VALTIOVARAINMINISTERIÖ

Digitaalisen turvallisuuden kustannus-vaikuttavuusarviointi julkisessa hallinnossa
Selvitystyön raportti
1.6.2020

Julkisen hallinnon tieto- ja viestintätekninen osasto

Sisällys

1 TIIVISTELMÄ

Selvitys perustuu valtioneuvoston Julkisen hallinnon digitaalisen turvallisuuden periaatepäätökseen 8.4.2020, jossa digitaalisen turvallisuuden kustannus-vaikuttavuuden seuraaminen on yksi kuudesta periaatteesta. Selvitystyö toteutettiin kirjallisuuskatsauksen sekä julkisen hallinnon organisaatioiden edustajien haastatteluiden kautta.

Julkisen hallinnon digitaalisen turvallisuuden kustannukset ja hyödyt eivät pääosin ole tunnistettavissa toiminnan ja talouden suunnitelmista tai raporteista. Tältä osin selvityksen johtopäätökset tukevat aiempien digitaalisen turvallisuuden resurssiselvitysten tuloksia. Kirjanpitoyksiköissä niitä ei pääosin ole erotettu muista tieto- ja viestintätekniikan kustannuksista. Myöskään vaikuttavuuden arviointiin ei ole olemassa yhtenäisiä menetelmiä. Tässä selvityksessä ehdotetaan, että digitaalisen turvallisuuden kustannus-vaikuttavuuden arviointi perustuisi virastojen vuosittain ylläpitämiin riskiarviointeihin sekä toiminnallisiin indikaattoreihin. Riskiarviointeihin sisällytettäisiin jokaisen merkittävän riskin arviointi myös digitaalisen turvallisuuden näkökulmasta kuvaamalla kvantitatiivisesti riskin todennäköisyys ja vaikutus sekä suojaustoimien vaikutuksia riskiin. Tavoitteena on riskianalyysin perusteella kohdistaa digitaalisen turvallisuuden investoinnit olennaisten riskien torjumiseksi. Toiminnallisten indikaattoreiden avulla mitattaisiin tavoitteita, joiden synnyttämiä hyötyjä ei voida arvioida euromääräisesti. Ehdotuksen tarkoituksena on saada aikaan digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyvöittäminen. Ehdotuksen tarkentaminen sekä soveltaminen virastoissa ovat tätä selvitystyötä seuraavia tehtäviä.

Raportti on valmisteltu selvitystyöryhmässä, jossa ovat toimineet suunnittelija Jani Pyrrö ja tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä. Työtä ovat kommentoineet valtiovarainministeriön palveluiden ja turvallisuuden ohjausyksikön asiantuntijat sekä KPMG:n konsultit Mikaiiro Laitinen ja Jasmiina Rousu.

2 JOHDANTO

Tässä julkisen hallinnon digitaalisen turvallisuuden kustannus-vaikuttavuusarviointia käsittelevässä raportissa tarkastellaan digitaalisen turvallisuuden kustannuksia ja hyötyjä sekä teorian että empiirisen selvityksen avulla.

Julkisen hallinnon digitaaliseen turvallisuuteen liittyvässä arvioinnissa on otettava huomioon laajasti erilaisia poliittisia ja sosioekonomisia kysymyksiä, joiden johdosta kustannus-hyötyarviointiin tulee sisällyttää sekä kvantitatiivisia että laadullisia tekijöitä. Toisin sanoen digitaalisen turvallisuuden vaikuttavuutta ja kustannuksia on arvioitava kokonaisvaltaisesti koko yhteiskunnan tasolla (Adar, Blobner, Hutter & Pettersen 2012, 2). Selvitystyön tuloksena on muodostettu ehdotus digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arvioinnin kehittämiseksi julkisessa hallinnossa.

Johdanto –kappaleessa kuvataan selvitystyön lähtökohdat, tavoitteet sekä menetelmät. Tämän jälkeen esitetään selvityksen yhteydessä tunnistamiamme kustannus-vaikuttavuusarviointiin liittyviä haasteita ja arvioinnin kannalta keskeisiä tekijöitä. Neljännen kappaleen kirjallisuuskatsauksen kautta tarkastellaan tutkimuksissa esitettyjä digitaalisen turvallisuuden kustannus-vaikuttavuusarviointimalleja. Raportin viidennessä kappaleessa kuvataan digitaalisen turvallisuuden kustannus-vaikuttavuusarvioinnin nykytilaa julkisessa hallinnossa haastattelututkimukseen perustuen. Kuudennessa kappaleessa kuvataan ehdotus julkisen hallinnon digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arviointiin. Seitsemännessä kappaleessa on selvitystyön kautta saavutetut johtopäätökset.

2.1 Selvityksen tavoitteet ja menetelmät

Selvityksen tavoitteena on kartoittaa digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arvioinnin nykytilaa julkisessa hallinnossa, sekä laatia haastatteluiden ja aiempien tutkimusten pohjalta digitaalisen turvallisuuden kustannus-vaikuttavuusmalliehdotus. Selvityksen lähtökohtana on valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta 8.4.2020 (Valtiovarainministeriö 2020a, 13). Siinä digitaalisen turvallisuuden kustannus-vaikuttavuuden seuraaminen on asetettu yhdeksi julkisen hallinnon digitaalisen turvallisuuden kehittämisen kuudesta periaatteesta. Periaatepäätöksen linjausten toimeenpanemiseksi on laadittu Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka) (Valtiovarainministeriö 2020b). Siinä on kuvattu 19 tehtävää. Selvitystehtävä on osa seuraavaa tehtävää:

”Valtiovarainministeriö yhdessä digi- ja väestötietoviraston kanssa laatii digitaalisen turvallisuuden vaikuttavuus-/kustannusmallin ja prosessin. Suunnitellaan digitaalisen turvallisuuden hallinnan ja kehittämisen vaikuttavuuden ja kustannusten arviointi valtion hallinnossa ja kunnissa. Tavoite on se, että julkinen hallinto panostaisi digitaaliseen turvallisuuteen määrärahalla joka vastaa viittä prosenttia ICT-menoista. Mallia pilotoidaan ja pilotoinnin kokemusten perusteella päivitetty malli otetaan käyttöön vuonna 2021. Malli otetaan soveltuvin osin käyttöön osana digi- ja väestötietoviraston kokonaiskuvapalvelua” (Valtiovarainministeriö 2020b, 16).

Nykytilan kartoittamiseksi selvitystyön yhteydessä toteutettiin puolistrukturoituja haastatteluita valtiohallinnossa ja kunnissa. Haastatteluissa pyrittiin kattamaan kaikki ennalta määritetyt kysymykset, jotka toimivat lähtökohtina jatkokysymyksille. Haastatteluihin osallistui kymmenen julkisen hallinnon organisaatiota. Haastatteluihin osallistuneet henkilöt ja haastattelukysymykset ovat listat-

tuina liitteissä 1 ja 2. Haastatteluiden avulla kartoitettiin digitaalisen turvallisuuden kustannus-vaikuttavuusarvioinnin nykytilaa, selvitettiin perusteita nykyisille käytänteille sekä haettiin näkemyksiä keskeisimmistä kehityskohteista.

Selvityksessä laadittiin myös kirjallisuuskatsaus digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arviointiin käytetyistä lähestymistavoista. Riskiarviointiin perustuvaa kustannus-hyötyanalyysiä on laajasti tehty esimerkiksi paloturvallisuuden ja tulvariskien hallinnan toimenpiteiden osalta1. Haastattelujen ja kirjallisuuskatsauksen perusteella laadittiin riskianalyysipohjainen ehdotus myös digitaalisen turvallisuuden kustannus-vaikuttavuuden arviointiin.

2.2 Julkisen hallinnon digitaalinen toimintaympäristö

Suomen kaltaiset tietoyhteiskunnat ovat yhä voimakkaasti etenevän digitalisoitumisen seurauksena riippuvaisia digitaalisista järjestelmistä ja tietoverkoista, jotka ovat tulleet kiinteäksi osaksi kansalaisten elämää ja yhteiskunnan toimintaa. Digitalisaation mahdollistavat uudet toimintatavat ja hyödykkeet toimivat suurena talouskasvun lähteenä tietoyhteiskunnassa.

Digitalisaatio tuottaa suuria taloudellisia hyötyjä, ja samanaikaisesti digitaalisen turvallisuuden merkitys kasvaa (Juuso ja Svento 2018, 191; Haapamäki & Sihvonen 2019, 811). Yhteiskunnan digitaalisessa toimintaympäristössä fyysinen ja digitaalinen maailma kietoutuvat tiiviisti toisiinsa, kun tietotekniikka ja digitaaliset ohjausjärjestelmät vastaavat yhteiskunnan jokapäiväisten ja kriittisten toimintojen ohjaamisesta. Tämän kehityksen seurauksena sekä kansalaisten sujuvan arjen että julkisen hallinnon toiminnan kannalta kriittisen infrastruktuurin, tietovarannot ja toimintaympäristöt altistuvat digitaalisen turvallisuuden riskeille (Haapamäki & Sihvonen 2019, 809). Esimerkkinä tietovarantoihin liitty-

[1] Esimerkiksi Zhang (2016) ja Lamothe & Görlach (2005).

västä riskistä on, että vuonna 2016 Euroopan Unionin jäsenvaltioissa raportoitiin 1,1 miljardia tietoturvaloukkausten yhteydessä vuotanutta tai tuhoutunutta henkilötietoa (ISTR 2017). Yhteiskunnan toiminnan riippuvuus tietoverkkoihin kytketyistä kriittisen infrastruktuurin osista, kuten vesihuolto-, vaali- ja maksuliikennejärjestelmistä, asettaa suuria vaatimuksia digitaaliselle turvallisuudelle. Näin ollen on yhä tärkeämpää varmistaa, että julkisen hallinnon digitaalisen toimintaympäristön turvallisuus on vahvalla tasolla.

