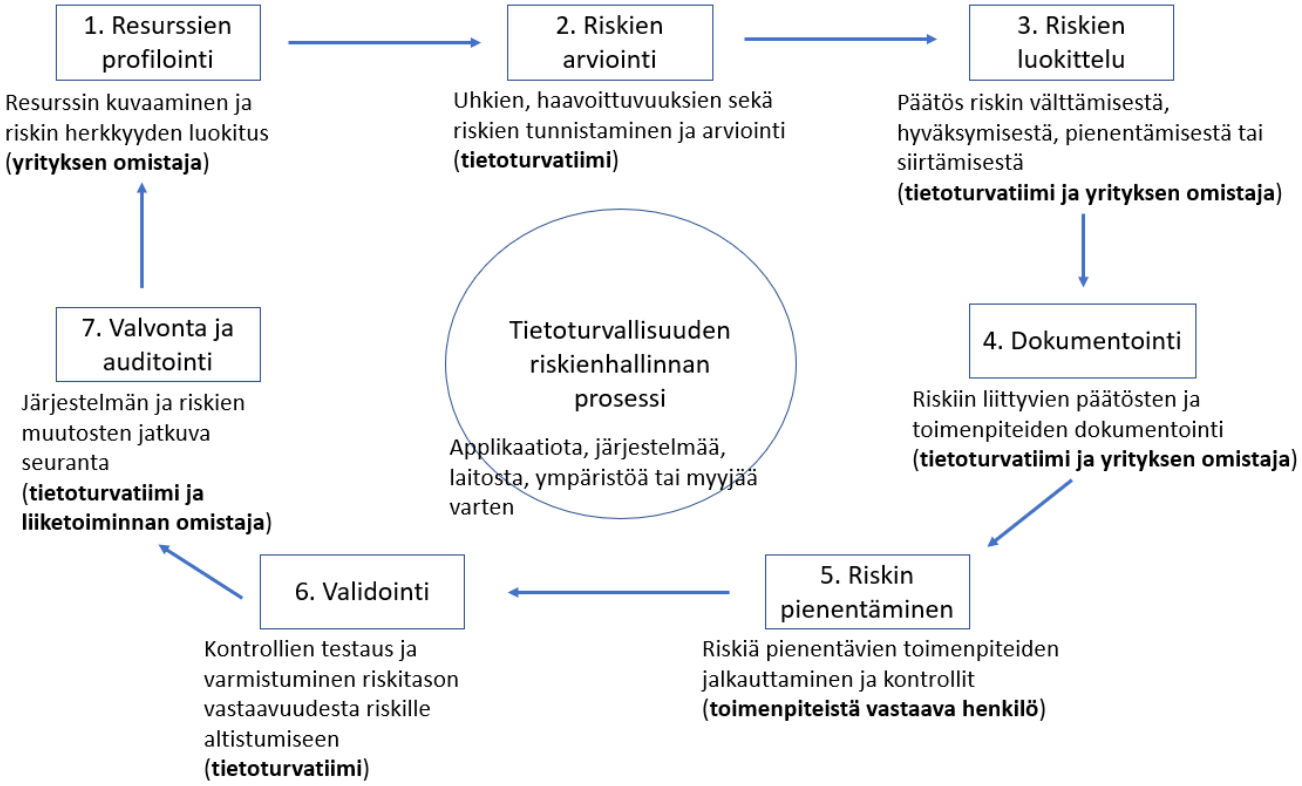
Berg (2010) esittää riskienhallinnalle kaksi erilaista periaatetta, jotka ovat seurauksiin perustuva hallinta ja riskeihin perustuva hallinta. Seurauksiin perustuvassa toimintamallissa pahin odotettavissa oleva tapahtuma pyritään rajaamaan erikseen määritetyillä turvallisuustoimilla niin, ettei tapahtumalla ole vaikutuksia tiettyjen rajojen ulkopuolelle. Riskeihin perustuvassa hallinnassa analysoidaan jäännösriskin suuruus riskin todennäköisyyden ja vaikuttavuuden suhteen, minkä jälkeen saadaan tietoa riskin merkittävyydestä ja voidaan tehdä päätös riskiin kohdennettavista jatkotoimenpiteistä. Tässä tapauksessa esimerkiksi epätodennäköisiä tapahtumia voidaan päättää sietää. Jälkimmäisenä esiteltyä tapaa pidetään perinteisenä riskienhallintana, kun taas ensimmäinen tapa vastaa enemmän eskaloituneisiin riskeihin reagointia (Berg, 2010).

Tietoturvariskien eskaloitumiseen ei välttämättä vaikuta järjestelmässä oleva tekninen haavoittuvuus, vaan useammin on kyse järjestelmän käyttäjän tekemästä virheestä. Käyttäjän huomioiminen on yksi oleellinen asia tietoturvallisuuden suunnittelussa, jossa saatetaan keskittyä liikaa itse järjestelmään ja siinä käytettyjen teknisten ratkaisujen mahdollistamiin riskeihin. Spears ja Barki (2010) tukevat tätä väitettä toteamalla, että käyttäjien mukaan ottaminen tietoturvan riskienhallintaan parantaa tietoturvaa lisäämällä käyttäjien tietoturvatietoisuutta.

Vaikka järjestelmän käyttäjä tai inhimilliset virheet voivat jäädä liian vähälle huomiolle riskienhallinnassa teknisten riskien painottamisen vuoksi, ei teknisiäkään riskejä voi jättää huomioimatta. Tietoturvallisuuden osalta riskien hallinnassa voidaan käyttää Venterin & Eloffin (2003) mukaan useita erilaisia teknologisia ratkaisuja riskien realisoitumisen välttämiseksi. Kyseisiä teknisiä ratkaisuja voivat olla esimerkiksi haittaohjelmaskannerit, pääsynvalvonta ja järjestelmään tunkeutumisen havainnointijärjestelmät. Tekniset ratkaisut mahdollistavat riskitilanteen seurannan ja tarvittaessa nopean reagoinnin realisoituvaa riskiä vastaan (Venter ym., 2003).

Salmela (2007) toteaa tietoturvariskin realisoitumisen yhdeksi tyypillisistä liiketappioon johtavista syistä. Tietoturvariskin realisoituminen voi aiheuttaa organisaatiolle mainehaittoja, menetettyä työaikaa ja sitä myötä menetettyjä tuloja tai luottamuksellisen tiedon vuotamisen ulkopuolisille tahoille (Salmela, 2007).

Riskienhallintaprosesseista on olemassa lukuisia erilaisia malleja eri käyttöympäristöihin, mutta prosessista riippumatta prosessin vaiheet ovat hyvin lähellä toisiaan. Wheeler (2011) esittää yhden version tietoturvallisuuden riskienhallintaprosessista. Prosessikaaviossa on esitetty riskienhallinnan vaiheet sekä kustakin vaiheesta vastuussa olevat toimijat (kuvio 4).



Kuvio 4 Tietoturvallisuuden riskienhallinnan vaiheet (Wheeler, 2011 mukaan)

ISO/IEC 27005-standardissa (2018) todetaan, että riskejä voidaan arvioida laadullisesti tai määrällisesti. Laadullinen riskianalyysi kuvailee riskin todennäköisyyttä ja vaikutusta laatumäärittelyillä (esim. pieni, keskitasoinen, suuri). Laa-

dullinen analyysi soveltuu erityisesti riskien alustavaan tunnistamiseen tai mikäli riskien analysointiin ei ole riittävästi numeerista dataa käytettävissä. Tällöin korostuu tosiasioihin pohjautuvien aineistojen ja tietojen käyttö. Laadullinen analyysi on helposti ymmärrettävä, mutta analyysiin laatuun voi vaikuttaa analyysituloksen subjektiivisuus riippuen käytettävän asteikon valinnasta (ISO/IEC 27005, 2018).

Määrällisestä riskianalyysistä ISO/IEC 27005-standardi (2018) toteaa, että määrällisessä analyysissä käytetään tyypillisesti numeroarvoja kuvaamaan riskien todennäköisyyksiä ja vaikutuksia. Saatujen arvojen tulisi perustua laajaan aineistoon, jonka tulisi olla myös sisällöltään luotettavaa. Menetelmä perustuu pitkälti aiemmista häiriöistä kerättyyn tietoon, jolloin tieto voidaan kytkeä organisaation määrittämiin tietoturvatavoitteisiin tai muihin organisaation ongelmakohtiin. Kyseistä aineistoa ei ole kuitenkaan saatavilla uusien riskien tai tietoturvahaavoittuvuuksien tapauksessa, sillä riskit vaihtelevat nopeasti. Määrällinen analyysi vaatii laajan tietoaineiston ollakseen luotettava analyysityökalu (ISO/IEC 27005, 2018). Mikäli analyysin tietoaineistossa on puutteita tai sitä ei ole, riskiarvio perustuu käytännössä yksittäisen henkilön näkemykseen riskin vakavuudesta ja riskiarvion luotettavuus kärsii.

Edellä mainittujen analyysimenetelmien lisäksi NIST (2012) esittelee puolikvantitatiivisen riskianalyysin (engl. semi-quantitative assessment), joka yhdistelee määrällistä ja laadullista analyysia. Menetelmässä hyödynnetään metodeja ja sääntöjä riskien hallintaan, kuten myös numeerisia arvoja luokittelemaan tai sijoittamaan riskejä asteikolle. Luokat (esim. 0–15, 16–35, 36–70, 71–85, 86–100) tai asteikot (esim. 1-10) pystytään kääntämään laadullisiksi termeiksi, esimerkiksi voidaan sanoa luokituksen 95 saaneen riskin olevan erittäin korkea. Samalla voidaan vertailla riskejä luokkien sisällä tai luokkien välillä. Asiantuntijoiden rooli arvojen määrittämisessä on merkittävämpi verrattuna määrälliseen riskianalyysiin. Jos asteikot tai luokat kykenevät tarjoamaan riittävän rakeisuuden, tulosten suhteellista priorisointia tuetaan paremmin kuin laadullisessa arvioinnissa. Analyysin täsmällisyys kärsii, kun subjektiiviset mielipiteet ovat osa arviota tai kun arvojen määrittäminen on epävarmaa. Oleellista on, että jokainen luokka ja käytettävät asteikot on määritelty selkeästi ja tarkoituksenmukaisesti (NIST, 2012).

Laadulliseen tietoturvariskien arviointiin perustuvat mallit ovat Harrisin (2013) mukaan usein vähän testattuja ja niistä saatavat tulokset perustuvat liikaa subjektiivisuuteen ja mielipiteisiin. Riskien arviointiin voi liittyä jopa arvailua. Laadullisiin malleihin liittyvä käytön yhdenmukaisuuden puute saa aikaan sen, että laadullisiin riskienhallintaprosesseihin ja sitä myötä saataviin tuloksiin tulee isoa vaihtelua käyttöympäristön mukaan. Määrällinen riskinarviointi on erittäin työläs prosessi, mikäli käytössä ei ole automatisoituja työkaluja. Määrällisen riskinarvioinnin tulokset voivat olla monimutkaisia ja vaikeasti ymmärrettävissä, mikä vaikuttaa riskienhallintatoimenpiteisiin. Määrälliseen arvioon tarvitaan runsaasti etukäteisvalmisteluja ja yksityiskohtaista tietoa. Määrälliseen riskien-

arviointiin ei ole myöskään yhdenmukaista tapaa toteuttaa arviointi, jolloin prosessin toteuttamisessa on suurta tulkinnanvaraa toteuttavan tahon mukaan (Harris, 2013).

Mainitut tietoturvariskienhallinnan mallit ovat laajalti käytettyjä ja laadukkaita työkaluja tietoturvariskienhallinnassa, mutta niissä on tunnistettu merkittäviä puutteita. Fenz, Heurix, Neubauer ja Pechstein (2014) mainitsevat yleisiä tietoturvariskienhallinnan lähestymistapoihin liittyviä puutteita:

- resurssien (engl. asset) ja käytettävien vastatoimien tunnistaminen
- resurssien arvon määrittäminen (resurssit eivät ole välttämättä esimerkiksi rahallisesti mitattavia)
- riskien ennakoiminen (riskien muuntuvaisuus vaikeuttaa riskeihin varautumista merkittävästi)
- liiallisen itseluottamuksen tuoma vaikutus (riskit arvioidaan liian optimistisesti)
- tietämyksen jakaminen organisaatiossa ja sen ulkopuolella
- riskin realisoitumisen hinta vs. riskiin varautumisen hinta

Riskienhallinnan voidaan todeta olevan hyvin haastavaa ja kokonaisvaltaista työskentelyä, jossa on paljon kehitettävää. Samaan aikaan riskienhallinta on erittäin oleellinen osa organisaatioiden normaalia toimintaa. Lähtökohdat riskienhallintaprosessien kehittämiselle ovat olemassa, sillä riskienhallintaa on tutkittu laajalti ja sitä myötä riskienhallinnan puutteet ovat hyvin tiedossa.

2.4 Projektiriskienhallinta

Projekti voidaan määritellä Westlandin (2006) mukaan pyrkimykseksi tuottaa palveluita tai tuotteita selkeästi määriteltyjen aika-, kustannus- ja laaturajoituksien mukaan. Lisäksi projekteihin liittyy aina epävarmuustekijöitä ja siitä johtuvia riskejä. Projekteilla tähdätään suotuisaan liiketoiminnan muutokseen. Projektista voidaan tunnistaa tiettyjä vaiheita sen elinkaaren aikana, joita ovat *käynnistys, suunnittelu, toteutus* ja *päättäminen.* Projekti käynnistyy, kun tunnistetaan liiketoimintamahdollisuus ja sille määritetään erilaisia ratkaisuvaihtoehtoja. Vaihtoehtojen toteutettavuutta tutkitaan ja valitaan sopivin vaihtoehto. Samalla määritellään projektin laajuus ja projektipäällikkö, joka kokoaa projektitiimin. Projektin suunnitteluvaiheessa luodaan projektisuunnitelma, joka sisältää projektissa suoritettavat aktiviteetit, tarvittavat resurssit ja materiaalit, aikataulun, budjetin, riskienhallinnan ja laatuvaatimukset. Projekti suunnitellaan yksityiskohtaisesti, jotta se on valmis suoritettavaksi. Projektin toteutusvaiheessa tehty projektisuunnitelma viedään käytäntöön ja projektia lähdetään toteuttamaan suunnitelman perusteella. Projektin etenemistä seurataan eri sektoreilla ja mahdolliset muutokset pyritään tunnistamaan aikaisessa vaiheessa, jotta niihin voidaan reagoida tehokkaasti. Kun kaikki projektisuunnitelmaan sisällytetyt vaatimukset on saatu tehtyä ja asiakas on hyväksynyt tarjotun ratkaisun, siirrytään projektin

päättämiseen. Projektin päättämisvaiheessa projektiin sidotut resurssit vapautetaan ja arvioidaan projektin onnistuminen, tarvittaessa tunnistetaan projektista kehityskohteita tulevia projekteja varten (Westland, 2006).