Julkisen hallinnon organisaatiot sekä valtionhallinnossa että kunnissa vastaavat toimintansa turvaamiseksi tarvittavan digitaalisen turvallisuuden kustannuksista ja suojaustoimien riittävyydestä. Digitaaliseen turvallisuuteen panostettujen resurssien vaikuttavuuden ja tarkoituksenmukaisuuden arviointi on näin ollen virastokohtaista. Digitaalisista järjestelmistä riippuvaisen yhteiskunnan voimakkaan verkottuneisuuden vuoksi erityisesti kriittisiin järjestelmiin kohdistuvat turvallisuuspoikkeamat voivat potentiaalisesti lamauttaa organisaation toiminnan, jolloin riskin toteutumisen vaikutukset ulottuvat kuitenkin laajasti koko yhteiskuntaan (Haapamäki & Sihvonen 2019, 811). Tämä tarkoittaa käytännössä sitä, että vaikka digitaalisen turvallisuuden kustannukset ovat pääosin yksittäisten virastojen vastuulla, niin turvallisuudesta hyötyy koko yhteiskunta.

Ulkoisvaikutukset ovatkin keskeinen syy sille, että organisaatiot usein investoivat liian vähän digitaaliseen turvallisuuteen yhteiskunnan kokonaisedun näkökulmasta (Juuso ja Svento 2018, 195; Anderson ja Moore 2006, 611). Ulkoisvaikutuksilla tarkoitetaan toiminnan vaikutuksia, jotka kohdistuvat organisaation ulkopuolelle. Turvallisuus synnyttää positiivisia ulkoisvaikutuksia. Kaikki turvallisuuspanostuksista syntyvät hyödyt eivät siis kohdistu organisaatiolle itselleen. Näin ollen julkisen hallinnon digitaalisen turvallisuuden kustannus-vaikuttavuuslaskelmissa on huomioitava laajasti riskien toteutumisesta aiheutuvat yhteiskunnalliset vaikutukset, eivätkä ne voi rajoittua vain yksittäisen organisaation sisäisiin kustannuksiin ja hyötyihin. Tieto- ja viestintäteknisen palvelu-

tuotannon keskittäminen kunnissa, kuntayhtymissä ja valtion hallinnossa on lisännyt julkisen hallinnon toimijoiden verkottuneisuutta ja näin ollen myös mahdollisen riskin toteutumisesta aiheutuvia kerrannaisvaikutuksia.

Yhä enemmän taloudellisesti hyödynnettäviä resursseja siirtyy digitaaliseen ympäristöön, ja tämän seurauksena riskialtistuksen pinta-ala kasvaa. Esimerkiksi sosiaali- ja terveydenhuollon sektorilla Suomessa palveluiden toteuttamiseen sekä kansalaisten terveystietojen hallintaan hyödynnetään laajasti digitaalisia järjestelmiä jotka ovat integroituneet kuntien tietoteknisiin palveluihin. Digitaalisen teknologian laaja hyödyntäminen sosiaali- ja terveydenhuollossa on lisännyt digitaaliseen turvallisuuteen liittyviä haasteita toimialalla (Vuorinen 2019, 13). Digitaalisiin järjestelmiin tukeutuvan terveydenhuollon potilasturvallisuus on suoraan riippuvaista digitaalisesta turvallisuudesta. Kriittisten hoitojärjestelmien lisäksi digitaalisiin tietovarantoihin kohdistuvat poikkeamat voivat vaikuttaa esimerkiksi potilastietojen ja laboratoriotestien tulosten luotettavuuteen, eheyteen sekä saatavuuteen. Ison-Britannian julkinen terveydenhuoltojärjestelmä National Health Service (NHS) joutui vuonna 2017 vakavan tietoturvaloukkauksen kohteeksi. *WannaCry*-kiristysohjelma hyödynsi käyttöjärjestelmän tiedossa olevaa haavoittuvuutta, ja hyökkäyksestä aiheutui NHS:lle jopa 48,8 miljoonan Englannin punnan suuruiset suorat taloudelliset menetykset (Ghafur, Kristensen, Honeyford, Martin, Darzi & Aylin 2019, 2).

Digitaalisen turvallisuuden keskeinen rooli yhteiskunnassa asettaa vaatimuksia sekä julkisen hallinnon, yksityisen sektorin että kansalaisten toiminnalle. Digitaaliseen toimintaympäristöön kohdistuvien riskien potentiaalisesti aiheuttamat menetykset kasvavat samalla kun digitaaliseen toimintaympäristöön integroitu arvo lisääntyy.

3 DIGITAALISEN TURVALLISUUDEN KUSTANNUS-VAIKUTTAVUUDEN ARVIOINTIA KÄSITTELEVÄ KIRJALLISUUS

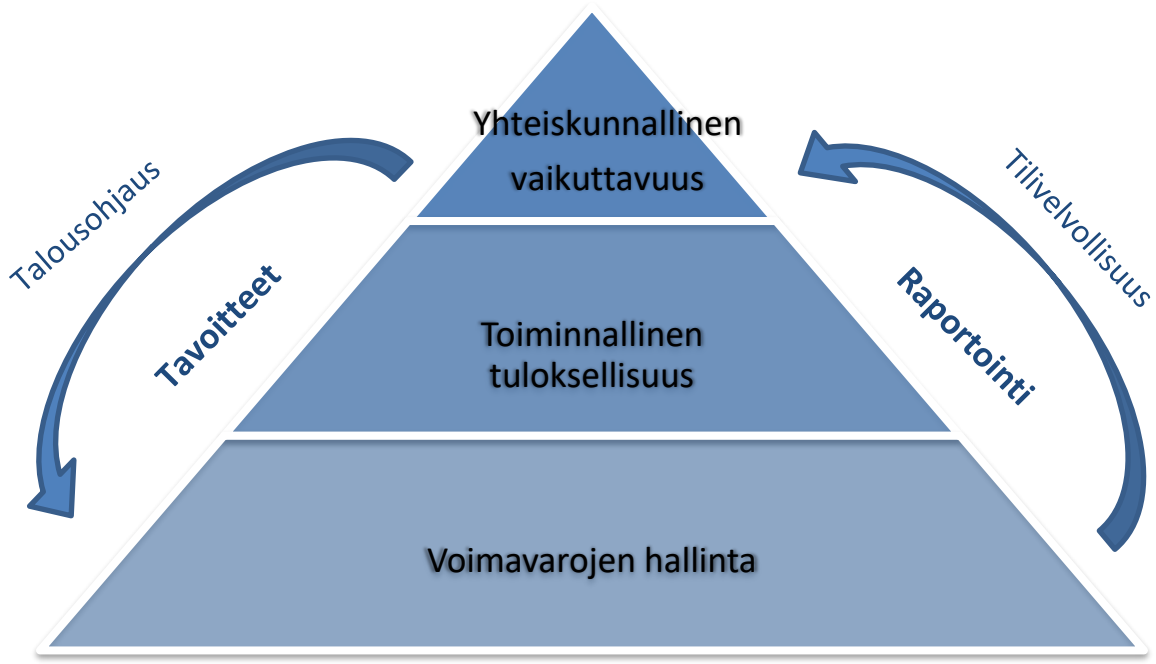
3.1 Lähtökohdat

Eurooppalaisen hallintotavan valkoisessa kirjassa tehokkuus mainitaan yhtenä hyvän hallintotavan viidestä periaatteesta (Euroopan komissio 2011). Tehokkuudella tarkoitetaan osaltaan taloudellista tehokkuutta, eli julkisten varojen järkevää käyttöä, jossa huomioidaan toiminnan tuottamien kustannusten ja yhteiskunnallisten hyötyjen suhde. Julkisilta toimijoilta siis edellytetään toiminnan tehokkuutta, joka taas edellyttää toiminnan kustannus-vaikuttavuuden arviointia ja punnintaa.

Digitaaliseen turvallisuuteen käytettyjen julkisten varojen arvioidaan olevan jatkuvassa kasvussa. Esimerkiksi Yhdysvaltain liittovaltion hallitus budjetoi vuonna 2019 noin 21 miljardia Yhdysvaltain dollaria digitaaliseen turvallisuuteen. Euroopan Unionin (EU) ja sen jäsenvaltioiden osalta tarkkoja tietoja ei ole käytettävissä, mutta kustannusten arvioidaan olevan pienempiä kuin Yhdysvalloissa (Euroopan Unioni 2019, 22). Tilastotietoportaali Statista on kerännyt informaatiota digitaaliseen turvallisuuteen käytetyistä resursseista suhteessa tietotekniikan kokonaiskustannuksiin. Informaatio on kerätty kansainvälisillä kyselytutkimuksilla, joihin on vastannut tuhansia organisaatioita laajasti yhteiskunnan eri sektoreilta vuosina 2005-2017. Tilastojen mukaan digitaalisen turvallisuuden osuus tietotekniikan kokonaiskustannuksista on kasvanut tasaisesti selvityksen ajanjaksolla saavuttaen 10,6 prosentin osuuden vuonna 2017 (Statista 2020).

Hallinnon kehittämisen tueksi tarvitaan analysoitua tietoa eri toimien vaatimista resursseista sekä resursseilla saavutettavasta vaikuttavuudesta. Tiedolla johtaminen tuottaa arvoa julkiselle hallinnolle ja laajemmin yhteiskunnalle, jos sen avulla kyetään tekemään valistuneempia päätöksiä ja vaikuttavampia toimen-

piteitä, sekä suuntaamaan resursseja tarkoituksenmukaisemmin. Valtionhallinnossa 1990-luvun alusta saakka toteutetun tulosohjauksen keskeisimmäksi periaatteeksi on nimetty yhteiskunnallinen vaikuttavuus (Opetusministeriö 2009, 6). Jotta hallinnon vaikutuksia yhteiskunnalliseen hyvinvointiin kyettäisiin osoittamaan, on sitä pyrittävä mittaamaan analysoituun tietoon perustuen.



Kuva 1. Tulosprisma (Lähde: Valtiovarainministeriö 2012, 16)

Valtion tulosohjauksen periaatteissa vaikuttavuudella tarkoitetaan organisaation toiminnan vaikutusta yhteiskuntaan suhteessa organisaatiolle asetettuihin tavoitteisiin. Tulosohjauksen perustana tulee olla selkeät ja mitattavissa olevat tavoitteet.

Kansalaisten ja julkisen hallinnon välillä vallitsee suhde, jossa kansalainen on palveluja tarvitseva asiakas ja julkinen hallinto niitä tarjoava toimija. Julkisen hallinnon organisaatiot ovat tilivelvollisia kansalaisille, jotka veronmaksun kautta kustantavat organisaatioiden toiminnan. Näin ollen julkisen hallinnon toimintaan kuuluu olennaisena osana raportointi toiminnan vaikuttavuudesta. Jul-

kisen hallinnon on kyettävä todistamaan kansalaisille, että se käyttää verotuksen kautta keräämiään varoja tarkoituksenmukaisesti. Kustannusten läpinäkyvyys lisää julkisen hallinnon uskottavuutta siinä, että se täyttää tilivelvollisuuden kriteerit. Digitaalisen turvallisuuden korostunut rooli herättää kysymyksiä siihen kohdennettavien resurssien tarkoituksenmukaisesta käytöstä.

Julkisen hallinnon tehokkuuden ja resursoinnin legitimiteetin vahvistamisen lisäksi kustannus-vaikuttavuusarvioinnin tärkeys perustuu myös siihen, että sen avulla voidaan kohdistaa resursseja olennaisiin kohteisiin ja arvioida resursoinnin tasoa suhteessa resursseilla saavutettaviin hyötyihin. Jotta hyvä resursoinnin taso voitaisiin määritellä, on verrattava keskenään panostuksista aiheutuvia kustannuksia ja niiden tuottamia rahallisia hyötyjä, sekä muita vaikuttavuustekijöitä. Digitaalisen turvallisuuden muuttuessa yhä keskeisemmäksi voimavaraksi julkisessa hallinnossa, on sitä pyrittävä johtamaan ja ohjaamaan tietoperustaisesti. Tiedolla johtamisen kehittämisessä on kustannus-vaikuttavuusarvioinnilla merkittävä rooli. Digitaaliseen turvallisuuteen panostettujen resurssien tulisi olla linjassa suojattavien kohteiden yhteiskunnallisen arvon ja siihen kohdistuvien lisääntyvien ja monimutkaistuvien riskien, sekä toimintaympäristön nopean muutoksen kanssa.

Digitaalisen turvallisuuden vaikuttavuuden arviointi on tärkeää myös, jotta turvallisuuden arvosta voitaisiin viestiä tehokkaasti resursoinnista päättäville tahoille. Voi olla mahdollista, että tietohallinto, tai muu digitaalisen turvallisuuden toteuttamisesta pääasiallisesti vastaava taho, sekä resursoinnista päättävä johto eivät arvota turvallisuutta yhteneväisellä tavalla. Mikäli riskejä ja suojaustoimien tehokkuutta kyettäisiin paremmin arvioimaan taloudellisesta näkökulmasta, lisäisi tämä ymmärrystä turvallisuuden arvosta läpi organisaatio- ja hallintorajojen (Hulthén 2009, 1). Vaikuttavuuden arvioinnin kehittämiseksi tulisi reaktiivisesta vikakeskeisyydestä siirtyä lähestymistapaan, jossa digitaalisen turvallisuuden arvo syntyy turvattavien kohteiden arvon, niihin kohdistuvien riskien sekä suojaustoimien tehokkuuden funktiona.

3.2 Keskeisiä tutkimuksia

Digitaalisen turvallisuuden yhteiskunnallisen merkittävyyden kasvun seurauksena 2000–luvulla on julkaistu paljon tutkimuksia, jotka keskittyvät digitaalisen turvallisuuden taloudellisen kustannus-vaikuttavuuden arvioimiseen (Haapamäki ja Sihvonen 2019, 818). Digitaalista turvallisuuden kustannus-vaikuttavuuden arviointia käsittelevästä kirjallisuudesta voidaan löytää tukea sekä digitaalisen turvallisuuden kustannusten arviointiin, investointimallien soveltamiseen että tarkoituksenmukaisen resursoinnin määrittämiseen.

Vuonna 2002 Marylandin yliopiston ekonomistit julkaisivat artikkelin *The Economics of Information Security Investment*, joka esittelee tietoruvallisuusinvestointien kustannuksia ja hyötyjä vertailevan taloustieteellisen mallin (Gordon & Loeb 2002). Kyseinen mallin merkitys digitaalisen turvallisuuden taloudellisesta arviointia koskevissa julkaisuissa on ollut erittäin huomattava. Mallin tarkoituksena on määritellä optimaalinen resursointi organisaation tietoturvallisuuteen, jotta vältetään negatiivisesti esimerkiksi tuottavuuteen vaikuttava yliresursointi sekä potentiaalisesti katastrofaaliset menetykset aiheuttava aliresursointi.

Mallin avulla voidaan arvioida tietoturvainvestoinnin optimaalista määrää nykytilanteessa. Mallilla siis verrataan inkrementaalisen lisäresursoinnin tuottamia hyötyjä ja kustannuksia verrattuna nykytilaan. Gordonin ja Loebin (2002) mukaan panostusta digitaaliseen turvallisuuteen kannattaa lisätä niin kauan kun lisäpanostusten avulla saavutettavat hyödyt ovat suurempia kuin niiden aiheuttamat kustannukset. Mallin oletuksena on, että tietoturvallisuuteen tehtyjen panostusten rajahyödyt ovat laskevia. Mallissa ei huomioida digitaalisen turvallisuuden kiinteitä kustannuksia, vaan siinä keskitytään nykytilan muutokseen, josta aiheutuu vain muuttuvia kustannuksia. Gordonin ja Loebin artikkelissa esitetään, että optimaalinen investointi tietoturvallisuuteen ei ylitä 36,8 %:a arvioidun menetyksen odotusarvosta.

$$z * < \left(\frac{1}{e}\right) vL$$

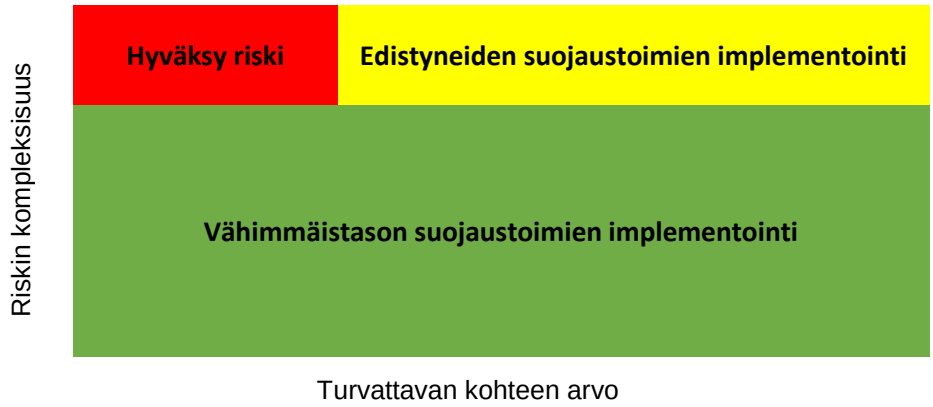
- z* = Optimaalinen resursoinnin taso
- L = Potentiaalinen menetys
- v= Riskin toteutumisen todennäköisyys
- vL = Menetyksen odotusarvo
- e = Luonnollisen logatiritmin kantaluku (~2,718)

Mallin keskeisenä puutteena sen käytännön sovellettavuuden kannalta on pidettävä epärealististista oletusta siitä, että päätöksentekijöillä on käytettävissään tiedot suojattaviin kohteisiin kohdistuvien riskien ja menetysten odotusarvoista. Käytännössä digitaalisen turvallisuuden riskien arviointi ja ennustaminen ovat hyvin vaikeita tehtäviä, sillä päätöksentekijöillä ei todennäköisesti ole käytettävissään kovinkaan tarkkoja ennusteita riskien todennäköisyyksistä ja vaikutuksista. Arvioinnin haasteita käsitellään tarkemmin jäljempänä raportissa. Gordonin ja Loebin mallissa ei huomioida ulkoisvaikutuksia, joiden seurauksena digitaalisen turvallisuuden riskeillä ja investoinneilla on laajempia vaikutuksia myös muihin toimintaympäristön organisaatioihin. Malli ei myöskään huomioi riskien mahdollisia keskinäisriippuvuuksia (Juuso & Svento 2018, 194).