Riskienhallinta on oleellinen osa projektityöskentelyä. Projektien luonteeseen kuuluu aina jonkun verran epätietoisuutta tai epävarmuutta tulevista tapahtumista, mikä vaikeuttaa kaikkien projektiin liittyvien asioiden huomioonottamista. Projektien ainutlaatuisuus tekee riskienhallinnan haastavaksi, jolloin on vaikeaa määrittää selkeitä yhteisiä riskejä kaikille projekteille. Arton, Kujalan, Martinsuon ja Sinivuoren (2006) mukaan projektien riskienhallintaan ei voi soveltaa objektiivista tietoa, kuten aiemmin koottua tilastotietoa tai toteutumafrekvenssejä riskeistä. Tällöin projektiriskien arviointiin käytetään subjektiivista arviointia, jonka tyypillisesti suorittaa projektityöryhmä tai projektipäällikkö. Projekteihin liittyy useita riskilähteitä, eli yleisiä riskejä aiheuttavia asioita, ilmiöitä tai tekijöitä. Artto ym. (2006) mainitsevat seuraavien asioiden olevan merkittävimpiä riskejä projekteissa:

- asiakas, käyttäjä, rahoittaja
- toimittaja, alihankkija
- uudet tekniset, toiminnalliset tai toteutustaparatkaisut
- päätöksenteko (päätöksenteon nopeus ja projektia koskevien päätösten sisältö yrityksessä), yrityksen johdon tuki projektille ja projektin käyttöönsä saamat resurssit
- viestintä, tiedonkulku, tiedon saatavuus
- muutokset suunnitelmiin
- inhimilliset tekijät, kuten optimismi arvioinnissa tai tiedon puutteesta tai muista syistä johtuva muutosvastarinta
- toisistaan riippuvien tehtävien tai projektin osien monimutkaisista riippuvuuksista johtuvat koordinointiongelmat

Projektityöskentelyssä riskejä voidaan pyrkiä tunnistamaan eri tavoin. Apuna voidaan käyttää tarkistuslistaa tai riskilistaa, johon on listattu aikaisemmista projekteista havaittuja riskejä ja huomioita. Myös projektiryhmän kesken suoritettu ideointi riskien tunnistamiseksi on tyypillinen työskentelytapa. Riskien tunnistamiseen on myös mahdollista hyödyntää erilaisia mallintamismenetelmiä tai visuaalisia kuvaamistekniikoita, kuten esimerkiksi matriisia. Riskien tunnistamiseksi voidaan myös tehdä selvityksiä ja tutkimuksia tai hyödyntää ulkopuolista konsultointia, mikäli projektiin sisältyy erityistä asiantuntemusta (Artto ym., 2006).

Riskien tunnistamisen jälkeen päätetään riskiin kohdennettavista hallintatoimenpiteistä. Tyypillisiä toimenpiteitä ovat Niemen (2018) mukaan *välttäminen*, *siirtäminen*, *hyväksyminen ja pienentäminen.* Välttämisessä organisaatio pidättäytyy riskiin liittyvästä toiminnosta tai vetäytyy käynnissä olevasta toiminnasta. Siirtämisessä riski siirretään toiselle osapuolelle sopimuskäytänteillä tai vakuutuksilla. Hyväksymällä riski ei toteuteta mitään hallintatoimenpiteitä, näin toi-

mitaan riskin ollessa vaikutukseltaan tai todennäköisyydeltään pieni tai hallintatoimenpiteiden kustannusten ollessa suuremmat kuin riskistä aiheutuvat kustannukset. Pienentämisessä riskin todennäköisyyttä tai vaikutusta pienennetään erikseen määritetyillä korjaavilla toimenpiteillä tai sisäisen valvonnan kontrolleilla (Niemi, 2018).

2.5 Riski-indikaattorit

Riski-indikaattoreita tai avainriskien indikaattoreita on käytetty yleisesti aiemmin lääketieteessä sekä finanssitoiminnan riskienhallinnassa, mutta tietoturvallisuuden riskienhallinnassa indikaattorien käyttö on ollut vähäisempää. Avainriskien indikaattorilla (engl. key risk indicator, KRI) tarkoitetaan Daviesin, Finlayn ja McLenaghenin (2006) mukaan mitattavia tai seurattavia mittareita, jotka seuraavat altistumista tai riskeistä aiheutuvia menetyksiä. Avainriskien indikaattorit ovat usein määrällisiä, mutta myös laadulliset mittarit ovat valideja. Tärkeintä on, että valittu indikaattori kykenee seuraamaan tilanteen kehitystä (Davies ym., 2006).

Antonuccin (2017) mukaan KRI voidaan määritellä myös mittariksi, jonka avulla organisaatio pyrkii seuraamaan riskitason muutoksia varmistaakseen normaalit toiminnot. KRI korostaa riskeille alttiita kohteita ja ne voivat johtaa tehokkaasti syntyvien riskien jäljille. Tyypillisesti indikaattorit ovat johdattelevia tai tulevaisuutta käsitteleviä (Antonucci, 2017).

Galvanizen (2019) julkaisussa kiteytetään KRI:n olevan apuväline riskien tunnistamiseen ja valvontaan. Avainriskien indikaattorit linkittyvät organisaatioiden operatiivisiin riskinhallintatoimiin ja prosesseihin, kuten riskien tunnistamiseen, arviointiin, valvontaan, riskinhallintakeinojen käyttöönottoon ja hallintoon. Riski-indikaattori voi olla mikä tahansa mittari, jolla voidaan tarkastella riskille altistumisen tasoa jollain ajanjaksolla. Riski-indikaattoreista tulee avainriskien indikaattoreita, kun ne seuraavat kriittiseksi määritettyä riskiä tai ne ovat erittäin tehokkaita riskien seuraamisessa (Galvanize, 2019).

Hyvällä indikaattorilla voidaan katsoa olevan seuraavia ominaisuuksia Daviesin ym. (2006) mukaan: Indikaattoreiden tulisi olla tehokkaita, jolloin indikaattorin tulisi kohdentua vähintään yhteen riskiin. Indikaattorin tulisi myös olla mitattavissa eri aikoina ja kuvata jostain näkökulmasta tapahtumaa (esim. jaksottaisuus tai vakavuus) sekä tuottaa hyödyllistä tietoa johdolle. Indikaattorien tulee myös olla vertailtavissa, jolloin niiden tulee olla määritettyjä määrän tai säännöllisyyden mukaan, riittävän tarkkoja, tuottaa vertailtavaa dataa ajankohdasta riippumatta ja olla yhdenmukaisia kaikkialla organisaatiossa. Lopuksi tulee huomioida indikaattorien helppokäyttöisyys, jolloin indikaattorien tulee olla saatavilla ajasta riippumatta, kustannustehokkaita ja olla helposti ymmärrettäviä ja kommunikoitavia. (Davies ym. 2006)

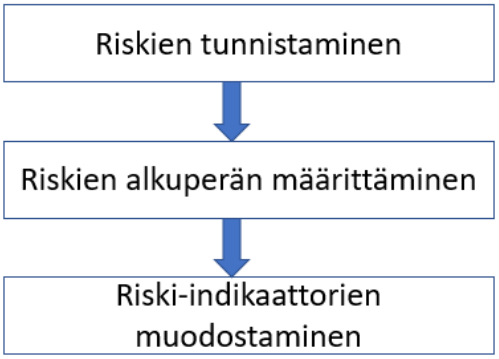
Saluja ja Idris (2014) esittelivät tutkimuksessaan prosessin, jossa määritettiin tietoturvariskeihin liittyvät indikaattorit. Indikaattoreiden määrittämisprosessi aloitettiin kartoittamalla riskejä erilaisten standardien ja riskityökalujen

avulla, joita olivat mm. Octave-Allegro, NIST:n ohjeistukset ja ISO/IEC 27005-standardi. Pohjana päädyttiin käyttämään ISO/IEC 27005-listausta potentiaalisista skenaarioista, sillä sen todettiin vastaavan parhaiten käsitystä potentiaalisista riski-indikaattoreista. Tutkimuksessa haastateltiin kohdeorganisaation turvallisuusjohtajia, turvallisuusanalyytikkoja ja organisaatioiden ydintoimintojen johtajia indikaattoreiden määrittämiseksi. Indikaattoreita tunnistettiin yli neljäkymmentä, ja ne kategorisoitiin seuraavasti:

1. Fyysiset vauriot: laitteistojen tuhoutuminen, luonnontuhot.
2. Olennaisten toimintojen menetys: sähkökatkot, telekommunikaation katkokset.
3. Tekniset ongelmat: järjestelmän toimintahäiriöt, haittaohjelmat.
4. Informaation vuotaminen: tietomurto luottamukselliseen tietoon, käyttäjän huijaaminen (social engineering)
5. Kielletyt toimenpiteet: kiellettyjen ohjelmistojen tai tiedostojen käyttö ja lataaminen, sallimaton pääsy tiloihin.
6. Operatiiviset haitat: puutteet henkilöstön koulutuksessa, osaamisen puute teknologian käytössä
7. Kolmannen osapuolen suorittamat kielletyt toimenpiteet: virheet tai kielletyt toiminnot, joita toimittaja, myyjä tai jokin muu alihankkija on suorittanut.

Havaittujen indikaattoreiden vakavuutta arvioitiin vertaamalla jokaista indikaattoria tietoturvallisuuden osa-alueisiin (saatavuus, luottamuksellisuus, eheys, ks. luku 2.1) sekä infrastruktuurissa ja organisaatiossa suoritettavien prosessien käytettävyyteen. Riskien vakavuus luokiteltiin merkitsemällä seitsemän kuukauden ajanjaksolla havaittujen vaikutuksien lukumäärä jokaista indikaattoria kohden, jolloin saatiin selville merkittävimmät riski-indikaattorit (Saluja & Idris, 2014).

Riski-indikaattoreiden määrittämiseen ei ole yhdenmukaista standardia tai viitekehystä. Tämä selittyy luultavasti sillä, että riskit ja indikaattorit liittyvät usein tiettyyn organisaatioon tai toimialaan. Matruglio ja Tymmons (2014) esittivät riski-indikaattorien luomisprosessin seuraavasti (kuvio 5):



Kuvio 5 Riski-indikaattorien määrittäminen (Matruglio & Tymmons, 2014 mukaan)

Riskien tunnistamisessa pyritään keskittymään erityisesti strategisiin riskeihin, jotka täytyy hallita tavoitteiden saavuttamiseksi. Toisessa vaiheessa tunnistetaan riskien taustat ja niihin liittyvät keskeiset oletukset, jolloin voidaan määrittää toimintatavat sekä milloin toimintatapoja käytetään. Viimeisessä vaiheessa määritetään tarvittavat resurssit ja kyvyt riskienhallintaan, määritetään riskien tunnistamiseen ja havaitsemiseen liittyvät suorituskyvyt sekä organisaation kyky reagoida riski-indikaattoreihin, mikäli niitä esiintyy (Matruglio & Tymmons, 2014).

Australian Finance Department (2016) esittää omassa mallissaan neliportaisen riski-indikaattoreiden luontiprosessin (kuvio 6):

Kuvio 6 Riski-indikaattoreiden määrittäminen (Australian Finance Department, 2016 mukaan)

Ensimmäisessä vaiheessa tarkoituksena on keskittyä tunnistamaan korkeat riskit ja määrittää näille sopivat mittarit. Toisessa vaiheessa valitaan indikaattorit. Erityisesti keskitytään valitsemaan helposti mitattavia ja seurattavia indikaattoreita, jotka kykenevät seuraamaan muutoksia riskissä. Lisäksi tässä vaiheessa voidaan määrittää erilliset hälytysrajat tai kynnykset, mikäli se soveltuu riskiin. Kolmannessa vaiheessa raportoidaan indikaattoreista niistä tehtyjen havaintojen perusteella, samalla tulee olla määritettynä indikaattorien seurantatiheys ja raportointitapa. Neljännessä vaiheessa siirrytään toimintaan, mikäli indikaattori lähestyy

määritettyä hälytysrajaa, samalla raportoidaan ennakoivien toimenpiteiden suoritusajankohdat (Australian Finance Department, 2016).

Indikaattoreiden määrittämisen ja tunnistamisen onnistuessa niiden tavoitteena on muuttaa riskienhallintaa tehokkaammaksi. Scarlat, Chirita & Bradea (2012) toteavat indikaattoreiden käytön tuovan useita etuja yrityksien riskienhallintaan. Heidän mukaansa yritys kykenee tunnistamaan ajoissa kasvavat trendit tai ongelmat sekä vallitsevan tilanteen paranemisen tai huonontumisen. Lisäksi indikaattorit auttavat tekemään päätöksiä niiden perustuessa tietolähteisiin ja arvioimaan organisaation suorituskykyä. Indikaattorien mainitaan myös tukevan ennakoivaa johtamista, parantavan ennustetta ja suorituskykyä yrityksen osalta tulevaisuudessa ja lisäävän asiakastyytyväisyyttä. (Scarlat ym., 2012). Jokaiselle tunnistetulle indikaattorille voidaan määrittää vastatoimet, joihin tulee ryhtyä hälytysrajan aktivoituessa. Tällä hetkellä riskien realisoitumiseen varaudutaan reagoivilla toimenpiteillä, jotka toimeenpannaan riskin realisoituessa. Riski voi kuitenkin aiheuttaa liiketoiminnallisia menetyksiä jo lyhyen ajan sisällä. Tällöin riski-indikaattorien käyttö olisi tehokkaampaa organisaation toiminnan kannalta, sillä indikaattoreille saataisiin riskeihin varautumiseen lisää pelivaraa. Indikaattorien käyttö sijoittuisi ajallisesti ennakoivien ja reagoivien toimenpiteiden väliin, sillä riskiin voitaisiin reagoida indikaattorin hälytysrajan aktivoituessa ennen riskin täydellistä realisoitumista. Jos indikaattoreita kyetään tunnistamaan ja niiden todetaan esiintyvän säännöllisesti, voidaan luoda työkalu, riskienhallintamalli tai lista indikaattoreista ja kyseisiin indikaattoreihin liittyvistä toimenpiteistä, kun indikaattori havaitaan. Edellä mainittuja keinoja hyödyntämällä projektien tietoturvariskienhallinta muuttuisi sujuvammaksi ja tehokkaammaksi.