Shimin (2011) mukaan digitaalisen turvallisuuden ulkoisvaikutuksilla on keskeinen rooli organisaatioiden optimaalisen resursoinnin tason suhteen. Tutkimus tuki Gordonin ja Loebin mallin tuloksia optimaalisesta resursoinnin tasosta, mutta vain jos ulkoisvaikutuksia ei huomioida. Digitaalisen toimintaympäristön verkottuneisuuden johdosta on mahdollista, että

poikkeamatilanteesta aiheutuvat menetykset kohdistuvat myös muihin organisaatioihin. Tämän johdosta yhteiskunnan kokonaisedun kannalta optimaalinen resursointi digitaaliseen turvallisuuteen voi olla huomattavasti korkeampi kuin 36,8 % arvioidun menetyksen odotusarvosta. Tutkimuksen tuloksista voidaan päätellä, että erityisesti julkisen hallinnon organisaatioiden tapauksessa tulisi aina arvioida riskien toteutumisen potentiaaliset vaikutukset myös muualla yhteiskunnassa.

Gilligan yms. (2013) esittivät, että jopa 75 % menetyksiä aiheuttavista digitaalisen turvallisuuden riskeistä on helposti torjuttavissa. Niiden välttämiseksi tai niiden aiheuttamien menetysten pienentämiseksi ei siis vaadita edistyneitä ja korkeita kustannuksia aiheuttavia suojaustoimia, vaan turvallisuuden vähimmäistason varmistusta. Vähimmäistaso on kontekstisidonnainen, mutta usein se määritellään lainsäädännössä asetettujen velvoitteiden kautta. Vähimmäistason suojaustoimet ylittävät panostukset taas tulisi kohdistaa turvattavien kohteiden arvon perusteella. Organisaatioiden tulisi siis tunnistaa turvattavat prosessit, toiminnot sekä järjestelmät, ja pyrkiä määrittämään niille arvo. Etenkin julkisessa hallinnossa turvattavien kohteiden arvon määrittämisessä tulee huomioida niiden arvo koko yhteiskunnalle, eli organisaatiolle itselleen, kansalaisille, palveluiden käyttäjille, yhteisöille sekä muille julkisen hallinnon organisaatioille. Suurempia kustannuksia aiheuttavat edistyneet suojaustoimet tulisi kohdistaa yhteiskunnan kannalta arvokkaimpien turvattavien kohteiden suojaamiseen (Gilligan yms. 2013, 7). Kompleksiset riskit, jotka vaativat edistyneitä ja kohdennettuja suojaustoimia tulisi hyväksyä niiden kohdistuessa ei-kriittisiin kohteisiin.



Kuva 2. Kyberturvallisuuden taloudellinen viitekehys (Gilligan yms. 2013)

Jotta digitaalisen turvallisuuden vaikuttavuutta voitaisiin arvioida, on keskeistä arvioida turvallisuuspanostusten vaikutuksia riskien todennäköisyyksiin ja vaikutuksiin. Su (2006) jaotteli poikkeamatilanteista aiheutuvat menetykset seuraavan jaottelun mukaisesti: taloudelliset menetykset, operationaaliset vaikutukset, vaikutukset asiakkaisiin ja vaikutukset henkilöstöön. Artikkelissa suositellaan digitaalisen turvallisuuden panostusten kohdentamista turvattavien kohteiden arvon perusteella. Tutkimuksen johtopäätös on siis yhteneväinen Gilliganin yms. (2013) kanssa.

Euroopan komission rahoittamassa vuosina 2017-2019 toteutetussa *Systemic Analyzer in Network Threat* (SAINT) –projektissa tavoitteena oli selvittää digitaalisen turvallisuuden kustannus-vaikuttavuuden tilaa Euroopassa. Projektissa digitaalista turvallisuutta tarkasteltiin poikkitieteellisestä näkökulmasta, ja siinä kerättiin tietoa digitaalisen turvallisuuden riskeistä, haavoittuvuuksista, poikkeamista sekä digitaaliseen turvallisuuteen käytetyistä resursseista EU:n jäsenvaltioissa.

SAINT- projektin kustannus-hyötyanalyysia käsittelevässä raportissa digitaalisen turvallisuuden hyödyt määriteltiin syntyvän riskien toteutumisesta aiheutuvien menetysten välttämisen sekä pienentämisen kautta. Digitaalisesta turvallisuudesta aiheutuvat kustannukset taas jaoteltiin toiminnallisiin menoihin

(Operational Expenditures, OPEX) ja pääomakustannuksiin (Capital Expenditures, CAPEX). Kustannus-hyötyjen arvioinnissa metodina käytettiin nettonykyarvomenetelmää, jonka avulla tarkasteltiin EU:n jäsenvaltioiden digitaalisesta turvallisuudesta saavutettavia hyötyjä sekä kustannuksia. (Rokkas, Neokosmidis ja Xydias 2018, 8).

Tutkimuksessa digitaalisen turvallisuuden kustannusten arviointi perustui eri suojaustoimikategorioiden keskimääräisiin markkinahintoihin, jotka skaalattiin yhteiskunnan tasolle. Skaalauksessa huomioitiin tieto- ja viestintäteknologian pääomaintensiteetti, palveluiden osuus kokonaistuotannosta sekä yritysten määrä ja koko eri kansantalouksissa. Tutkimuksessa käytetyt suojaustoimikategoriat olivat tietoturvaohjelmistot, auditoinnit ja havaitsemisjärjestelmät (Rokkas, Neokosmidis ja Xydias 2018, 33).

Arvioinnissa ei keskitytty julkiseen sektoriin, vaan kustannus-hyötylaskelmat toteutettiin valtioiden tasolla hyödyntäen muun muassa Euroopan unionin tilastotoimisto Eurostatin sekä OECD:n tarjoamia tilastotietoja. Tutkimuksessa verrattiin keskenään nykytilannetta sekä skenaariota, missä organisaatiot eivät käyttäisi lainkaan resursseja digitaaliseen turvallisuuteen. Kunkin jäsenvaltion yritykset jaettiin niiden henkilöstön lukumäärän perusteella neljään kategoriaan: mikrokokoiset (1-9), pienet (10-49), keskisuuret (50-249) ja suuret (250 tai enemmän) yritykset. Näille eri yrityskategorioille luotiin riskiprofiilit keskimääräisiä poikkeamatilanteista aiheutuneita menetyksiä hyödyntäen. Tämän lisäksi arvioitiin eri yrityskategorioiden digitaaliseen turvallisuuteen käyttämät resurssit, sekä kyselytutkimusten kautta selvitetty suojaustoimien tehokkuus riskien torjunnassa.

Tutkimuksessa riskit jaoteltiin seuraaviin viiteen kategoriaan: haittaohjelmat, tietojen kalastelu, roskaposti, kiristysohjelmat ja tietoturvaloukkaukset. Riskien toteutumisesta aiheutuvat menetykset taas jaettiin seuraaviin kategorioihin: immateriaalioikeudelliset menetykset, toiminnan keskeytykset, datan ja ohjelmistojen menetykset, kiristystapauksista ja petoksista aiheutuneet menetykset,

luottamuksellisen tiedon vuotamisesta aiheutuvat seuraukset, korvausvelvollisuudet kolmansille osapuolille, vaikutukset maineeseen, fyysiseen omaisuuteen kohdistuvat menetykset, henkeen ja terveyteen kohdistuvat menetykset sekä poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset (Rokkas, Neokosmidis ja Xydias 2018, 48).

Arvioituja riskien aiheuttamia menetyksiä verrattiin digitaaliseen turvallisuuteen käytettyihin resursseihin, jotka yritykset käyttävät suojaustoimiin sekä niiden arvioituun tehokkuuteen riskien torjunnassa. Tutkimuksessa digitaalisen turvallisuuden nettohyötyjen arvioitiin olevan yhteensä 801 ja 1868 miljoonan euron välillä Suomessa vuosina 2018-2021 (Rokkas, Neokosmidis ja Xydias 2018, 64).

Tutkimuksen tuloksia on pidettävä parhaimmillaankin suuntaa-antavina, sillä kerätyn datan epätarkkuus vaikuttaa merkittävästi saavutettuihin tuloksiin. Mekanistiset turvallisuustuotteiden markkinahintoihin perustuvat olettamat eri organisaatioiden rahallisista panostuksista digitaaliseen turvallisuuteen ovat väistämättä epätarkkoja. Myös turvallisuuspanostuksilla saavutettavat hyödyt on tutkimuksessa määritelty hyvin mekanistisesti ilman sofistikoitunutta analyysimallia. Tutkimuksessa ei huomioida esimerkiksi yritysten toimialan vaikutusta digitaalisen turvallisuuden kustannuksiin ja hyötyihin. Myöskään riskien toteutumisesta aiheutuvia yhteiskunnallisia ulkoisvaikutuksia ei ole huomioitu.