3 Tutkimusmenetelmät

Tässä luvussa käydään tutkimuksen teon eri vaiheet ja tutkimuksessa käytetyt tutkimusmenetelmät. Luvussa kuvataan, kuinka tutkimus tehtiin, miten materiaalia kerättiin ja käytettiin sekä mitä hyödynnetyt työkalut ja tutkimuksessa ilmenneet ongelmat olivat.

Tutkimus pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

- Mitä tietoturvariskien indikaattoreita projekteista voidaan tunnistaa?
    - Miten havaittuja indikaattoreita voidaan hyödyntää projektien tietoturvariskien hallinnassa?
    - Mitkä käytännön työkalut tai menetelmät olivat haastateltavien mielestä toimivia tietoturvallisuuden riskienhallinnassa?

3.1 Tutkimuksen tekeminen

Tutkimuksen tekeminen aloitettiin alkuvuodesta 2020 pro gradu-seminaarin aikataulun tahdissa. Tutkimus lähti liikkeelle aiheen ideoinnista ja tutkimussuunnitelman teosta, jonka jälkeen kirjoitettiin tutkimuksen teoriaosuus. Tutkimuksen aihe ideoitiin työnantajan kanssa, jolloin tutkimus tuotettiin tilaustyönä organisaation käyttöön.

Tutkimuksessa käytettyä aineistoa etsittiin käyttäen eri hakukoneita ja tietokantoja, kuten Google Scholar, JYKDOK ja ACM Digital Library. Tutkielmaa ja käytetty lähdeaineistoa säilytettiin sekä työnantajan tarjoamalla tietokoneella ja työnantajan OneDrivessä varmuuskopiona.

Tutkimuksen aikataulun saneli tutkimuksen alkupuolella pro gradu-seminaarin aikataulu. Seminaarin päätyttyä tutkimuksen teossa noudatettiin seminaarin aikana suunniteltua aikataulua sekä tilaajaorganisaation kanssa sovittuja tavoitteita.

3.2 Laadullinen tapaustutkimus

Tutkimus toteutettiin laadullista tutkimusmenetelmää käyttäen. Tuomen ja Sarajärven (2018) mukaan laadullisessa tutkimuksessa keskitytään ymmärtämään ja kuvailemaan tutkittavaa asiaa tai ilmiötä kokonaisvaltaisesti. Laadullista tutkimusta voikin kuvata ymmärtäväksi tutkimukseksi, kun taas määrällinen tutkimus on luonteeltaan selittävää. Laadullisen tutkimuksen aineisto kootaan usein tietystä kohderyhmästä luonnollisissa tilanteissa, kuten käyttämällä haastatteluita tai kyselyjä. Haastattelut jakautuvat edelleen niiden rakenteen mukaan lomakehaastatteluun (strukturoitu haastattelu), teemahaastatteluun (puolistrukturoitu haastattelu) ja syvähaastatteluun (Tuomi & Sarajärvi, 2018). Laadullinen

tutkimus pyrkii Alasuutarin ja Alasuutarin (2012) mukaan viittaamaan aktiivisesti aiempaan tehtyyn tutkimukseen ja teoreettisiin viitekehyksiin päämääränä ns. ”ymmärtävä selittäminen”. Laadulliseen tutkimukseen kuuluu olennaisesti myös laadullinen analyysi, jossa selitetään koko aineistoon päteviä havaintoja (Alasuutari & Alasuutari, 2012).

Laadullinen tutkimus valikoitui tutkimustavaksi, sillä tarkoituksena on haastatella projektityöntekijöitä aikaisempiin projekteihin liittyen ja kerätä heidän havaintojaan riski-indikaattoreista. Tutkittavasta datasta ei ole mahdollista tai tarkoituksenmukaista saada numeerista dataa, mikä myös puoltaa laadullisen tutkimuksen käyttöä tutkimusongelmaan.

Tämän tutkimuksen tarpeisiin soveltui parhaiten puolistrukturoitu haastattelu. Puolistrukturoidussa haastattelussa on osittain määrätty kysymysrunko, mutta siinä on jouston varaa haastattelussa käytävän keskustelun ja esiin nousseiden kysymysten mukaan (DiCicco-Bloom & Crabtree, 2006). Haastatteluista saatava informaatio ei välttämättä ole luotettavaa, sillä haastattelu voi olla keinotekoinen tai jopa painostava haastateltavalle. Yksi keino parantaa haastatteluiden luotettavuutta on käyttää useampia haastateltavia, joilta saa erilaisia näkökulmia haastatteluissa esitettäviin kysymyksiin. Näin aineistosta saadaan esiin eroavaisuuksia ja samankaltaisuuksia (Eisenhardt & Graebner 2007).

Tutkimusstrategiana käytettiin tapaustutkimusta (engl. case study). Tapaustutkimus tutkii ilmiötä sen tosielämän kontekstissa käyttäen useita lähteitä. Painopisteenä on ilmiön ja sen kontekstin syvällinen ymmärtäminen. Tähän päästään tutustumalla muutamaan tai yhteen tapaukseen perusteellisesti tutkien sitä eri näkökulmista. Tämän tutkimuksen tavoitteena on tutkia muutamia tapauksia, eli toimeksiantajayrityksen projekteja. Tapaustutkimus pyrkii vastaamaan erityisesti kysymyksiin ”kuinka” ja ”miksi” (Yin, 1994). Lisäksi tapaustutkimus mahdollistaa useiden erilaisten aineistojen käytön tutkimuksessa, kuten haastattelut, havainnot, kyselyt ja dokumentit (Benbasat, Goldstein & Mead, 1987; Darke, Shanks & Broadbent, 1998). Tapaustutkimusta kritisoidaan usein sen heikosta tilastollisesta yleistettävyydestä, sillä yksi tai muutama tutkittava tapaus ei tuota riittävää pohjaa tilastollisille yleistyksille. Toisaalta tapaustutkimus ei tähtääkään laajaan yleistettävyyteen.

Tapaustutkimuksessa voidaan tutkia joko yksittäistapausta tai useita tapauksia. Yksittäinen tapaustutkimus on perusteltua, jos tarkoituksena on tutkia ainutlaatuista tapausta. Yksittäistä tapausta tutkimalla kyetään ymmärtämään perusteellisesti tutkittavaa ilmiötä, sillä yksittäiseen tapaukseen voidaan keskittyä täysin ja kuvata se yksityiskohtaisesti. Monitapaustutkimuksessa kerätään havaintoja useista tapauksista, joita verrataan keskenään. Monitapaustutkimus voidaan nähdä kattavampana tutkimuksena, mutta se voi olla hyvin työlästä ja aikaa vievää tutkijan osalta. Lisäksi tapausten valintaan tulee kiinnittää erityistä huomiota, jotta ne palvelevat tutkimusta mahdollisimman hyvin eivätkä tapaukset virheellistä tulkintaa (Yin, 1994).

Tapaustutkimukseen kuuluvia keskeisiä työvaiheita ovat (Eriksson & Koistinen, 2014):

- tutkimuskysymysten muotoilu

- tutkimusasetelman jäsentely
- tapausten määrittäminen ja valinta
- käytettävien teoreettisten näkökulmien ja käsitteiden määrittely
- aineiston ja tutkimuskysymysten välillä olevan vuoropuhelun logiikan selvittäminen
- aineiston analyysiin ja tulkintaan liittyvien sääntöjen päättäminen
- raportointitavan päättäminen

Tämä tutkimus eteni edellä mainittujen vaiheiden mukaisesti. Tutkimuskysymykset muotoiltiin tilaajaorganisaation kanssa yhteistyössä. Lisäksi tutkimuksessa hyödynnetyt tapaukset ja haastateltavat henkilöt valikoitiin tilaajaorganisaation yhteyshenkilön kanssa yhteistyössä.

Tämän tutkimuksen tarkoituksena ei ollut tuottaa laajasti yleistettävää tietoa, vaan tarjota toimeksiantajaorganisaatiolle työkaluja organisaation sisäisten prosessien esittämiseen. Vaikka laaja yleistettävyys ei ole tutkimuksen tavoitteena, voi lopputulosten hyödyntäminen tai siitä saadun tiedon soveltaminen olla mahdollista laajemmin.

Tutkimuksen tavoitteena oli ymmärtää projekteihin liittyvät tietoturvariskit, kartoittaa toimeksiantajaorganisaation projektien tietoturvariskeistä kertovia indikaattoreita ja luoda löydettyjen indikaattoreiden perusteella riskienhallinnan malli/työkalu, jolla indikaattoreita voidaan hyödyntää projektiriskienhallinnassa.

3.3 Tutkimuskohde: Huld Oy

Huld Oy on Suomessa ja Tšekissä toimiva kansainvälinen teknologian suunnittelutalo, jossa työskentelee n. 400 henkilöä. Huld Oy tarjoaa asiantuntijapalveluita liiketoiminnan digitalisointiin, ohjelmisto- ja tuotekehitykseen, toiminnalliseen turvallisuuteen ja tietoturvallisuuteen. Yrityksen asiakkaisiin kuuluu suuria teollisuusyrityksiä, julkisia organisaatioita sekä viranomaistoimijoita.

Tutkimuksen tavoitteena oli parantaa Huld Oy:n projektiriskienhallintaprosessia tietoturvariskien osalta. Huld Oy:ssä tapahtui yritysmigraatio alkuvuodesta 2020, jolloin yritys halusi päivittää samalla projektiriskienhallintaa. Tähän kehitystyöhön liittyi halu kartoittaa projektien tietoturvariskeistä varoittavia riski-indikaattoreita ja luoda niistä työkalu tai riskienhallintamalli avuksi projektiriskienhallintaan, sillä yrityksen liiketoiminta perustuu projektityöskentelyyn.

Huld Oy:stä valikoitiin haastatteluihin henkilöitä, joilla on kokemusta tietoturvallisuuden kanssa työskentelystä (taulukko 1). Haastateltavat 1 ja 2 ovat tietoturvakonsultteja, jotka toimivat eri toimialoilla toimivien asiakkaiden kanssa. Haastateltavat 3 ja 4 toimivat ohjelmistoprojekteissa, joissa haastateltava 3 keskittyy erityisesti testaukseen ja 4 turvalliseen ohjelmistokehitykseen. Haastateltava 5 toimii erityisesti terveydenhuollon asiakkaiden parissa, jossa hän keskittyy tiedonhallintaan. Haastateltava 6 toimii ohjelmistoarkkitehdin roolissa myös

toteuttaen ohjelmistoja, samalla hän vastaa organisaation ohjelmisto-osaamisen kehittämisestä. Haastateltavat 7, 8 ja 9 toimivat projektipäällikköinä. Haastateltava 7 toimii projektipäällikön tehtävien ohella liiketoiminnan kehittämistehtävissä. Haastateltava 8 työskentelee turvallisuuskriittisten järjestelmien parissa projektipäällikkönä keskittyen ohjelmistokehitykseen liittyviin tehtäviin, samalla hän toimii organisaation liiketoiminnan kehitystehtävissä. Haastateltava 9 toimii projektipäällikkönä erityisesti lääkinnällisiin laitteisiin liittyvissä projekteissa.

Taulukko 1 Haastatellut henkilöt ja heidän asemansa

Haastateltava	**Titteli**	**Kuvaus työtehtävistä**
Haastateltava 1	vanhempi tietoturvakonsultti	Toimii projektipäällikkönä ja tietoturvakonsulttina erityisesti kansallisen turvallisuuden projekteissa
Haastateltava 2	vanhempi tietoturvakonsultti	Toimii tietoturvakonsulttina erilaisissa tietoturvakriittisissä projekteissa
Haastateltava 3	it-konsultti	Toimii projektipäällikkönä tai konsulttina erityisesti ohjelmistoprojektien testauksessa
Haastateltava 4	ohjelmistosuunnittelija	Työskentelee erilaisissa ohjelmistoprojekteissa korkean turvallisuuden hankkeissa, kokemusta myös tietoturvakonsultoinnista
Haastateltava 5	vanhempi konsultti, projektipäällikkö	Toimii projektipäällikkönä ja konsulttina sosiaali- ja terveydenhuollon sektorilla
Haastateltava 6	ohjelmistoarkkitehti/team leader	Tekee ohjelmistojen suunnittelua ja toteutusta, kehittää organisaation ohjelmisto-osaamista
Haastateltava 7	projektipäällikkö, liiketoiminnan kehittäminen	Toimii projektipäällikkönä turvallisuuskriittisissä projekteissa, vastaa organisaation liiketoiminnan kehittämisestä

(jatkuu)

Haastateltava	Titteli	Kuvaus työtehtävistä
Haastateltava 8	projektipäällikkö	Työskentelee turvallisuuskriittisten järjestelmien parissa, projektipäällikkönä organisaation turvallisuusliiketoiminnan projekteissa
Haastateltava 9	projektipäällikkö	Toimii projektipäällikkönä lääkinnällisten laitteiden projekteissa

Haastateltavilla on paljon työkokemusta erilaisista projekteista, monet ovat tehneet projektimuotoista työskentelyä koko työuransa ajan. Monilla on kokemusta hyvin suurista projekteista ja eri projektirooleista. Projektit ovat olleet usein turvallisuuskriittisiä. Samalla heidän erikoistumisalueensa eroavat toisistaan. Haastatelluilta kerätystä datasta pyrittiin tunnistamaan projektien tietoturvariskeihin liittyviä indikaattoreita käyttäen apuna aiempaa tutkimusta ja malleja.

3.4 Empiirisen aineiston kerääminen

Tutkimuksessa analysoitava aineisto kerättiin puolistrukturoidulla haastattelulla (liite 1). Haastattelujen tavoitteena oli saada haastateltavilta mahdollisimman kattavia vastauksia haastattelukysymyksiin ja antaa haastateltaville mahdollisuus jakaa omia ajatuksiaan ja näkemyksiään aiheesta. Tarkoituksena oli saada tarpeeksi laaja sekä laadukas aineisto analyysivaihetta varten. Haastatteluista saatu empiirinen aineisto kerättiin kevään 2020 aikana. Haastattelut suoritettiin etänä koronaepidemian aiheuttaman poikkeustilan vuoksi.

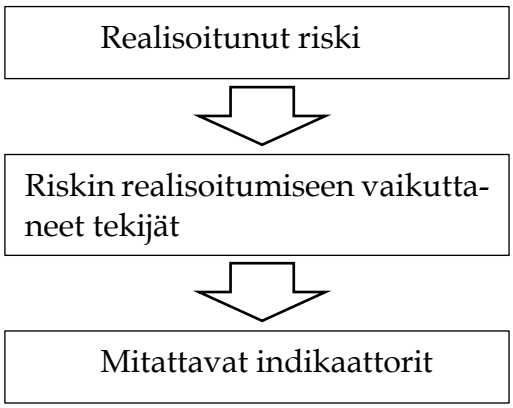
Haastattelut tehtiin käyttäen Microsoft Teams-palvelua, jossa haastattelut käytiin ja nauhoitettiin. Haastattelut litteroitiin, eli muutettiin puheesta tekstiksi. Ruusuvuoren, Nikanderin ja Hyvärisen (2010) mukaan litteroinnin tarkkuus tulee määrittää tutkimusongelman ja tutkimusmetodin mukaan. Jos tarkoituksena on tutkia haastatteluvuorovaikutusta tai henkilöiden välisiä suhteita, on oleellista litteroida aineisto yksityiskohtaisesti ja keskittyä *miten* tai *milloin* jotakin sanotaan. Mikäli haastattelussa keskitytään enemmän asiasisältöön, eli esimerkiksi halutaan tietää tiettyyn tilanteeseen tai prosessiin liittyvät tapahtumat, riittää tällöin vähemmän tarkka litterointi (Ruusuvuori ym., 2010). Tässä tutkimuksessa oleellista on haastattelujen asiasisältö, jolloin vähemmän tarkka litterointi riitti aineiston analysoinnissa. Tällöin puheeseen kuuluneet täytesanat jätettiin litteroiduista haastatteluista pois.

Tutkimusta varten haastateltiin yhdeksää henkilöä. Haastattelujen pituudet vaihtelivat, mutta haastattelut kestivät 20–30 minuuttia haastateltavasta riippuen. Tekstiksi muutettu aineisto luokiteltiin haastattelurungon mukaisesti. Litteroidut haastattelut lähetettiin ja hyväksytettiin haastateltavilla sekä opinnäytteen

tilanneen organisaation vastuuhenkilöllä. Haastattelujen hyväksyttämisen yhteydessä haastateltavien oli vielä mahdollista täydentää aikaisemmin annettua haastattelua tai poistaa haastattelusta materiaalia, mikäli he eivät olisi halunneet julkaista osaa materiaalista.

3.5 Aineiston analyysi

Litteroidut haastattelut analysoitiin yksitellen läpi haastattelurungon mukaisesti. Niistä etsittiin realisoituneita tietoturvariskejä, niihin vaikuttaneita tekijöitä sekä riskeihin liittyviä indikaattoreita. Projektien kohdealueet ja asiakkaat on häivytetty materiaalista liikesalaisuuksien pitämiseksi. Realisoituneiden riskien löytäminen projekteista oli oleellista, sillä niiden kautta oli mahdollista löytää realisoitumiseen vaikuttaneet tekijät. Riskejä pyrittiin ymmärtämään Matruglion ja Tymmonsin (2014) prosessia mukaillen (kuvio 7). Tekijöistä pystyttiin edelleen johtamaan indikaattoreita, jotka vastaavat mahdollisimman hyvin realisoituneeseen riskiin.



Kuvio 7 Indikaattorien määrittäminen

Analyysissa hyödynnettiin tutkimuksen teoriaosassa esiteltyjä materiaaleja. Erityisesti aiempia aiheeseen liittyviä tutkimuksia vertailtiin tässä tutkimuksessa tehtyihin havaintoihin ja löydöksiin. Realisoituneet tietoturvariskit jaoteltiin luvussa 2.1.1 esitellyn Kraemerin ym. (2009) kategorisoinnin mukaan. Tätä kategorisointia hyödynnettiin myös riskien realisoitumiseen vaikuttaneiden tekijöiden nimeämisessä. Inhimillisiin tekijöihin liittyneitä riskejä luokiteltiin käyttäen apuna Hughesin ja Ferretin (2007) määrittämää kategorisointia, jolloin tapauksia voitiin lajitella erilaisten juurisyiden perusteella.

Ensisijaisesti havaituista riskeistä pyrittiin johtamaan mitattavia indikaattoreita, jotta niiden seuraaminen olisi helpompaa. Indikaattoreita johdettiin teoriaosassa esiteltyjen aiempien tutkimuksien havaintojen perusteella sekä hyödyntämällä soveltuvin osin ISO/IEC 27005 (2018) esiteltyä listaa tyypillisimmistä haavoittuvuuksista. Osa indikaattoreista muodostettiin aineistolähtöisesti haastatteluissa esille tulleiden havaintojen perusteella, sillä aikaisemmat tutkimukset

tai materiaalit eivät vastanneet kaikkiin realisoituneisiin riskitapauksiin riittävän hyvin.

Aineiston analysointi oli haastavaa erityisesti inhimillisten syiden vuoksi realisoituneiden riskien osalta. Inhimillisistä syistä on haastava erottaa selkeitä ja mitattavia indikaattoreita, sillä riskin realisoitumisen taustalla olevat syyt ovat voineet olla monimutkaisia. Haastatteluista saadusta materiaalista ei pysty aukottomasti päättelemään kaikkia tapaukseen vaikuttaneita syitä, eivätkä haastateltavat osanneet täsmentää tapaukseen liittyneitä taustoja inhimillisten syiden osalta. Indikaattorien muodostamisen helpottamiseksi inhimillisistä syistä johtuneita riskejä pyrittiin jaottelemaan eri syistä johtuneisiin virheisiin.

Analyysin jälkeen toteutettiin yhteenveto tuloksista, joissa esiteltiin tunnistetut indikaattorit ja merkittävimmät tekijät, jotka vaikuttivat tietoturvariskien realisoitumiseen.

4 Projektien tietoturvariski-indikaattorit

Tässä luvussa käsitellään tutkimuksessa saadut tulokset. Luvussa esitellään Huld Oy:n aiemmista projekteista havaittuja realisoituneita tietoturvariskejä ja niihin liittyneitä indikaattoreita. Lisäksi luvussa esitellään aiemmissa projekteissa havaittuihin riskeihin liittyviä indikaattoreita, jotka on pyritty johtamaan aiempien tutkimusten ja ohjeistusten (ISO/IEC 27005) perusteella.

Inhimillisten virheiden vuoksi realisoituneet riskit olivat huomattavasti yleisempiä verrattuna teknisistä ratkaisuista johtuneisiin tietoturvariskeihin, tämä havainto toistui haastateltavien välillä. Haastateltavien työkokemuksen määrällä ei ollut selkeästi havaittavaa vaikutusta kykyyn tunnistaa indikaattoreita, vaan kyse oli enemmänkin sattumasta, jossa haastateltava oli osallistunut realisoituneita tietoturvariskejä sisältäneeseen projektiin.

4.1 Projekteissa realisoituneet tietoturvariskit ja niihin liittyneet tekijät

Haastatteluissa ilmeni toistuvasti, että realisoituneet tietoturvariskit oli tunnistettu riskienarviointivaiheessa, mutta ilmeisesti riskien vakavuuden ja todennäköisyyden arvioinnin haasteellisuuden vuoksi niihin ei ollut varauduttu riittävästi. Oli myös mahdollista, että käytettävissä ollut aika ei täysin riittänyt riskin realisoitumisen estämiseen. Aineistosta ilmenneet riskit ja niihin liittyneet indikaattorit pystyttiin luokittelemaan teknisistä ja inhimillisistä syistä johtuneisiin kategorioihin. Kappaleessa 4.1.1 käsitellään teknisistä syistä realisoituneet riskit ja niiden indikaattorit, kappaleessa 4.1.2 inhimillisiin virheisiin liittyneet riskit ja indikaattorit ja lopuksi kappaleessa 4.1.3 haastateltavien kokemukset määrällisten riskityökalujen toimivuudesta.

4.1.1 Tekniset indikaattorit

Seuraavia teknisiä indikaattoreita tunnistettiin liittyvän projekteissa realisoituneisiin tietoturvariskeihin: järjestelmässä esiintyvien käyttökatkojen määrä, järjestelmien/ohjelmistojen päivitysaste prosentteina, järjestelmien/ohjelmistojen päivitysten aikaväli sekä tunnistettujen haavoittuvuuksien lukumäärä järjestelmässä. Kaikki aineistossa mainitut riskit eivät realisoituneet, mutta kyseisiä riskejä on kuvailtu tästä huolimatta niiden realisoitumismahdollisuuden vuoksi.

Yksi haastateltavista kuvasi riskiä, jossa laitteiden oli mahdollista päätyä hyökkääjien haltuun.

> Eli se mikä itseasiassa siellä kaikista todennäkösintä oli se että kun ne (järjestelmät) pyörii jonkunnäkösissä embedded-linuxeissa tai vastaavissa että joku hyökkääjä ottaa haltuunsa sen laitteen ja käyttää sitä johonkin DDOS-hyökkäykseen tai mihin tahansa.

> - - Et jos ne päätyy hyökkääjien haltuun niin ne tekee niillä jotain inhottavaa ja toisaalta sit taas tää tiedon saavutettavuus häiriintyy sen takia kun laitteet, laskentakapasiteetti on jossain muussa käytössä kun mihin se on tarkotettu. (Haastateltava 4)

Kyseinen riski realisoitui myöhemmin projektin aikana, kun laitteita päätyi hyökkääjien haltuun puutteellisten päivitysten ja suojaustoimenpiteiden puuttumisen vuoksi. Järjestelmissä olevat puutteet oli havaittu jo aiemmin ja niihin ryhdyttiin tekemään päivitettävyyttä parantavia ratkaisuja sekä kovennuksia. Korjaavat toimenpiteet eivät ehtineet estää riskiä realisoitumasta. Riskin realisoitumisen indikaattorina voidaan pitää järjestelmän testauksen yhteydessä löytyneitä tuloksia, jotka osoittivat järjestelmän turvallisuuden olevan heikolla tasolla. Kraemerin ym. (2009) kategorisoinnin mukaan tämä voidaan lukea teknologisen kategorian alle.

> - - jos niille ajo niille käyttöjärjestelmille Nessuksella tämmösen CISin koventamislistoja, ja Nessuksella sä voit ajaa jotain käyttöjärjestelmää vastaan sen testin ja kattoo kuinkas turvallinen tää on niin kyllähän ne Nessus-raportit oli aika synkkää luettavaa tossa mielessä, että kyllä ne oli ihan selvästi tiedossa että nää on heikoissa kantimissa. (Haastateltava 4)

Tämän perusteella voidaan sanoa yhden indikaattorin olevan järjestelmistä löytyvien haavoittuvuuksien lukumäärä. Özçakmak (2019) tunnisti myös haavoittuvuuksien lukumäärän olevan yksi tunnistettu riski-indikaattori. Taulukossa 2 tätä indikaattoria kuvaa numero 1. Haavoittuvuuksien lukumäärä ei kuitenkaan kerro kaikkea, vaan yhtenä tärkeänä piirteenä voidaan pitää haavoittuvuuksien vakavuutta. Haavoittuvuutta voidaan sietää, mikäli sitä ei pystytä hyödyntämään, hyödyntäminen on erittäin vaikeaa tai sen vaikutus on vähäinen. Haavoittuvuuden vakavuutta voidaan mitata CVSS-arvolla (Common Vulnerability Scoring System), jonka avulla haavoittuvuuden vakavuus määritetään arvioimalla sen sisältämiä ominaisuuksia. Haavoittuvuudet listataan asteikolla 1–10, jossa luku 10 kuvaa kriittistä haavoittuvuutta (NVD, 2020). Näin ollen yhtenä indikaattorina voidaan pitää haavoittuvuuden CVSS-luokitusta, indikaattorin raja-arvoina voidaan käyttää haavoittuvuuden vakavuuden arvioimiseen määritettyjä arvoja (taulukko 2, indikaattori 2).

Kyseisiin järjestelmiin liittyi myös päivitettävyys ja päivitysten puuttuminen, joka auttoi hyökkääjiä saamaan laitteet haltuunsa. Näin ollen voidaan sanoa, että yhtenä teknisenä indikaattorina voitaisiin pitää ohjelmistojen päivitysastetta, jota seurattaisiin joko päivitysten lukumääränä tai päivitettyjen laitteiden osuutena kaikista laitteista (taulukko 2, indikaattori 3). Päivityksiin liittyvä indikaattori on myös päivitysten aikaväli, sillä säännöllisellä päivittämisellä taataan laitteiston tai ohjelmiston ajantasaisuus (taulukko 2, indikaattori 4).

Myös toisessa verifiointi- ja testauspainotteisessa projektissa havaittiin poikkeamien lukumäärällä olevan mahdollinen yhteys tietoturvariskin realisoitumiseen, vaikka tätä ei tapahtunutkaan.