Tutkimus	Keskeiset johtopäätökset
Gordon, L. & Loeb, M. (2002). *The economics of information security investment*	Digitaaliseen turvallisuuteen tehtävien panostusten rajahyödyt ovat laskevia. Optimaalinen resursointi digitaaliseen turvallisuuteen ei ylitä 37 % menetyksen odotusarvosta.
Shim, W. (2011). *Vulnerability and Information Security Investment Under Interdependent Risks: A Theoretical Approach*	Digitaalisen toimintaympäristön verkottuneisuuden johdosta ulkoisvaikutusten huomioiminen on keskeistä digitaalisen turvallisuuden kustannus-vaikuttavuuden arvioinnin kannalta. Gordon-Loeb mallin johtopäätökset eivät ole päteviä, jos ulkoisvaikutukset huomioidaan.
Gilligan, J. (2013). *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*	Tärkeintä on varmistaa perustason suojaustoimien implementointi. Edistyneemmät, suuria kustannuksia aiheuttavat suojaustoimet tulisi kohdistaa arvokkaimpien turvattavien kohteiden suojaamiseen. Ei-kriittisiin turvattaviin kohteisiin kohdistuvat edistyneitä suojaustoimia vaativat riskit tulisi hyväksyä.
Su, X. (2006). *An Overview of Economic Approaches to Information Security Management*	Vaikuttavuus syntyy vältetyistä menetyksistä. Tämän johdosta digitaalisen turvallisuuden hyötyjen arvioinnissa on keskeistä suhteuttaa panostuksilla saavutettava hyöty turvattavien kohteiden arvon mukaisesti.
Rokkas, Neokosmidis ja Xydias. (2018). *Report on Cost-Benefit Analysis of Cyber-security Solutions, Products and Models*	Digitaalisen turvallisuuden nettoarvo vuosina 2018-2021 on huomattavan positiivinen lähes kaikissa Euroopan unionin jäsenvaltioissa.

Taulukko 1. Kustannus-vaikuttavuuden arviointia käsitteleviä tutkimuksia

3.3 Investointimallit

Investointimallien suora soveltaminen edellyttää tarkkaa informaatiota kustannuksista ja hyödyistä, sekä oletuksena niissä on kaikkien merkityksellisten seikkojen huomiointi. Vaikka tämä ei todennäköisesti olekaan reaalimaailmassa mahdollista, voivat mikrotaloudelliset investointimallit mahdollisesti toimia hyvänä lähtökohtana laajempaan digitaalisen turvallisuuden kustannus-hyötyanalyysiin.

Digitaalisen turvallisuuden investointilaskelmissa hyödynnetään usein sovellettua versioita sijoitetun pääoman tuottoasteen tunnusluvusta (Return On Investment, ROI), jonka laskentakaava on kuvattu alla:

$$ROI = \frac{tuotot - investoinnin\ kustannukset}{\text{investoinnin kustannukset}}$$

Return On Security Investment (ROSI) on turvallisuusinvestointeihin sovellettava versio pääoman tuottoasteen tunnusluvusta. ROSI:n erona pääoman tuottoasteeseen verrattuna on, että siinä investoinnin hyötynä ei synny tuottoja, vaan taloudellinen hyöty syntyy riskien pienentymisen seurauksena (ISACA 2012). Jotta ROSI voitaisiin laskea, on ensin määriteltävä seuraavat parametrit:

- Vuosittainen riskien realisoitumisten lukumäärä (Annual Rate of Occurrence, ARO).
- Yksittäisen poikkeaman aiheuttama menetys (Single Loss Expectancy, SLE), joka sisältää sekä suorat että epäsuorat menetykset. Esimerkki suorista menetyksistä ovat katkokset palvelutuotannossa. Epäsuorista menetyksistä esimerkkinä toimivat organisaation maineeseen kohdistuvat haitat.

- Vuosittainen menetysten määrä, joka saadaan ARO:n ja SLE:n tulona (Annual Loss Expectancy, ALE)

$$ROSI = \frac{(ALE\ ennen\ investointia - ALE\ investoinnin\ jälkeen) - investoinnin\ kustannukset}{\text{investoinnin kustannukset}}$$

Samoin kuin Gordon-Loeb –mallissa, myös ROSI:n laskemiseen tarvitaan tarkkoja arvioita menetysten suuruudesta, niiden toteutumisen todennäköisyyksistä sekä turvallisuusinvestointien tehokkuudesta. Vaadittujen tietojen tarkkuuden vuoksi sen suora soveltaminen digitaalisen turvallisuuden investointien suhteen on haasteellista. Pitkän taloudellisen käyttöajan suurissa kertainvestoinneissa on huomioitava myös rahan aika-arvo, jota ROSI ei huomioi.

Toinen yleisesti digitaalisen turvallisuuden resursointiin sovellettu investointimalli on nettonykyarvomenetelmä. Nettonykyarvolaskelman kaava on kuvattu alla:

$$Nettonykyarvo = \frac{R\ t}{(1+i)^t} - I$$

Jossa:

- R = hyöty; i = diskonttokorko; t = aikajaksojen määrä; I = investointi

Digitaaliseen turvallisuuteen käytetyistä resursseista saavutettavat hyödyt voivat usein realisoitua hyvin pitkällä aikavälillä, vaikka investoinnin kustannukset realisoituvat täysimääräisesti jo investointihetkellä. Näin ollen turvallisuusinvestoinneista saavutettavat taloudelliset hyödyt ja kustannukset eivät ole keskenään vertailukelpoisia. Tulevaisuuteen sijoittuvat taloudelliset hyödyt tulee

diskontata, jotta niiden arvottaminen nykyhetkessä olisi mahdollista. Nettonykyarvomenetelmän avulla tulevaisuudessa saavutettavat taloudelliset hyödyt muutetaan niiden nykyarvoon diskonttaamalla ne asetetulla tuottovaateella. (Flores, Sommestad, Holm & Ekstedt 2011).

Sisäisen korkokannan menetelmä on nettonykyarvon tunnusluvusta sovellettu versio. Se tarkoittaa diskonttokorkoa, jolla tarkastellun hankkeen arvioitujen kustannusten ja hyötyjen nettonykyarvo on nolla.

4 DIGITAALISEN TURVALLISUUDEN TALOUDELLINEN ARVIOINTI

4.1 Digitaalisen turvallisuuden kustannukset ja hyödyt

Teoreettisessa tarkastelussa digitaalisen turvallisuuden optimaalinen resursointi saavutetaan pisteessä, jossa turvallisuudesta saatavat rajahyödyt kohtaavat turvallisuuspanostuksista aiheutuvat rajakustannukset. Riskien todennäköisyys huomioiden tässä pisteessä riskien pienentämisestä aiheutuvat kustannukset olisivat suurempia kuin riskien toteutumisesta aiheutuvat menetykset. Reaalimaailmassa digitaalisen turvallisuuden rajahyötyjä ja –kustannuksia ei ole mahdollista verrata näin tarkasti, sillä panostuksista aiheutuvat kustannukset eivät lisäänny lineaarisesti vaan porrastetusti lisäpanostusten myötä. Turvallisuuspanostuksilla saavutettavat hyödyt taas voivat kohdistua vuosien päähän. On myöskin epärealistista olettaa, että päätöksentekijöillä olisi käytettävissään täydellinen informaatio digitaalisen turvallisuuden kustannuksista ja riskeistä, tai muista saavutettavien hyötyjen arvioimiseksi vaadittavista asioista.

Jotta digitaaliseen turvallisuuteen tehtyjen panostusten tehokkuutta voitaisiin arvioida, ei ole riittävää tarkastella niitä pelkästään taloudellisesti, vaan on huomioitava digitaalisen toimintaympäristön tekniset realiteetit. Teoreettisesti tarkasteltuna on oletettava, että digitaaliseen turvallisuuteen tehtävien panostusten rajahyödyt ovat laskevia (Gordon ja Loeb 2002, 445). Lisäpanostukset siis tuottavat hyötyjä, mutta niiden kasvuvauhti on vähenevä. Täydellisen turvallisuuden saavuttaminen on käytännössä mahdotonta, vaikka turvallisuuteen panostettaisiin kuinka paljon.

Resursoinnista päättäessään päätöksentekijä arvioi ja vertaa investoinnin hyötyjä sekä kustannuksia. Digitaalisen turvallisuuden suhteen hyödyt saavutetaan varmistamalla organisaation toimintavarmuus sekä täyttämällä lainsäädännössä asetetut vaatimukset. Näiden tavoitteiden saavuttaminen voidaan pelkistää poikkeamien ja häiriötilanteiden välttämiseen. Jotta vaikuttavuutta

voitaisiin mitata, olisi päätöksentekijän saatava tietoonsa riskien todennäköisyydet ja potentiaaliset vaikutukset sekä ennen että jälkeen suojaustoimien asettamisen. Tämän lisäksi olisi tiedettävä suojaustoimista aiheutuneet kustannukset.

Keskeinen digiturvallisuudesta saatava hyöty on turvattaviin kohteisiin kohdistuvien riskien toteutumisen estäminen tai niiden vaikutusten pienentyminen. Tämä tarkoittaa käytännössä digitaaliseen turvallisuuteen käytettyjen resurssien vaikutusta riskien realisoitumisesta aiheutuneiden tappioiden laatuun ja määrään.

Digitaalisen turvallisuuden kustannus-vaikuttavuutta voidaan mallintaa seuraavalla tavalla:

- A= Turvattavan prosessin, palvelun tai tietovarannon arvo huomioiden ulkoisvaikutukset
- T= Digitaalisen turvallisuuden taloudellisten nettohyötyjen nykyarvo
- U= Riskin realisoitumisesta aiheutuvan menetyksen odotusarvo
- Z= Riskin arvon lasku, eli menetysten väheneminen
- I= Digitaalisen turvallisuuden kustannukset
- D= Diskonttokorko, joka määrittää tulevaisuuteen allokoituvien hyötyjen nykyarvon

Digitaalisen turvallisuuden toimenpiteiden mitoittamista eli digitaalisen turvallisuuden kustannuksia (I) on tarkasteltava suhteessa turvattavan kohteen arvoon (A). Toisaalta digitaaliseen turvallisuuteen panostaminen myös kasvattaa turvattavan kohteen arvoa. Erittäin laajan menetyksen realisoituessa koko tur-

vattavan kohteen arvo voidaan menettää, eli riskin realisoitumisesta aiheutuvan menetyksen odotusarvo (U) voi pahimmillaan olla sama tai suurempi kuin suojattavan kohteen arvo (A). Tämä tarkoittaa, että

$$U = mA, missä\ m \geq 0$$

Jos riskin realisoitumisesta aiheutuvan menetyksen arvioidaan olevan suurempi kuin turvattavan kohteen arvon, eli m>1, niin digitaaliseen turvallisuuteen tehtävä lisäpanostus on erittäin tärkeää tai jopa välttämätöntä. Usein tällaisessa tilanteessa digitaalinen turvallisuus käytännössä toimii turvattavan kohteen eli jonkin prosessin, palvelun tai tietovarannon välttämättömänä mahdollistajana.

Digitaalisen turvallisuuden taloudellisten hyötyjen nettoarvo (T) saadaan vähentämällä riskien arvon laskusta eli potentiaalisten menojen pienenemisestä (Z) digitaalisen turvallisuuden kustannukset (I) diskontattuna nykyarvoon. Tämä tarkoittaa, että:

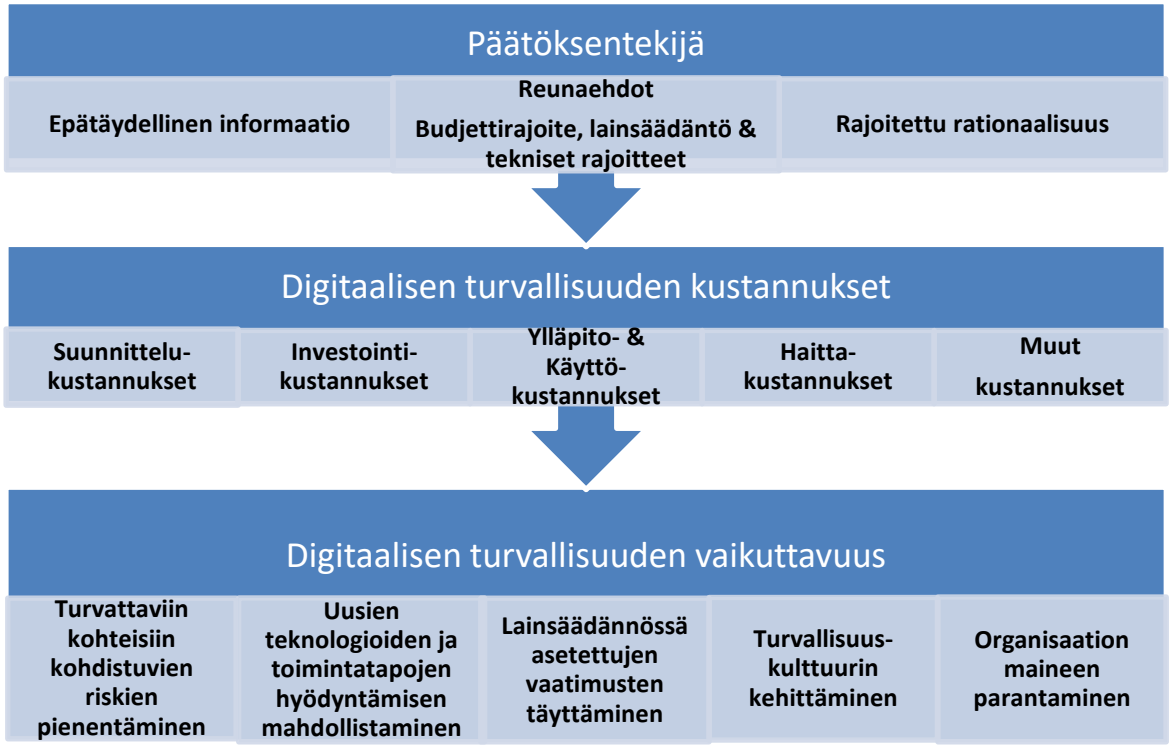
$$T = (Z - I)/D$$

Yllä olevasta voidaan päätellä, että jos digitaalisen turvallisuuden kustannukset ylittävät riskien arvon vähentymisen, niin digitaalisen turvallisuuden taloudellisten hyötyjen nettoarvo kääntyy negatiiviseksi. Digitaalisen turvallisuuden kustannusten tunnistamisen lisäksi huomiota on siis kiinnitettävä riskien arvon vähenemiseen eli potentiaalisten menetysten pienentämiseen.

Taloudellisten hyötyjen arvioinnin suhteen on otettava huomioon psykologiset tekijät, ajan vaikutus ja keskinäisriippuvuudet, jotka vaikuttavat riskiarviointiin. Riskien sieto-, käsittely- ja tunnistamiskyky vaihtelevat eri organisaatioiden ja yksilöiden välillä. Riskien arviointi siis usein on vahvasti subjektiivista (VM 2017, 26). Näin ollen optimaalista arviointia rajoittavat monet tekijät, minkä johdosta päätöksentekijöiden voidaan sanoa toimivan rajoitetun rationaalisuuden puitteissa.

Digitaalisen turvallisuuden resursoinnin avulla tavoiteltavana hyötynä on myös julkisen hallinnon organisaation maineen vahvistaminen keskeisten sidosryhmien kuten kansalaisten, organisaation henkilöstön, yhteistyökumppaneiden, muiden julkisen hallinnon toimijoiden sekä median silmissä.

Institutionaalisen organisaatioteorian mukaan rationaalisesti toimivat organisaatiot mukauttavat toimintaansa ympäristönsä instituutioiden asettamien muutospaineiden mukaisesti, minkä seurauksena organisaatioiden toimintatavat ja rakenteet alkavat muuttua yhtenäisemmiksi (DiMaggio ja Powell 1983). Muutospaineet voidaan jakaa kolmeen kategoriaan, joiden avulla voidaan ymmärtää digitaalisesti turvallisuudesta saavutettavia hyötyjä julkisen hallinnon toimijoiden näkökulmasta. Pakottavat muutospaineet liittyvät lainsäädännön asettamiin turvallisuusvaatimuksiin. Digitaalisen turvallisuuden resursoinnin välttämätön tavoite onkin säädöksin asetettujen vaatimusten täyttäminen. Jäljittelevä isomorfismi taas johtuu muutospaineista, jotka syntyvät yhteiskunnan odotuksista ja vaatimuksista organisaatioiden digitaalisen turvallisuuden suhteen. Keskeiset sidosryhmät kuten kansalaiset, organisaation henkilöstö sekä muut julkisen hallinnon toimijat odottavat jokaisen toimijan panostavan turvallisuuteen. Tämän johdosta vahvempi digitaalisen turvallisuuden taso voi vaikuttaa myönteisesti organisaatioiden maineeseen. Kolmantena muutospaineena on taloudellisiin paineisiin liittyvä ulottuvuus. Resurssien niukkuus pakottaa organisaatioita omaksumaan keskenään samankaltaisia, kustannustehokkuuteen pyrkiviä rakenteita ja käytäntöjä (Mänttäri-van der Kuip, Tammelin ja Anttila 2018, 235).



Kuva 3. Digitaalisen turvallisuuden kustannukset ja hyödyt julkisen hallinnon päätöksentekijän näkökulmasta

Kustannusten ja hyötyjen vertaamiseksi on muodostettava indikaattoreita, jotka kuvaavat vaikuttavuutta mahdollisimman luotettavasti ja tarkasti. Indikaattorilajit erotellaan usein niiden mitta-asteikon mukaisesti numeerisia arvoja saaviin määrällisiin indikaattoreihin sekä sanallisesti kuvaileviin laadullisiin indikaattoreihin. Laadullisille indikaattoreille voidaan kuitenkin antaa sekä sanallisia että numeerisia arvoja jollakin tietyllä luokittelu- tai järjestysasteikolla. Voidaan esimerkiksi kuvata mitattavan asian suoritustasoa tai laatua asteikolla 1-10. Jotta digitaalista turvallisuutta voitaisiin johtaa ja kehittää tietoon perustuen, on vaikuttavuudelle kehitettävä sekä määrällisiä että laadullisia mittareita.

Lainsäädännössä asetettujen vaatimusten täyttämisen arvioiminen on kuvassa 3 esitetyistä viidestä hyötykategoriasta selkeintä. Julkisen hallinnon toimijoiden on lähtökohtaisesti aina toiminnassaan täytettävä lainsäädännössä asetetut

velvoitteet. Säännöstenmukaisuus voidaan kuitenkin saavuttaa erilaisilla tavoilla ja näin ollen myös erilaisilla kustannuksilla, jolloin myös lainsäädäntö voi toimia lähtökohtana kustannus-hyötyanalyysissa.

Digitaalisen turvallisuuden tuottamat hyödyt eivät synnytä suoria rahavirtoja. Rahamääräisesti arvioitavissa olevat digitaalisen turvallisuuden hyödyt syntyvät vältetyistä menetyksistä, jotka olisivat kohdistuneet turvattavien kohteiden arvoon. Vältettyjä menetyksiä arvioidaan usein osana riskiarviointia, ja sen johdosta digitaalisen turvallisuuden kustannus-vaikuttavuusanalyysi liittyy riskiarviointiin.

Riskiarviointiin kytkeytyvän analyysin sijaan digitaalisen turvallisuuden taloudellisia hyötyjä organisaatioille voitaisiin mahdollisesti arvioida myös subjektiivisten arvottamismenetelmien avulla (Schneier 2013, 206). Tällöin arvoa mitattaisiin marginaalisella maksuhalukkuudella. Digitaalisen turvallisuuden tapauksessa maksuhalukkuus paljastaisi esimerkiksi sen, kuinka paljon organisaatio olisi valmis maksamaan yhden ennalta määritellyn yksikön suuruisesta parannuksesta jonkin tietyn kohteen turvallisuuteen. Maksuhalukkuutta mittaavia menetelmiä voidaan toteuttaa esimerkiksi kyselyiden tai monitavoitearvioinnin kautta. Riskiarviointiin pohjautuvassa kustannus-hyötyanalyysissa puolestaan asiantuntijat tekevät arvioinnin vertaamalla vältettäviä menetyksiä ja suojaustoimien aiheuttamia kustannuksia.