> No siis kun tää oli tämmönen kolmannen osapuolen verifiointiprojekti niin mehän tehtiin sen projektin aikana melkein 300 havaintoa. Joista sanosin että karkeesti kolmasosa

> on sellasia että ne on jollain tavalla merkittäviä. Näähän on yleensä tällasia laadullisia poikkeamia mitä me tunnistettiin, taikka toiminnallisuuteen liittyviä. Mutta nää, ne sen verran hyvin korreloi tällasen tietoturvariskien kanssa laadulliset/toiminnalliset poikkeamat että kyllä siellä varmaan niitten joukossa oli sen kaltasiakin. Kuten esimerkiks just tällasia puskurin ylivuotoihin liittyviä tai vastaavia. (Haastateltava 7)

Teknisiin ratkaisuihin liittyviä realisoituneita tietoturvariskejä liittyi palvelun saatavuuteen. Haastateltava 2 kuvasi saatavuusriskin realisoitumista tyypilliseksi ongelmaksi projekteissa. Hänen mukaansa tyypillinen esimerkki toteutuneesta riskistä oli järjestelmän käytön estyminen käyttöpisteessä. Tällöin perusmenettely riskiin reagoimiseen oli tietojen kirjaaminen paperille ja siitä toimittaminen pisteeseen, jossa tietojen kirjaaminen oli mahdollista. Kyseinen riski oli tunnistettu jo aikaisemmassa vaiheessa projektia ja haastateltava näki kyseisen riskin realisoitumisen kokonaisuuden huomioiden kiusallisena, mutta sillä ei ollut suurempaa vaikutusta projektin lopputulokselle. Tästä tapauksesta ei ollut mahdollista muodostaa indikaattoria, sillä aineistosta ei pystynyt luotettavasti päättelemään riskin realisoitumiseen vaikuttaneita syitä.

Myös muut haastateltavat kuvasivat tiedon saatavuuteen liittyviä riskejä projektin aikana.

> - - mikä liittyy myös tietoturvallisuuteen mun ajatusmaailmassa on saatavuus. Niin siinähän me saatiin sit vaikka minkänäkösiä ongelmia kun oltiin päästy tuotantoon niin sitten aina välillä tuli ihan isompia ja pienempiä tämmösiä ongelmia ettei ollut tiedot käytettävissä. (Haastateltava 5)

Projektissa kehitettävässä tietojärjestelmässä esiintyi huomattavia viiveitä ja käyttökatkoja ennen järjestelmän kaatumista, jolloin voidaan sanoa yhden indikaattorin olevan järjestelmässä esiintyvien häiriöiden tai käyttökatkojen määrä (taulukko 2, indikaattori 5).

> No jälkeenpäin jos tollain miettii niin se että alkaa hitautta tulemaan eli tulee tämmösiä ennen kuin homma kosahtaa ihan kokonaan, niin hitaus hiipi. Ja ihan selkeesti tuli käyttäjiltä varoitusmerkkejä että nyt tämä on hidas, nyt tässä on jotain hitauksia. Niitä raportoitiin pikkuhiljaa ja ne oli hiljaisia signaaleja tosta. (Haastateltava 5)

Riskin realisoitumiseen liittyvinä tekijöinä pidettiin projektin kokoluokasta aiheutunutta kompleksisuutta. Projektiin kuului useita organisaatioita ja sitä myötä erilaisia toimintatapoja, jotka lisäävät tyypillisten projektiriskien eskaloitumisen mahdollisuutta. Useiden eri toimijoiden kesken toteutetussa projektissa projektin kokonaiskuva katoaa herkästi ja projektissa ajaudutaan tekemään projektin kannalta vääriä asioita. Kompleksisuus edesauttoi tietoturvariskin realisoitumista, sillä riskin kehittymistä oli vaikea havaita useiden eri elementtien joukosta. Kompleksisuus ei kuitenkaan suoranaisesti ole tietoturvariski, vaan pikemminkin yleinen projektiriski.

> No tuota, ehkä noissa realisoituneissa tapauksissa nimeäisin kaks tekijää. Toinen on se yleinen monimutkaisuus, kompleksisuus tossa kokonaisuudessa. Siinä oli monta eri

> organisaatiota, monta eri lähdejärjestelmää, monta eri toimintamallia ja sit nää ympättiin yhteen ja teknologia oli vähän uutta. Niin siellä oli paljon semmosia mitä ei vaan yksityiskohtien määrästä johtuen saatu ennakoitua tai sit ne ei ehkä pompannu esiin. Että joskus mietittiin että jos tässä otettas käyttöön rautakankea niin siinä ois aika paljon vähemmän liikkuvia osia niin että pystyttäs ennakoimaan helpommin. (Haastateltava 5)

Edellisestä lainauksesta käy ilmi, että projektiin kuului myös uutta teknologiaa, mikä voi aiheuttaa projektissa viivästyksiä käytettävyysongelmien ja osaamisen puutteen vuoksi.

Realisoituneita teknisiä tietoturvariskejä liittyi myös salassa pidettävään tietoaineistoon. Tästä syystä projektin riskienarvioinnissa korostuivat luottamuksellisuuteen liittyvät toimet ja tiedon luottamuksellisuuden rikkoutuminen nähtiin merkittävimpänä riskinä. Luottamuksellisuuteen liittyvä riski ei kuitenkaan realisoitunut haastateltavan kuvaamassa projektissa.

> - - salassapidettävää aineistoahan on paljon kun ollaan käyttökohteessa, niin se luottamuksellisuus korostuu siellä hyvinkin paljon. (Haastateltava 5)

Luottamuksellisuuteen liittyvät riskit voivat olla sekä teknisistä että inhimillisistä syistä johtuvia. Riskien realisoitumiseen johtaneita inhimillisiä syitä ja niistä johdettuja indikaattoreita käsitellään seuraavassa kappaleessa.

4.1.2 Inhimilliset indikaattorit

Tässä kappaleessa esitellään inhimillisistä virheistä aiheutuneet riskit ja niihin liitettävät indikaattorit. Osassa tapauksia oli havaittavissa päällekkäisyyksiä haastateltavien välillä. Osassa tapauksia indikaattorien muodostaminen ei ollut mahdollista, sillä tapaukseen liittyneitä yksityiskohtia ei voinut tunnistaa aineistosta. Inhimillisistä virheistä johtuneet riskit olivat teknisiä riskejä tyypillisempiä.

Eräs haastateltavista korosti turvallisuuskriittisessä projektissa juuri inhimillistä puolta ja siitä aiheutuvia potentiaalisia riskitilanteita. Muut haastateltavat eivät korostaneet inhimillisten virheiden mahdollisuutta samalla tavalla, mutta ne ovat selkeästi tunnistettavissa myös muista projekteista.

> Mut siis hyvin tällasia inhimillisiä asioita mitä siellä oikeestaan tarkastellaan. Että ihmiset toimii oikeesti koska ne, koska se prosessi on niin paljon, ei nyt jäykempää mutta tarkempaa noissa käyttökohteen projekteissa. Versus se tällaseen normaaliin ohjelmistoprojektiin, jossa voidaan testailla ja kokeilla että toimisko tää hyvin, otetaanko tämmönen koodinpätkä mukaan täältä vai ei. Niin sellanen ei oo mahdollista ollenkaan. (Haastateltava 1)

Haastateltava kuvasi myös inhimillisten virheiden olleen merkittävä tekijä projektissa realisoituneiden riskien osalta, vaikka niihin oli pyritty varautumaan mahdollisimman hyvin ennakkoon. Kiinnostavaa oli myös havainto siitä, että haastateltavalla oli kokemusta aiemmin realisoituneiden riskien uudelleen realisoitumisesta, vaikka asiaan oli pyritty puuttumaan.

> No siinä ihan nää inhimilliset, eli siis unohtui tai ei muistettu että piti tehdä sitä tätä tuota, ennen kuin teen tätä. - - No mulla on pari keissiä, sellanen jossa riski on realisoitunu pariinkin otteeseen. Ne nyt on selkeesti sellasia että vaikka on keskusteltu asiat läpi että hei, nyt pääs käymään näin, niin sit se pääs käymään vielä uudestaan. (Haastateltava 1)

Koska kyseessä oli korkean turvallisuuden projekti, kuului siihen oleellisena osana turvallisuuskoulutus projektihenkilöstölle, jossa käytiin läpi turvallinen ja sallittu toiminta projektin aikana. Yhtenä mahdollisena indikaattorina voitaisiin pitää turvallisuuskoulutuksen tai turvallisuuskertauksen määrää, jota saattaisi olla tarpeellista lisätä, mikäli virheitä tai unohduksia tapahtuu liian paljon. Saluja ja Idris (2014) tunnistivat tutkimuksessaan yhdeksi indikaattoriksi työntekijöiden puutteellisen koulutuksen, josta seurasi useita erilaisia virheitä (esim. vahingossa poistettu data, tiedon lähettäminen väärälle vastaanottajalle, datan syöttövirheet). Myös Kraemer ym. (2009) tunnistivat harjoittelun ja koulutuksen puutteen yhdeksi teemaksi, jossa oli puutteita sekä käyttäjien että kehittäjien osalta. Haastateltavan nimetessä unohduksien olevan syynä riskien realisoitumiseen voidaan todeta kyseessä olevan osaamiseen perustuvat virheet, joiden alle kuuluvat muistamiseen liittyvät virheet. Tämä tukee myös harjoittelun ja koulutuksen määrän ja siinä osoitetun osaamisen seuraamista indikaattorina (taulukko 3, indikaattori 1).

Haastateltava 5 kuvasi toisenlaisen projektiin liittyneen inhimillisen tekijän, joka johtui osaamisen puutteesta.

> Ja sitten tavallaan ei päästy siihen ongelmaan käsiks koska se porukka jonka kanssa puhuttiin niin se oli, se ei riittänyt osaaminen näihin asioihin. (Haastateltava 5)

Myös Kraemer ja kollegat (2009) tunnistivat tutkimuksessaan resurssienhallinnan kategoriaan kuuluvat tekijät, joita olivat puutteet tiedoissa tai kokemuksissa laitteiden tai tietoturvallisuuden osalta. Osaamista on haastava indikoida määrällisesti, mahdollisesti työkokemuksen määrä kyseiseen tehtävään nähden tai tehtävän edellyttämän koulutuksen omaavien työntekijöiden lukumäärä voisi toimia mitattavana indikaattorina (taulukko 3, indikaattori 2). Hughes ja Ferretin (2007) taksonomiaa tarkastellen kyseisessä projektissa on ollut selkeästi kyse osaamiseen perustuvista virheistä, myös haastateltava osoittaa tämän selkeästi.

> Ja sit toinen varotusmerkki minkä tosta oppi, että jos mä kysyn jotain teknistä spesifikaatiota ja se toinen osapuoli ei tiedä oikeen että se vastaa jotain häröä, niin sit se on varotusmerkki siitä että onko nää ajantasalla nää ihmiset, tietääkö ne ees mistä puhutaan. (Haastateltava 5)

Osaamisen puute voi johtaa herkästi inhimillisiin virheisiin. Eräässä projektissa varomaton toiminta vaaransi järjestelmän luottamuksellisuuden.

> Yks semmonen että siellä oli semmonen platform-tiimi joka piti embedded-käyttöjärjestelmistä huolta, niin siellä oli yks kaveri vahingossa copypastennu root-salasanan, käyttöjärjestelmän root-salasanan IRCiin. Ja se miks se synty oli tietysti se että niillä oli salasanat siellä. (Haastateltava 4)

Kyseiseen virheeseen on voinut vaikuttaa monikin asia. Tämän vuoksi indikaattorin osoittaminen tästä tapauksesta on haastavaa. Inhimillisten virheiden kategorian suhteen kyseinen tapaus voidaan luokitella todennäköisesti kuuluvan erehdyksiin. Luultavasti tapauksen osalta puutteita on ollut sekä säännöistä että tiedoissa, joiden myötä erehdys on tapahtunut. Oletettavasti projektin henkilöstöllä on ollut aiempaa kokemusta vastaavista projekteista, joten osaamiseen liittyviä syitä ei voida pitää yhtä todennäköisenä. Kyse voi olla myös puutteista tietoliikennevälineitä ja viestintää koskevissa toimintaperiaatteissa, joiden ISO/IEC 27005 (2018) mainitsee olevan uhka tietoturvallisuudelle. Tästä voidaan johtaa indikaattori turvallisuuskoulutukseen osallistumisasteesta tai koulutusten tiheydestä (taulukko 3, indikaattori 3).

Haastateltavat kuvasivat myös aiemmissa projekteissa käyttäjien aiheuttaneen tilanteita, joissa palvelun saatavuus oli estynyt käyttäjän toiminnan vuoksi. Projekteissa ei ollut osattu huomioida riittävällä laajuudella käyttäjien aiheuttamia poikkeustilanteita, vaan merkittävimpinä riskeinä pidettiin järjestelmien sisältämän tiedon luottamuksellisuutta.

> Mä muistaisin että yks ainut riski tai tavallaan yks ainut isompi ongelma siinä oli ja se tuli heti ensimmäisellä kerralla kun se ensimmäinen asiakas otti käyttöön sen. Siellä oli semmonen kiva rekursio-ongelma, että kun sen datan sinne generoi tietyllä tavalla tai toisen datan niin sitten se tukehtu tavallaan rekursioon se palvelu. (Haastateltava 6)

Haastateltavan mukaan kyseistä tapausta ei ollut osattu ennakoida. Käyttäjän toiminnan ennakoiminen ja arvioiminen on hyvin haastavaa, sillä useita järjestelmiä pystytään käyttämään monilla erilaisilla tavoilla ja kaikkien näiden tapojen löytäminen tuotetta kehitettäessä on vaikeaa. Useat mahdolliset käyttäjät ja sitä myötä erilaiset tavat käyttää järjestelmää olivat merkittävimmät tekijät riskin realisoitumiseen.

> No varmaan nyt ensisijaisesti aina vaikuttaa se että kun ajattelee että ohjelmistoa käytetään tietyllä tavalla niin kun tulee sitten ihan, tulee käyttäjiä jotka ei tiedä ohjelmistoista mitään niin ne löytää aina semmosia tapoja mitä ei ajatellutkaan että sitä vois käyttää niin. (Haastateltava 6)

Kraemer ym. (2009) mainitsee käyttäjien koulutuksen puutteen olleen yksi tekijä, joka vaikuttaa merkittävästi tietoturvallisuuteen. Tällöin voidaan todeta käyttäjän erehtyneen järjestelmän käyttöön liittyvien tietojen puutteen vuoksi. Tässä tapauksessa indikaattorina voitaisiin pitää käyttäjäkoulutukseen käytettyä aikaa tai koulutuskertojen lukumäärää (taulukko 3, indikaattori 4).

Myös muut haastateltavat kuvasivat käyttäjän toiminnan aiheuttaneen riskin realisoitumisen. Eräässä projektissa käyttäjän toimintaan liittyviä riskejä oli pyritty tunnistamaan, mutta riskien tunnistus ei ollut onnistunut riittävässä laajuudessa käyttäjän toiminnan osalta. Haastateltava 2 kuvasi pienen osan käyttäjistä jättäneen tekemättä lopullisen toimenpiteen vahvistuksen järjestelmää käytettäessä, minkä seurauksena prosessi jäi kesken, eikä tieto kirjautunut järjestelmään. Kyseisen virheen seurauksena koko toimintaprosessi jouduttiin uusimaan

niiden käyttökohteitten osalta, joissa käyttäjät eivät tehneet lopullista vahvistusta. Haastateltavan mukaan kyseessä oli esimerkki riskistä, jossa käyttäjien erilaisia toimintatapoja ja niihin liittyviä riskejä ei kyetty ennakoimaan riittävästi. Myös tämä tapaus tukee käyttäjien puutteellisen osaamisen olleen merkittävin tekijä riskin realisoitumiseen, jolloin mahdollisena ratkaisuna ja indikaattorina voitaisiin pitää käyttäjien koulutusta (taulukko 3, indikaattori 4).

Eräs haastateltavista kuvasi projektissa isoimmaksi riskiksi henkilökohtaista tietoa sisältävän laitteen katoamisen. Riski ei ollut realisoitunut, mutta kyseisessä riskissä esiin nousee myös selkeästi inhimillisen tekijän merkitys riskin realisoitumisen mahdollistajana. Laitteen katoaminen voidaan liittää puutteelliseen osaamiseen, jolloin mahdollisena indikaattorina myös tässä tapauksessa voidaan sanoa olevan puutteet käyttäjän koulutuksessa.

> - - meillähän on siis käyttökohdedataa tai käyttökohdemittaustuloksia mobiililaitteella. Ja mobiililaitteethan katoaa helposti koska ne ei oo pultattu kiinni mihinkään pöytään, me ei tietenkään voida hallita fyysisesti mihin ihmiset vie niitä. Me voidaan sanoa ihmisille, että älkää viekö niitä ulos rakennuksesta mutta käytännössä me joudutaan kuitenkin suunnittelemaan erilaisia featureita mitkä mitigoi sitä riskiä että se laite katoaa tai joku ihminen, jolla ei oo mitään asiaa pääsee fyysisesti käsiks siihen laitteeseen. (Haastateltava 9)

Aineistosta voitiin havaita, että inhimilliset riskit olivat yleisiä ja niihin oli pyritty varautumaan. Inhimilliseen virheeseen johtaneet syyt olivat moninaisia, jolloin niihin varautuminen oli haastavaa. Monilla tapauksista oli yhteisiä piirteitä, jolloin myös indikaattoreissa oli päällekkäisyyttä. Useat indikaattoreista liittyivät osaamisen puutteisiin, mutta näkökulma puutteelliseen osaamiseen vaihteli.

4.1.3 Muodostetut riski-indikaattorit

Taulukossa esitetään yhteenvetona tunnistettuja teknisiä (taulukko 2) sekä inhimillisiä (taulukko 3) riski-indikaattoreita. Taulukoissa tarkastellaan sekä tässä tutkimuksessa muodostettuja että aiemmissa tutkimuksissa havaittuja indikaattoreita, joista taulukoihin on pyritty valikoimaan tämän tutkimuksen kannalta merkittävimmät. Molempiin taulukoihin on numeroitu riski-indikaattorit, niille mahdollisesti annetut seurattavat arvot ja indikaattoreiden tunnistamisen apuna käytettävä data. Indikaattorit on pyritty määrittämään luvussa 2.5 kerrottujen ominaisuuksien mukaan. Tässä tutkimuksessa johdetuille indikaattoreille ei ole määritetty raja-arvoja, mutta taulukoihin on listattu soveltuvin osin muissa tutkimuksissa määritettyjä indikaattoreita ja raja-arvoja. Tässä tutkimuksessa havaittiin indikaattorit 1–5 taulukosta 2 sekä indikaattorit 1–4 taulukosta 3.

Salujan ja Idrisin (2014) tekemässä tutkimuksessa ei otettu kantaa siihen, minkälaista dataa voidaan hyödyntää riskin kehittymisen seuraamiseen, jolloin tässä tutkimuksessa esitetään taulukossa kuvatut datalähteet riskin seuraamiseksi. Taulukoiden sarakkeet ”seuraamiseen käytettävä data” on tutkijan itsensä muodostama.

Taulukossa 2 mainitut tekniset indikaattorit 2–5 on muodostettu aineistolähtöisesti tämän tutkimuksen aineiston perusteella. Indikaattorit 6–10 ovat Özçakmakin (2019) ja Salujan ja Idrisin (2014) tekemiä havaintoja indikaattoreista, jotka eivät olleet suoraan johdettavissa tämän tutkimuksen aineistosta, mutta jotka tukevat tätä tutkimusta.

Taulukko 2 Tunnistetut tekniset riski-indikaattorit

Indikaattori	**Indikaattorin sanallinen kuvaus**	**Indikaattorin seuraamiseen käytettävä data**	**Indikaattorin raja-arvot**
Indikaattori 1 (Özçakmak, 2019)	Tunnistettujen haavoittuvuuksien lukumäärä järjestelmässä	Tarkastuslistojen ajaminen järjestelmää vastaan ja siitä saatujen haavoittuvuuksien lukumäärä	<5 normaali tilanne <5-15> kohonnut riski >15 riski lähellä realisoitua
Indikaattori 2	Löydettyjen haavoittuvuuksien CVSS-arvo	Haavoittuvuusdokumentaatio ja vakavuusarviot	<4,0 normaali tilanne <4,0-6,9> kohonnut riski <7,0-10,0> riski lähellä realisoitua
Indikaattori 3	Järjestelmien/ohjelmistojen päivitysaste prosentteina	Järjestelmien päivitysloki	-
Indikaattori 4	Järjestelmien/ohjelmistojen päivitysten aikaväli	Järjestelmien päivitysloki	-
Indikaattori 5	Järjestelmässä esiintyvien käyttökatkojen määrä	Järjestelmien käyttöloki	-
Indikaattori 6 (Özçakmak, 2019)	Poikkeavan tietoliikenteen osuus normaalista tietoliikenteestä	Tietoliikennelokin seuranta, poikkeavan liikenteen black-listing (haitallinen liikenne ja osoitteet) ja white-listing (luotetut sivustot ja osoitteet)	<1% normaali tilanne <1-2%> kohonnut riski >2% riski lähellä realisoitua

(jatkuu)

Indikaattori	Indikaattorin sanallinen kuvaus	Indikaattorin seuraamiseen käytettävä data	Indikaattorin raja-arvot
Indikaattori 7 (Özçakmak, 2019)	Ilman tukea olevien järjestelmien tai sovellusten lukumäärä	Järjestelmien ja sovellusten käyttöloki sekä ylläpitoloki	<1% normaali tilanne <1-2%> kohonnut riski >2% riski lähellä realisoitua
Indikaattori 8 (Saluja ja Idris , 2014)	Järjestelmien ja tiedostojen vaurioitumisen tai tuhoutumisen lukumäärä	Vaurioituneiden tai tuhoutuneiden tiedostojen ja järjestelmien lukumäärä, tiedostojen ja laitteiden saatavuus	-
Indikaattori 9 (Saluja ja Idris, 2014)	Riittämättömät käytänteet järjestelmien haavoittuvuuksiin reagoimisessa ja hallinnassa	Haavoittuvuuden korjaamiseen/päivittämiseen käytetty aika	-
Indikaattori 10 (Saluja ja Idris, 2014)	Riittämättömät toimenpiteet ja käytänteet teknisten laitteiden huollon osalta	Laitteisiin tehtyjen huoltojen aikavälit, aikaisemmin tehtyjen huoltojen sisältö ja tarkoitus	-

Taulukossa 3 mainitut inhimilliset indikaattorit 1-4 on muodostettu aineistolähtöisesti ja indikaattorit 5-9 on tunnistettu aiemmissa tutkimuksissa (Özçakmak, 2019; Saluja & Idris., 2014). Muodostetut indikaattorit eivät kata täydellisesti tiettyä riskiä niiden inhimillisen puolen vuoksi, sillä inhimilliseen virheeseen vaikuttaneet syyt voivat olla monitahoisia ja niihin varautuminen täydellisesti on äärimmäisen haastavaa.

Taulukko 3 Tunnistetut inhimilliset riski-indikaattorit

Indikaattori	Indikaattorin sanallinen kuvaus	Indikaattorin seuraamiseen käytettävä data	Indikaattorin raja-arvot
Indikaattori 1	Käyttäjä/henkilöstökoulutuskertojen lukumäärä	Koulutusten aikavälit, osallistujien lukumäärä koulutuksiin, koulutuksessa osoitettu osaaminen	-
Indikaattori 2	Työntekijän työkokemuksen määrä vaaditussa tehtävässä	Työntekijän soveltuva koulutus, työkokemus asiantuntijatehtävissä, työntekijän testaaminen soveltuvuuskokeella	-

(jatkuu)

Taulukko 3 (jatkuu)

Indikaattori	**Indikaattorin sanallinen kuvaus**	**Indikaattorin seuraamiseen käytettävä data**	**Indikaattorin raja-arvot**
Indikaattori 3	Projektin henkilöstön tietoturvalliseen toimintaan liittyvien koulutusten lukumäärä	Koulutusten aikavälit, osallistujien lukumäärä koulutuksiin, koulutuksessa osoitettu osaaminen	-
Indikaattori 4	Käyttäjien koulutukseen käytetty aika	Koulutusten aikavälit, osallistujien lukumäärä koulutuksiin, koulutuksessa osoitettu osaaminen	-
Indikaattori 5 (Saluja ja Idris, 2014)	Työntekijöiden tekemien virheiden lukumäärä projektissa käytettävien järjestelmien käytössä	Vahingossa poistettu data, vahingossa väärään osoitteeseen lähetetty data, datan syöttövirheet, ohjelmointivirheet	-
Indikaattori 6 (Saluja ja Idris, 2014)	Henkilöstön tietoturvatietoisuuden taso	Henkilöstön tekemien tietoturvavirheiden lukumäärä ja vakavuus, henkilöstön kokemus vaaditussa tehtävässä	-
Indikaattori 7 (Özçakmak, 2019)	Puuttuvien henkilöiden määrän keskiarvo tietoturvatietoisuuden koulutuksissa	Koulutuksissa läsnä olleiden lukumäärä	<10% normaali tilanne <10-20%> kohonnut riski >20% riski lähellä realisoitua
Indikaattori 8 (Özçakmak, 2019)	Parhaiden käytäntöjen vastaisesti muodostettujen ja käytettyjen salasanojen osuus	Salasanan pituus ja sisältö, saman salasanan käyttö useassa eri kohteessa	<2% normaali tilanne <2-3%> kohonnut riski >3% riski lähellä realisoitua

Tässä tutkimuksessa tietoturvariskien inhimillinen puoli painottui teknistä puolta enemmän. Tämä ei käy ilmi taulukosta, sillä taulukoihin on tuotu havaintoja aiemmista tutkimuksista.

4.1.4 Haastateltavien kokemukset määrällisten riskityökalujen toimivuudesta

Haastatelluilta kysyttiin toimeksiantajaorganisaation toivomuksesta heidän kokemuksistaan määrällisten riskiarviointityökalujen toimivuudesta. Haastatelluilla henkilöillä on työkokemusta hyvin erilaisista projekteista ja niissä käytetyt työkalut ovat voineet vaihdella merkittävästi. Näin ollen haastatelluilta haluttiin kysyä heidän näkemystään siitä, mitkä riskien arvioinnissa käytetyt työkalut tai

menetelmät olivat osoittautuneet toimiviksi heidän toimialoillaan. Haastateltavien kokemusten perusteella olisi mahdollista kerätä toimivaksi osoittautuneista työkaluista tai menetelmistä työkalupakki organisaation tietoturvariskienhallintaan tai hyödyntää haastateltavien kokemuksiin perustuvia ominaisuuksia riski-indikaattoreiden hyödyntämisessä. Haastateltavien kokemuksia haluttiin kuulla myös siksi, että kokemuksia voitaisiin tarvittaessa hyödyntää rakennettaessa riski-indikaattoreista oma työkalu organisaation käyttöön ja hyödyntää siinä haastatteluissa ilmenneitä ominaisuuksia.

Haastateltavat totesivat määrällisten riskityökalujen antamien arvioiden olleen yleensä oikeansuuntaisia, suuria erehdyksiä ei ollut juurikaan sattunut riskienarvioinnissa. Haastateltavat pitivät määrällisten riskiarviointien hyvinä puolina niiden suhteellisen helppoa käyttöä ja kykyä nostaa esiin merkittävimmiksi arvioidut riskit. Haastateltavat kokivat määrällisten riskienarvioinnin tulosten olleen suurimmaksi osaksi realistisia.

Haastateltavat kokivat määrällisten riskiarviointien heikkouksina siihen sisältyvän arvioinnin subjektiivisuuden, jolloin arvioijan oma näkemys riskin vakavuudesta vaikutti merkittävästi arvioinnin tulokseen. Yksi haastateltavista kuvasi pienemmiksi arvioitujen riskien realisoitumisen tyypillisemmäksi kuin vakaviksi arvioitujen riskien. Syynä tähän voi olla se, että projektiorganisaatio keskittyy pelkkiin vakaviin riskeihin ne tunnistettuaan tai riskejä ei ole arvioitu oikein. Haastatteluissa korostettiin myös sitä, että harvinaisempien riskien arvioiminen on erittäin haastavaa, sillä jokin riski voi toistua kerran kymmenien vuosien aikana ja olla realisoituessaan äärimmäisen vakava. Tämä edellyttää pitkää projektikokemusta, jotta kyseiset harvinaiset mutta vakavat riskit kyetään arvioimaan ja tunnistamaan realistisesti. Voidaan todeta, että haastateltavien havainnot määrällisten riskiarviointien heikkouksista tukevat luvussa 2.2 esitettyjä Coxin (2008) havaintoja aiheesta.