Laadullisia vaikuttavuustekijöitä, kuten digitaalisen turvallisuuden tason ja resursoinnin vaikutusta organisaation maineeseen sidosryhmien keskuudessa voidaan arvioida esimerkiksi kyselyiden avulla. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) on jo 2000-luvun alusta saakka toteuttanut VAHTI-kyselyjä ja vuodesta 2016 alkaen tietoturvabarometria, joilla tietoturvallisuuden tasoa julkisen hallinnon organisaatioissa mitataan laadullisten indikaattoreiden avulla (Valtiovarainministeriö 2018, 9).

Tämän raportin liitteessä 4 kuvatuilla digitaalisen turvallisuuden laadullisen arvioinnin indikaattoreilla pyritään täydentämään VAHTI:n julkaiseman henkilöstön ja johdon tietoturva barometrin kysymyksiä selvittämällä henkilöstön näkemyksiä digitaalisen turvallisuuden järjestämisen taloudellisen tarkoituksenmukaisuuden suhteen. Digitaalisen turvallisuuden tarkoituksenmukainen toteuttaminen vaatii organisaation sisällä läpinäkyvyyttä kustannusten sekä niiden kohdistamisperusteiden suhteen. Raportissa kuvatuilla laadullisilla indikaattoreilla mitataankin sekä näkemyksiä kustannus-vaikuttavuudesta että tietojen läpinäkyvyydestä.

4.2 Arviointiin liittyvät epävarmuustekijät

Julkisessa hallinnossa ei tällä hetkellä ole käytössä yhteisesti käytettyä menetelmää digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arviointiin. Jotta arviointia voitaisiin kehittää, on otettava huomioon digitaalisen toimintaympäristön erityispiirteisiin liittyviä haasteita.

Yksi suurimmista haasteista on digitaaliseen turvallisuuteen liittyvien riskien dynaaminen luonne. Turvallisuuspoikkeamien frekvenssien ja vaikutusten hajonta on suuri. Jotta suojaustoimien vaikutuksia riskeihin voitaisiin luotettavalla tavalla ennustaa, olisi kerättävä systemaattisesti tietoa toteutuneiden poikkeamien vaikutuksista ja määristä. Tilastollisesti merkitsevän aineiston tulisi sisältää laajasti havaintoja poikkeamista sekä ennen että jälkeen eri suojaustoimenpiteiden käyttöönottoa. Riskit ovat monimuotoisia ja niiden välillä vallitsee digitalisoituvan yhteiskunnan verkottuneisuuden vuoksi voimakas keskinäisriippuvuus. Tämän vuoksi riskien todennäköisyyksiä ja niiden potentiaalisesti aiheuttamia menetyksiä on haasteellista ennustaa, eikä riskien realisoitumisen jälkeenkään ole helppoa arvioida aiheutuneita menetyksiä (Su 2006, 10). Keskinäisriippuvuuksien johdosta yhden riskin toteutumisella voi olla huomattavia kerrannaisvaikutuksia, jotka kohdistuvat hyvin laajasti eri toimijoihin. Näin ollen

yksittäisen organisaation panostukset digitaaliseen turvallisuuteen vaikuttavat myös muiden toimintaympäristön organisaatioiden riskeihin. Esimerkiksi poikkeamasta aiheutuneet toiminnan keskeytykset ja niihin kulunut työaika voivat olla suhteellisen helposti mitattavissa. Riskiarvioissa tulisikin pyrkiä arvioimaan potentiaaliset vaikutukset mahdollisimman laajasti koko yhteiskunnan tasolla.

Historiallisen riskidatan arvo on digitaalisissa toimintaympäristöissä huomattavasti vähäisempi kuin staattisempia riskejä analysoitaessa (Panou, Ntantogian & Xenakis 2017, 1). Riskidataan perustuvien ennusteiden laatimisesta saavutettavat hyödyt ovat näin ollen hyvin rajallisia.

Toinen keskeinen haaste on digitaalisen turvallisuuden aiheuttamien kustannusten arvioiminen. Yksittäisen toimenpiteen kustannukset riippuvat aina hankinnan toteutustavasta ja toimintaympäristöstä. Digitaalinen turvallisuus on usein sisäänrakennettu ominaisuus eri järjestelmissä, toimintatavoissa ja prosesseissa. Kustannustehokkuuden parantamiseksi onkin keskeistä, että toimintatavat, prosessit sekä muut digitaalisen turvallisuuden riskeiltä suojattavat kohteet olisivat turvalliseksi suunniteltuja (Valtiovarainministeriö 2014, 42). Ad hoc –ratkaisuina toteutettavien turvallisuustoimien kustannukset heikentävät digitaalisen turvallisuuden kustannustehokkuutta. Huomioimalla digitaalinen turvallisuus jo hankintoja, tietoverkkoja ja toimintatapoja suunniteltaessa voidaan vähentää turvattavien kohteiden haavoittuvuutta riskeille ja tarvetta lisäpanostuksille myöhemmässä vaiheessa (Rokkas, Neokosmidis & Xydias 2018, 28).

Valtiovarainministeriön *julkisen hallinnon digitaalisen turvallisuuden resurssitilannekuva* –selvityksessä (Koikkalainen 2019) kävi ilmi, että digitaaliseen turvallisuuteen liittyvät palvelut ovat usein sisällytettyinä palvelusopimuksilla tehtyihin hankintoihin, jolloin niiden osuutta sopimuksen kokonaiskustannuksista ei ole mahdollista jaotella ja arvioida tarkasti. Selvityksen loppuraportissa todetaan, että digitaalinen turvallisuus on usein erottamaton osa digitaalisia proses-

seja, palveluita sekä tietovarantoja. Näin ollen digitaalisen turvallisuuden kustannusten tarkka mittaaminen on usein mahdotonta, ja on tyydyttävä karkeampiin arvioihin (Koikkalainen 2019, 13).

Digitaalisen turvallisuuden tuottamat taloudelliset hyödyt perustuvat sen riskien todennäköisyyksiä sekä potentiaalisia negatiivisia vaikutuksia pienentäviin vaikutuksiin. Tämän johdosta on huomattavasti haasteellisempaa arvioida digitaalisen turvallisuuden vaikuttavuutta verrattuna esimerkiksi perinteiseen pääomainvestointiin, joka tuottaa liikevaihtoa tai muuta helposti mitattavissa olevaa hyötyä (Rodewald 2005, 139).

Kolmas tunnistettu kustannus-vaikuttavuusarviointiin liittyvä keskeinen haaste on riskejä pienentävien toimien vaikutusten arviointi ja mittaaminen. Turvallisuuspoikkeamien frekvenssien ja vaikutusten hajonta on suuri. Jotta suojaustoimien vaikutuksia riskeihin voitaisiin luotettavalla tavalla ennustaa, olisi kerättävä systemaattisesti tietoa toteutuneiden poikkeamien vaikutuksista ja määristä. Tilastollisesti merkitsevän aineiston tulisi sisältää laajasti havaintoja poikkeamista sekä ennen että jälkeen eri suojaustoimenpiteiden käyttöönottoa. Myös informaation epäsymmetria häiritsee vaikuttavuusanalyysin tekemistä, sillä palveluntarjoaja tietää huomattavasti paremmin tuottamansa palvelun turvallisuudesta kuin asiakkaan roolissa toimiva organisaatio.

Suojaustoimien vaikuttavuuden mittaamisen täytyy perustua teoreettisesti perusteltuihin tai empiirisesti toteennäytettyihin syy-seuraussuhteisiin riskien suhteen. Organisaation tasolla on käytössä paljon erilaisia digitaalisen turvallisuuden suojaustoimia, ja yksittäisten toimenpiteiden vaikuttavuutta voi olla haasteellista suoraan kohdistaa tiettyihin suojattaviin kohteisiin. Niiden arvoa siten ei välttämättä aina voida määrittää rahamääräisesti säästettyjen menetysten kautta (OECD 2017, 111). Erityisesti torjuttujen uhkien osalta hyötyjen havaitseminen on vaikeaa, sillä toteutumatta jääneet uhkat eivät useinkaan tule näkyviksi, eikä niiden toteutumattomuus välttämättä johdu panostuksista digitaaliseen turvallisuuteen.

Toimenpiteillä voidaan saavuttaa muitakin kuin menetysten odotusarvon laskuun liittyviä hyötyjä. Digitaaliseen turvallisuuteen siis liittyy myös laadullisia vaikuttavuustekijöitä, kuten organisaation maineen parantuminen ja kohentunut työhyvinvointi. Näiden laadullisten tekijöiden mittaaminen on haasteellista (Panou et al. 2017, 1). Vaikuttavuuden arvioinnin kehittämiseksi tulisi julkisessa hallinnossa ottaa käyttöön indikaattorit, joiden avulla laadullisia vaikuttavuustekijöitä kyettäisiin mittaamaan, arvioimaan ja seuraamaan nykytilannetta tarkemmin.