> Tällaset kvantitatiiviset arvioinnit riskeistä ja niitten, kyllä ne nyt suhteellisen hyvin mun mielestä täsmää mutta siis se mikä on erittäin vaikee että sitten kun lähtee noita vähän harvinaisempia riskejä analysoimaan. - - Että sillon kun sä puhut siitä että okei, sulla on korkean severityn riskejä, mutta sitten ne on sellasia jotka tapahtuu kerran 50 vuodessa tai vastaavaa tai kerran 50 projektissa sun kvantitatiivinen mittari sille, niin sulla pitää olla järkyttävän pitkä projektikokemus että sä pystyt realistisesti tunnistamaan noita. (Haastateltava 7)

Haastateltavien mielestä tietoturvallisuuteen liittyvien riskien tunnistusta voitaisiin parantaa hyödyntämällä erilaisia tarkastuslistoja, jotka ohjaavat riskienarviointia ja auttavat tunnistamaan projektiin liittyviä tekijöitä systemaattisesti. Haastateltavat mainitsivat myös yhä pidemmälle etenevän digitaalisuuden lisäävän projektien kompleksisuutta tietoturvallisuuden osalta, jolloin tarvittaisiin enemmän seurantatietoa projektin aikana tapahtuneista asioista sekä parempaa informaatiota projektiin kuuluvien asioiden välisistä yhteyksistä. Teknisiin ratkaisuihin liittyen haastateltavat mainitsivat koodikatselmoinnin ja uhkamallinnuksen olleen toimivia ratkaisuja projektien tietoturvallisuuden parantamisessa. Haastateltavat korostivat myös koulutuksen ja osaamisen merkitystä

osana parempaa tietoturvariskien tunnistusta. Tavoitteena on, että työntekijöillä on riittävän hyvä ymmärrys tietoturvariskeistä, niihin varautumisesta ja riskienhallintaprosessin kulusta.

5 Tutkimuksen johtopäätökset ja yhteenveto

Tässä luvussa esitetään yhteenveto tutkimuksessa saaduista tuloksista. Tutkimuksen tavoitteena oli selvittää, löytyykö Huld Oy:n aiemmista asiakasprojekteista tietoturvariskeihin liittyviä riski-indikaattoreita ja mitä nämä indikaattorit ovat. Lisäksi selvitettiin tutkimuksessa haastateltujen henkilöiden näkemyksiä hyvistä käytännöistä ja työkaluista, joita voitaisiin hyödyntää tietoturvariskienhallinnassa. Tutkimus toteutettiin laadullisena tapaustutkimuksena, jossa keskeisin tietoaineisto kerättiin puolistrukturoiduilla haastatteluilla.

5.1 Yhteenveto

Tutkimuksessa pyrittiin keräämään haastatteluilla havaintoja mahdollisista riski-indikaattoreista. Tapaustutkimus soveltui tähän tutkimukseen hyvin, sillä se mahdollistaa erilaisten aineistojen käytön tutkimusmateriaalina ja auttaa ymmärtämään tutkittavaa ilmiötä. Tutkimuksen tavoitteena ei ollut tuottaa numeerista dataa indikaattoreista vaan ymmärtää, löytää ja nimetä indikaattorit, jolloin laadullinen tapaustutkimus valikoitui tutkimusmenetelmäksi. Tutkimuksen kulku oli johdonmukaista.

Tutkimuksen alussa esitettiin yksi tutkimuskysymys ja kaksi alakysymystä. Seuraavissa kappaleissa esitetään lyhyt yhteenveto tutkimuskysymyksittäin.

Mitä tietoturvariskien indikaattoreita projekteista voidaan tunnistaa?

Aineistosta muodostetut indikaattorit jaoteltiin teknisiin ja inhimillisiin. Aineistosta voitiin tehdä havainto, että inhimillisistä syistä realisoituneet tietoturvariskit olivat teknisistä syistä johtuneita riskejä yleisempiä. Inhimillisten syiden taustalla vaikuttivat olevan osaamattomuudesta johtuneet virheet (unohdukset, käyttäjävirheet), joihin voidaan vaikuttaa kouluttamisella. Inhimillisistä syistä tulee kuitenkin huomata, että niihin vaikuttaneet tekijät voivat olla hyvin moninaisia. Näin ollen tässä tutkimuksessa tehdyt päätelmät riskin realisoitumisen syistä ja riskiä mittaavista indikaattoreista eivät ole täydellisiä.

Myös teknisiin syihin liittyviä indikaattoreita havaittiin aineistosta, mutta ne eivät olleet yhtä yleisiä riskin realisoitumiseen johtaneita syitä. Teknisistä indikaattoreista havaittiin joitain yhtäläisyyksiä (ks. taulukko 2, indikaattori 1) aikaisemmissa tutkimuksessa tehtyihin havaintoihin.

Miten havaittuja indikaattoreita voidaan hyödyntää projektien tietoturvariskien hallinnassa?

Havaittuja indikaattoreita voidaan hyödyntää yhtenä lisätyökaluna projektiriskienhallinnassa. Indikaattoreista voidaan muodostaa esimerkiksi oma lista, jota verrataan käynnissä olevaan projektiin. Listasta voidaan poimia soveltuvat

indikaattorit projektien tietoturvariskien seuraamiseen. Tämä mahdollistaa yksittäisen riskin seuraamiseen suuremmalla tarkkuudella, mikäli indikaattorit ovat määritetty riittävän tarkoiksi riskin seurantaan.

Mitkä käytännön työkalut tai menetelmät olivat haastateltavien mielestä toimivia tietoturvallisuuden riskienhallinnassa?

Haastateltavat mainitsevat erilaisten tarkastuslistojen olleen toimivia, sillä ne tarjoavat selkeän seurattavan prosessin riskienhallintaan. Haastateltavat kertoivat kaipaavansa yhä monimutkaistuvassa projektiympäristössä laajaa ja reaaliaikaista tilannekuvaa projektin tilanteesta sekä eri asioiden välisistä yhteyksistä. Kompleksisissa projekteissa tilannekuva katoaa herkästi, mikä voi altistaa useille riskeille.

Tekniseen tietoturvariskienhallintaan haastateltavat mainitsivat koodikatselmointien ja uhkamallinnuksen osoittautuneen toimiviksi työkaluiksi. Lopuksi voidaan todeta, että monet haastateltavista totesivat koulutuksen ja sitä myötä kehittyvän osaamisen olevan tärkein apuväline tietoturvariskienhallinnassa.

5.2 Tutkimuksen rajoitteet

Tutkimuksia arvioidaan usein reliabiliteetin (tutkimuksen toistettavuus) ja validiteetin (tutkimusmenetelmän kyky mitata tutkittavaa asiaa tai ilmiötä) käsitteiden mukaan. Tuomen & Sarajärven (2018) mukaan nämä käsitteet eivät sovellu kovin hyvin laadullisen tutkimuksen arviointiin. Heidän mukaansa laadullisen tutkimuksen arviointiin soveltuvat paremmin muun muassa seuraavat asiat: tutkimuksen kohde ja tarkoitus (tutkittava ilmiö ja miksi sitä tutkitaan), tutkijan oma sitoumus tutkimukseen (miksi tutkija pitää aihetta tärkeänä, tutkijan ennakko-oletukset), aineiston keruu (aineistonkeruumenetelmä – ja tekniikka, aineistoon keräämiseen liittyneet erityispiirteet), aineiston analyysi ja tutkimuksen raportointi (Sarajärvi ym., 2018).

Tähän tutkimukseen kohdistui joitakin rajoitteita, jotka ovat voineet vaikuttaa tutkimukseen. Merkittävimmät rajoitteet kohdistuivat haastateltaviin, laadulliseen tapaustutkimukseen, aikaisempaan aiheesta tehtyyn tutkimukseen ja tutkijaan itseensä. Haastateltavien osalta mahdollisina rajoitteina voidaan nähdä haastattelutilanne, joka on luonteeltaan keinotekoinen. Haastateltava voi kokea olevansa tarkkailtavana haastattelun aikana, mikä voi vaikuttaa haastateltavan antamiin vastauksiin. Tällöin materiaalista voi jäädä puuttumaan jotain tai haastateltavan lausunto voi olla erilainen verrattuna asian todelliseen tilaan. Haastatteluihin liittyy myös aina kielellisen tulkinnan osuus, joka voi aiheuttaa virheellisiä tulkintoja. Toisaalta voidaan mainita, että haastateltavat olivat hyvin yhteistyökykyisiä ja kokeneita työtehtävissään, haastatteluissa nämä seikat ilmenivät hyvänä ilmapiirinä ja avoimena keskusteluna.

Tutkimuksessa käytetyn laadullisen tapaustutkimuksen rajoitteena voidaan nähdä rajallinen tutkimusotanta, josta seuraa haasteita aineiston laajemman

yleistämisen osalta. Tässä muodossaan tutkimus vastaa luotettavimmin tilaaja-organisaatiolta kerättyihin tapauksiin, mutta tutkimus ei ole välttämättä yleistettävissä muihin tapauksiin tai organisaatioihin. Laadullisen tutkimuksen puutteista huolimatta laadullinen tapaustutkimus oli soveltuvin tutkimustapa, sillä se mahdollisti uuden tiedon keräämisen aiheesta ja tutkimukseen voitiin hyödyntää useita erilaisia aineistoja. Merkittävimmän aineiston tässä tutkimuksessa muodostivat haastattelut, joita on mahdollista analysoida syvällisesti laadullisella tapaustutkimuksella. Tavoitteena oli myös ymmärtää tutkittavaa ilmiötä ja nimetä tunnistetut indikaattorit, ei tuottaa määrällistä dataa tutkittavasta ilmiöstä.

Aikaisemman tutkimuksen merkittävin rajoite oli vähäinen aikaisempi tutkimustieto. Lukuun ottamatta muutamaa aiheeseen liittyvää tutkimusta materiaalia oli haastava löytää tämän tutkimuksen tueksi. Vähäinen aikaisempi materiaali voi vaikuttaa siihen, että tutkimuksessa saadut tulokset ja niistä tehdyt johtopäätökset eivät ole täsmällisiä. Tulosten mahdollinen epämääräisyys voi edelleen vaikuttaa tutkimuksen yleistettävyyteen heikentävästi.

Tutkijan osalta rajoitteina voidaan pitää kokemattomuutta ja ammattitaitoa tutkijana, sillä tämä on tutkijan ensimmäinen laajempi tutkimus. Näiden seikkojen lisäksi tutkimuksessa käytetyn materiaalin analysointi ja materiaalista saadut tulokset perustuvat pitkälti tutkijan omaan tulkintaan, mikä voi johtaa yksipuolisiin johtopäätöksiin ja tuloksiin. Eskolan & Suorannan (1998) mukaan aineiston tulkinnan luotettavuutta voidaan parantaa hyödyntämällä useampaa havainnoitsijaa. Tähän pyrittiin käyttämällä tutkittavaa materiaalia ja esitettyjä johtopäätöksiä tilaajaorganisaation edustajalla sekä käyttämällä mahdollisimman monipuolisia lähteitä näkökulman laajentamiseksi.

6 Pohdinta

Tutkimuksen lähtökohtana oli tarkastella Huld Oy:n aiemmissa asiakasprojekteissa realisoituneita tietoturvariskejä ja pyrkiä tunnistamaan niistä riski-indikaattoreita, jotka seuraavat riskin kehittymistä projektin aikana. Tutkimuksessa havaittiin, että aiemmissa projekteissa realisoituneet tietoturvariskit johtuivat useammin inhimillisistä virheistä kuin teknisten ratkaisujen vikaantumisesta. Myös teknisiä indikaattoreita kuitenkin havaittiin. Teknisiin riskeihin liittyvät indikaattorit olivat suurilta osin yhteneväisiä aiempien tutkimusten havaintojen kanssa (Özçakmak, 2019; Saluja ym., 2014).

Inhimillisten riskien suuri osuus oli tutkimuksen kannalta kiinnostava löytö, sillä aiemmat aiheeseen liittyneet tutkimukset (Özçakmak, 2019; Saluja ym., 2014) olivat keskittyneet lähinnä teknisiin riskeihin liittyviin indikaattoreihin. Inhimilliset syyt olivat esillä myös aiemmissa aiheeseen liittyvissä tutkimuksissa, mutta aiemmat tutkimukset painottivat selkeästi enemmän tietoturvallisuuteen liittyviä teknisiä riskejä. Taulukoita 2 ja 3 tarkastellessa tämä ero ei käy ilmi, sillä taulukoihin on tuotu havaintoja myös aiemmista tutkimuksista. Kuitenkin haastattelut tukivat havaintoa, jonka mukaan inhimillisistä syistä realisoituneet tietoturvariskit olivat huomattavasti tyypillisempiä kuin teknisistä ratkaisuista johtuneet riskit.

Inhimillinen puoli painottui enemmän tässä tutkimuksessa kenties siksi, että useat tutkimuksessa käsitellyt projektit olivat turvallisuuskriittisiä. Turvallisuuskriittisten projektien kohdalla tietoturvariskit otetaan todella kattavasti huomioon, jolloin realisoituneet tietoturvariskit voivat olla erilaisia verrattuna muihin tilanteisiin tai projekteihin. Turvallisuuskriittisissä projekteissa järjestelmien ja teknisten ratkaisujen turvallisuus sekä niihin kohdistuvat uhat ovat usein kattavan tarkastelun kohteena, mutta inhimillistä puolta ei välttämättä oteta huomioon yhtä kattavasti tai sitä ei osata huomioida yhtä hyvin. Tämä ei kuitenkaan tarkoita inhimillisten tekijöiden huomiotta jättämistä, sillä haastateltavat kertoivat myös inhimillisten syiden kuuluneen projektin riskiarvioon. Inhimillisten virheiden mahdollisuus kasvaa turvallisuuskriittisissä projekteissa, joissa sallittu toiminta on tarkemmin säädeltyä ja virheet voivat tapahtua herkemmin. Riskien suuri määrä vaikeuttaa niihin varautumista entisestään, erityisesti inhimillisten virheiden osalta.

Inhimillisiin syihin liittyviä indikaattoreita oli haastava muodostaa, sillä inhimilliseen virheeseen liittyneet seikat voivat olla hyvin moninaisia. Aiemman tutkimuksen perusteella voitiin kuitenkin todeta, että usein inhimillisen virheen taustalla on henkilön osaamattomuus tai tietämättömyys, joka johtuu puutteellisesta perehdytyksestä tai koulutuksesta. Henkilöstön osaamisen kehittämiseen liittyvät toimenpiteet sekä käyttäjien kouluttaminen ja heidän osallistamisensa riskienhallintaan ovat toimivia ratkaisuja riskien realisoitumisen välttämiseksi (Merete Hagen ym., 2008; Spears & Barki, 2010). Inhimillisten syiden tarkempi ymmärtäminen vaatii jatkotutkimusta.

Tutkimusta tehtäessä oli kohtuullisen haastavaa löytää aiempaa tutkimusta liittyen tietoturvariskien indikaattoreihin. Aihetta on tutkittu sangen vähän aiemmin, vaikka harvat aiemmat tutkimukset (Özçakmak, 2019) ovat todenneet indikaattorien hyödyntämisen olevan mahdollista myös tietoturva-alalla. Varsinaista syytä indikaattorien käyttämisen puutteelle ei löytynyt. Tähän vaikuttaa kenties se, että indikaattorien hyödyntäminen tietoturva-alalla on ajatuksena melko uusi, jolloin niiden toimivuudesta, määrittämisestä ja käytöstä ei ole kokemuksia. Prosessina indikaattoreiden määrittäminen on työlästä, sillä mahdollisimman tehokkaita ja tarkkoja indikaattoreita kyetään määrittämään vain tarkalla taustatyöllä, mikä tarkoittaa suuren tietomäärän läpikäyntiä ja haarukointia. Indikaattoreiden tulee ennustaa luotettavasti vallitsevan tilanteen kehittymistä, olla helposti mitattavissa ja ymmärrettävissä. Lisäksi indikaattoreiden raja-arvojen määrittäminen vaatii huolellisuutta, jotta indikaattoreille määritetyt rajat eivät anna valheellista kuvaa riskin kehittymisestä.

Tämä tutkimus tarjoaa indikaattoreita tietoturvallisuuden riskienhallinnan parantamiseksi. Tutkimus täydentää aiempaa tietoturvariskien indikaattoreista tehtyä tutkimusta ja osoittaa, että erityisesti tietoturvariskien indikaattoreita ja riskien realisoitumiseen liittyviä inhimillisiä tekijöitä on tutkittu rajallisesti. Tämä tutkimus ja siinä saadut tulokset täyttävät osaltaan tätä vajetta.

6.1 Tutkimuksen käytännöllinen merkitys

Tässä ja aiemmissa tutkimuksissa havaittuja indikaattoreita voitaisiin hyödyntää yhtenä lisätyökaluna projektien riskienhallinnassa. Riskeihin varautuminen on haastavaa, eikä kaikkiin riskeihin voida varautua hyödyntämällä samoja työkaluja. Indikaattoreiden käyttö osana riskienhallintaa voisi parhaassa tapauksessa tarjota keinon seurata yksittäistä riskiä ja sen kehittymistä tarkasti, mikä helpottaisi riskiin varautumista tai siihen reagoimista. Riski-indikaattoreiden raja-arvojen seuranta voitaisiin tuoda luontevaksi osaksi organisaatioiden projektiriskienhallintaa ja projektipalaveria, jossa riskitilannetta seurataan ja päivitetään.

Tutkimus osoitti, että inhimillisiä riskejä ei ollut tyypillisesti osattu ottaa huomioon riskejä arvioitaessa tai inhimillinen riski oli arvioitu todellisuutta pienemmäksi. Inhimillisiin tekijöihin tuleekin kiinnittää nykyistä enemmän huomiota, sillä inhimilliset tekijät ovat usein merkittäviä projektien onnistumisen kannalta. Tutkimuksessa ilmeni, että usein inhimilliset virheet johtuivat osaamattomuudesta. Osaamattomuutta voidaan ehkäistä henkilöstön ajantasaisella koulutuksella ja osaamisen kartoittamisella.

6.2 Jatkotutkimus

Jatkotutkimuksissa olisi hyödyllistä selvittää tarkemmin, mitkä inhimilliset syyt vaikuttavat tietoturvariskien realisoitumiseen ja kuinka inhimilliset virheet saadaan siirrettyä mitattaviksi indikaattoreiksi. Toisena mahdollisena jatkotutkimusaiheena voitaisiin tutkia indikaattoreiden raja-arvojen määrittämistä ja siihen käytettävää prosessia, sillä tässä tutkimuksessa indikaattoreille ei määritetty raja-arvoja. Myös indikaattorien vienti osaksi projektia ja niiden seuraaminen projektin aikana toimisi loogisena jatkotutkimuksena.

LÄHTEET

Al-Ahmad, W., & Mohammed, B. (2015). A code of practice for effective information security risk management using COBIT 5. In *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)* (pp. 145-151). IEEE. Viitattu 31.03.2020.

Alasuutari, P. & Alasuutari, P. (2012). Laadullinen tutkimus 2.0. Tampere: Vastapaino. Viitattu 01.04.2020.

Anthony (Tony)Cox, L. (2008). What's Wrong with Risk Matrices? Risk Analysis, 28(2), pp. 497-512. doi:10.1111/j.1539-6924.2008.01030.x. Viitattu 18.03.2020.

Antonucci, D. (2017). The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities.

Artto, K. A., Kujala, J., Martinsuo, M. & Sinivuori, E. (2006). *Projektiliiketoiminta*. Helsinki: WSOY. Viitattu 26.03.2020.

Australian Government. (2016). Deparment of Finance. Understanding and Developing Key Risk Indicators. Viitattu 24.03.2020.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *The Journal of Systems & Software, 81*(12), pp. 2118-2133. doi:10.1016/j.jss.2008.03.059. Viitattu 18.03.2020.

Benbasat, I., Goldstein D. & Mead M. (1987). The Case Research Strategy in Studies of Information Systems. MIS Quarterly, 11(3), 369-386. Viitattu 02.03.2020.

Berg, H. P. (2010). Risk management: procedures, methods and experiences. *Reliability: Theory & Applications*, *5*(2 (17)). Viitatti 24.03.2020.

Bloom, B. & Crabtree B.F. (2006). The qualitative research interview. Medical Education 2006. 40: 314–321. Viitattu 06.04.2020.

Committee on National Security Systems, Committee on National Security Systems (CNSS) Glossary, CNSS Instruction (CNSSI) 4009, April 6, 2015. Viitattu 25.03.2020.

Darke, P., Shanks, G. & Broadbent, M. (1998). Successfully completing case study research: Combining rigour, relevance and pragmatism. Information Systems Journal, 8(4), pp. 273-289. Viitattu 02.03.2020.

Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). Key risk indicators–their role in operational risk management and measurement. ARM and RiskBusiness International, Prague, 1-32. Viitattu 13.03.2020.

Eisenhardt, K. M. & Graebner, M. E. (2007). Theory Building from Cases: Opportunities and Challenges. The Academy of Management Journal, 50(1), pp. 25-32. Viitattu 02.03.2020.

Eriksson, P. & Koistinen, K. (2014). Monenlainen tapaustutkimus. Kuluttajatutkimuskeskuksen tutkimuksia ja selvityksiä 11. Viitattu 06.04.2020.

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

Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security, 22*(5), pp. 410-430. doi:10.1108/IMCS-07-2013-0053. Viitattu 02.04.2020.

Galvanize. (2019). KRI Basics for IT Governance – How Information Technology & Information Security can Implement This Crucial Part of Risk Management. Viitattu 20.03.2020.

Gordon, L.A. and Loeb, M.P. (2002). Return on Information Security Investments, Myths vs Realities, Strategic Finance 84(5): 26–31. Viitattu 19.03.2020.

Harris, S. (2013). CISSP All-in-One Exam Guide, Sixth Edition. Viitattu 31.03.2020.

Hughes, P. & Ferret, E. (2007). Introduction to Health and Safety in Construction. 3rd Ed., Elsevier Ltd., Oxford, UK. Viitattu 10.06.2020.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. (2013). Johda riskejä: Käytännön opas yrityksen riskienhallintaan. [Helsinki]: Finva Finanssi- ja vakuutuskustannus.

ISO/IEC 27005:2018. (2018). Information Technology – Security Techniques – Information Risk Management.

Kraemer, S., Carayon, P. & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), pp. 509-520. doi:10.1016/j.cose.2009.04.006. Viitattu 10.06.2020.

Malmén, Y. & Wessberg, N. (2004). Mitä tarkoitetaan riskillä, riskianalyysillä, riskin arvioinnilla ja riskienhallinnalla? Teknologian tutkimuskeskus VTT Oy. Viitattu 17.03.2020.

Matruglio, P. & Tymmons, B. (2014). Key risk indicators. Viitattu 24.02.2020.

Merete Hagen, J., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), pp. 377-397. doi:10.1108/09685220810908796. Viitattu 02.04.2020.

Niemi, P. (2018). Sisäinen tarkastus käytännössä (1. painos.). [Helsinki]: Alma. Viitattu 26.03.2020.

NIST. (2011). NIST Special Publication 800-39. Managing information security risk. Organization, Mission and Information System view. Viitattu 18.03.2020.

NIST. (2012). NIST Special Publication 800-30. Guide for Conducting Risk Assessments. Information Security. Viitattu 24.03.2020.

NVD. (2020). Vulnerability metrics. Viitattu 02.09.2020.

Raggad, B. G. (2010). *Information security management: Concepts and practice*. Boca Raton, Florida ; London, [England] ; New York: CRC Press. Viitattu 25.03.2020.

Ruusuvuori, J., Nikander, P. & Hyvärinen, M. (2010). *Haastattelun analyysi*. Tampere: Vastapaino. Viitattu 07.04.2020.

Sabău-Popa, D., Bradea, I., Boloș, M., & Delcea, C. (2015). The information confidentiality and cyber security in medical institutions. Annals of the University of Oradea: Economic Science Series, 24, 95-96. Viitattu 13.03.2020.

Salmela, H. (2007). Analysing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology, 23*(3), p. 185. doi:10.1057/palgrave.jit.2000122. Viitattu 02.04.2020.

Saluja, U., & Idris, N. B. Risk Indicators for Information Security Risk Identification. International Journal of Computer Science and Network, Volume 3, Issue 5, October 2014. Viitattu 20.03.2020.

Sanastokeskus TSK. (2004). TSK 31. Tiivis tietoturvasanasto. Viitattu 18.03.2020.

Scarlat, E., Chirita, N., & Bradea, I. A. (2012). Indicators and metrics used in the enterprise risk management (ERM). *Economic Computation and Economic Cybernetics Studies and Research Journal*, *46*(4), 5-18.

Spears, J., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 503-522. doi:10.2307/25750689. Viitattu 02.04.2020.

Straub, D. W. & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making.(includes appendix). MIS Quarterly, 22(4), p. 441. doi:10.2307/249551. Viitattu 19.03.2020.

Suomen standardoimisliitto SFS ry. (2018). Riskit hallintaan – SFS-ISO 31000:2018. Viitattu 17.03.2020.

Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä. ISSN=1797-2957. 2019, 7. Tietoturva . Helsinki: Tilastokeskus. Viitattu 06.08.2020.

Suominen, A. (2003). Riskienhallinta (3. uud. p.). Helsinki: WSOY.

Thun, J. & Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics, 131*(1), pp. 242-249. doi:10.1016/j.ijpe.2009.10.010. Viitattu 24.03.2020.

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos.). Helsinki: Kustannusosakeyhtiö Tammi. Viitattu 01.04.2020.

Turvallisuuskomitea. (2018). Kyberturvallisuuden sanasto. Viitattu 25.03.2020.

Valtiovarainministeriö. (2008). VAHTI 8/2008. Valtionhallinnon tietoturvasanasto. Viitattu 18.03.2020.

Venter, H. & Eloff, J. (2003). A taxonomy for information security technologies. *Computers & Security, 22*(4), pp. 299-307. doi:10.1016/S0167-4048(03)00406-1

Von Solms, B., & Von Solms, R. (2004b). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. doi: 10.1016/j.cose.2004.05.002. Viitattu 02.04.2020.

Von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*(C), pp. 97-102. doi:10.1016/j.cose.2013.04.004. Viitattu 25.03.2020.

Wallace, L. & Keil, M. (2004). Software project risks and their effect on outcomes. Communications of the ACM, 47(4), pp. 68-73. doi:10.1145/975817.975819. Viitattu 16.03.2020

Westland, J. (2006). The project management lifecycle: A complete step-by-step methodology for initiating, planning, executing and closing a project successfully. London: Kogan Page. Viitattu 31.03.2020.

Wheeler, E. (2011). Security Risk Management : Building an Information Security Risk Management Program From the Ground Up. Syngress. Viitattu 26.03.2020.

Whitman, M.E.; Mattord, H.J. (2009). Principles of information security (3rd ed.), Thompson Course Technology. Viitattu 25.03.2020.

Yin, R. K. (1994). Case study research: Design and methods (2nd ed.). Los Angeles: Sage. Viitattu 06.04.2020.

Özçakmak, F. (2019). *SUPPLEMENTING ISRM MODELS BY KRI IMPLEMENTATION* (Doctoral dissertation, MIDDLE EAST TECHNICAL UNIVERSITY). Viitattu 24.03.2020.

LIITE 1 TUTKIMUSHAASTATTELUN KYSYMYKSET

Aloituskeskustelu

1. Haastateltavan työhistoria?
    a. Kokemus projektityöskentelystä?
2. Tausta riskienhallinnasta ja tietoturvasta?

Tausta ja projektien ominaisuudet

1. Mikä oli projektin kokoluokka ja kohdealue?
2. Mikä oli roolisi projektin suhteen?
3. Mikä oli roolisi projektiriskien arvioinnissa?
4. Miten riskienhallintaa tehtiin projektissa?

Riskit

1. Millaisia tietoturvallisuuteen liittyviä riskejä projektiin kohdistui?
    a. Miten vakavia projektiin kohdistuneet tietoturvariskit olivat?
2. Miten riskit vaikuttivat projektin etenemiseen tai projektityöskentelyyn?
3. Mitkä tekijät vaikuttivat mielestäsi riskin realisoitumiseen?
    a. Oliko realisoitunut riski tunnistettu?
    b. Oliko suojattava kohde, johon riski kohdistui, tunnistettu?
    c. Mikäli käytettiin kvantitatiivisia riskienhallintamenetelmiä, oliko riskiarvio (todennäköisyys ja vaikuttavuus) oikea?
4. Millaisia riskeihin liittyviä varoitusmerkkejä oli havaittavissa (indikaattorit)
    a. Voitko antaa esimerkin, miten tämä käytännössä näkyi projektissa?
5. Mitkä olisivat mielestäsi hyviä käytännön työkaluja, joilla tietoturvallisuuden riskienhallintaa voitaisiin parantaa?