4.3 Kustannusten arviointi ja luokittelu

Valtiontalouden tarkastusviraston vuonna 2017 julkaisemassa tuloksellisuustarkastuskertomuksessa mainitaan, että valtionhallinnon organisaatioiden digitaaliseen turvallisuuteen käyttämien resurssien tarkoituksenmukaisuus on epäselvää. Julkisen hallinnon organisaatiot budjetoivat digitaaliseen turvallisuuteen käytettävät varat toimintamenomomentille erittelemättömänä osana organisaation toiminnasta aiheutuvia kustannuksia (VTV 2017). Tämä on ongelmallista digitaalisen turvallisuuden kustannus-vaikuttavuuden arvioinnin kannalta. Tuloksellisuustarkastuskertomuksessa tuodaan esille, että valtion talousarvion laadintamääräyksissä ei ole menettelyä, joka riittävällä tasolla huomioisi digitaalisen turvallisuuden resurssien tarkoituksenmukaisen kohdistuksen.

Digitaalisen turvallisuuden kustannusten kategorisoimiseen ja budjetointiin on olemassa useita vaihtoehtoisia menetelmiä. Pääsääntöisesti julkisen hallinnon organisaatioiden budjetoinnissa ja kustannuslaskennassa ei eritellä tietotekniikan, tietohallinnon tai turvallisuuden kustannuksia. Digitaaliset prosessit, toimintatavat ja teknologiat ovat tiiviisti ja erottamattomasti läsnä kaikkialla organisaatioiden toiminnassa. Digitaalisen toimintaympäristön myötä syntyy aina myös tarve varmistaa digitaalinen turvallisuus. Jotta kustannus-vaikuttavuus-

analyysia ja sen tukemana tietoperustaista turvallisuuden kehittämistä voitaisiin tehdä, on välttämätöntä pyrkiä erottamaan digitaalisen turvallisuuden kustannukset muista tietohallinnon, palveluhankintojen sekä henkilöstön kustannuksista. Julkisen hallinnon organisaatioiden budjetoinnissa ja kustannuslaskennassa on siis määriteltävä, millä tavalla kustannuksia mitataan. Vertailukelpoisuuden vuoksi tulisi julkisen hallinnon organisaatioissa ottaa käyttöön mahdollisimman yhteneväinen menetelmä digitaalisen turvallisuuden kustannusinformaation kokoamiseen.

Valtiovarainministeriön selvityksessä (Koikkalainen 2019) kartoitettiin erilaisia malleja digitaalisen turvallisuuden kustannusten jaotteluun julkisessa hallinnossa. Selvityksessä pyrittiin määrittelemään julkisen hallinnon organisaatioiden digitaaliseen turvallisuuteen käyttämät resurssit hyödyntäen konsulttiyhtiö Gartnerin tarjoamaa viitekehystä. Gartner jaottelee kustannukset seuraaviin neljään kategoriaan: infrastruktuuri, haavoittuvuuksien hallinta ja analytiikka, sovellukset ja ohjaus sekä riskien- ja vaatimustenmukaisuuden hallinta (Koikkalainen 2019, 7; Gartner 2018, 5). Selvityksessä todettiin, että Gartnerin tarjoama kustannusjaottelu ei ole optimaalinen malli Suomen julkisen hallintoon, sillä siinä ei huomioida yhteiskunnan eri sektoreilla toimivien organisaatioiden erilaisia palvelutuotantomalleja eikä julkisen hallinnon momenttiperusteista kustannuslaskentaa.

Digitaalisen turvallisuuden kustannuksia arvioitaessa ei tulisi rajoittua pelkästään suorien kirjanpidollisten kustannusten mittaamiseen, sillä panostukset turvallisuuteen voivat aiheuttaa myös huomattavia epäsuoria kustannuksia. Tällaisia ovat esimerkiksi toiminnan nopeuteen, tehokkuuteen ja mukavuuteen negatiivisesti vaikuttavat tekijät. Turvallisuuspanostuksista aiheutuvat haittakustannukset eivät aiheuta rahavirtojen muutoksia, vaan niiden vaikutukset syntyvät epäsuorasti tuottavuuden laskun myötä. Haittakustannuksia voi syntyä sekä turvallisuustoimien toteutusvaiheessa, että käyttöönoton jälkeen toiminnassa ilmenevinä haittoina.

4.3.1 Pääomakustannukset ja toiminnalliset menot

Digitaalisesta turvallisuudesta aiheutuvat kustannukset voidaan jaotella pääomakustannuksiin (Capital Expenditures, CAPEX) ja toiminnallisiin menoihin (Operational Expenditures, OPEX). Jaottelu pääomakustannusten ja toiminnallisten menojen välillä perustuu niiden taloudelliseen käyttöaikaan. Investoinnit pääomaan ovat pitkäaikaisia ja niiden avulla saavutetaan hyötyjä useiden vuosien aikana. Näin ollen kustannuslaskennassa pääomainvestointien kustannukset tulee jakaa poistoina useille vuosille niiden käyttöajan mukaisesti, ja niillä saavutettavat hyödyt tulee muuntaa nykyarvoon diskonttaamalla. Toiminnalliset kustannukset taas syntyvät organisaation juoksevista digitaalisen turvallisuuden menoista. Määritelmällisesti toiminnalliset menot sisältävät myös digitaaliseen turvallisuuteen käytetyt henkilöstökustannukset. On kuitenkin mahdollista erottaa henkilöstökustannukset myös omaksi kustannuslajikseen.

	CAPEX	OPEX
Määritelmä	Investoinnit jotka ovat käytössä pitkään. Niiden hyödyt allokoituvat vuosien päähän.	Päivittäisen toiminnan rahoittamiseksi vaaditut menot. Hyödyt realisoituvat käyttöajanjaksolla.
Esimerkki	Laitteisto ja ohjelmistot.	Ohjelmistojen lisenssimaksut ja henkilöstökulut.
Käsittely kirjanpidossa	Kustannukset huomioidaan poistoina taloudellisen käyttöajan mukaisesti.	Kustannukset syntyvät käytön mukaisesti.

Taulukko 2. (Franklin ja Chee 2019)

Digitaalisen turvallisuuden kustannusten jaottelu pääoman ja toimintamenojen välillä on karkea jaottelu, joka ei mahdollista luotettavaa vertailua kustannusten ja niiden avulla saavutettujen hyötyjen välillä. Jotta riskien todennäköisyyksiä ja poikkeamista aiheutuneita menetyksiä voitaisiin peilata käytettyihin resursseihin, olisi kustannuslajittelun oltava hienojakoisempaa. Tämä on edellytys kustannus-vaikuttavuusanalyysin suorittamiselle. Pääomakustannusten ja toimintamenojen seuranta voi kuitenkin olla hyvä lähtökohta digitaalisen turvallisuuden kustannusten arviointiin, mikäli tarkempi kustannuslajittelu ei ole mahdollista.

4.3.2 NIST:n viitekehyksen mukainen kustannuslajittelu

Yhdysvaltain kauppaministeriön alainen kansallinen standardointi- ja teknologiainstituutti National Institute of Standards and Technology (NIST) ylläpitää ja julkaisee digitaalisen turvallisuuden ohjeistusta ja standardeja. NIST:n julkaisu *Cyber Security Framework for Improving Critical Infrastructure* (2018) tarjoaa viitekehyksen, joka sisältää viisi digitaalisen turvallisuuden toimintoluokkaa: tunnistus (identify), suojaustoimet (protect), havainnointi (detect), reagointi (respond) sekä palautuminen (recover). Toimintoluokkiin sisältyy yhteensä 22 alakategoriaa. Kyseinen toimintopohjainen viitekehys tarjoaa mahdollisuuden myös kustannusten budjetointiin ja vaikuttavuusarviointiin. NIST:n viitekehystä on tarkoitettu sovellettavan organisaatioiden toiminnallisten tavoitteiden arviointiin.

Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness & Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and events
	Security continuous monitoring
	Detection processes
Response	Response planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery planning
	Improvements
	Communications

Taulukko 3. NIST Cyber Security Framework

Toimintopohjaisen kustannusjaottelun vahvuutena on, että sen avulla panostuksilla saavutettavat hyödyt voidaan luotettavasti allokoida eri investoinneille. Mikäli kustannusten budjetointiin ja seuraamiseen käytetään karkeampaa jaottelua, kuten OPEX/CAPEX, on vaikeata arvioida eri toimenpiteiden ja investointien kustannustehokkuutta. Digitaalisen turvallisuuden kustannus-vaikuttavuusarvioinnin näkökulmasta on keskeistä kyetä luotettavasti vertaamaan eri investointien ja toimenpiteiden kustannuksia sekä niiden vaikutuksia riskien todennäköisyyksiin ja potentiaalisiin vaikutuksiin.

Vuonna 2017 Yhdysvalloissa velvoitettiin presidentin asetuksella kaikki liittovaltion hallituksen alaiset virastot NIST:n viitekehyksen käyttöön digitaalisen turvallisuuden riskien hallinnassa. Näin ollen viitekehyksen käyttö on lain mukaan pakollista Yhdysvaltain julkisessa hallinnossa. Asetuksessa mainittiin

myös, että kyberturvallisuuden budjetointia on tehtävä riskiarviontiin perustuen[2]. Tämän voidaan tulevaisuudessa nähdä johtavan kyseisen viitekehyksen hyödyntämiseen digitaalisen turvallisuuden kustannusten seurannassa ja suunnittelussa kansainvälisesti.

Esimerkiksi Yhdysvaltain energiaministeriön (Department of Energy) digitaalisen turvallisuuden budjetoinnissa sovelletaan kyseistä viitekehystä jyvittämällä kustannukset viitekehyksen viiteen toimintaluokkaan. Tämä mahdollistaa myös kustannusluokkia vastaavien konkreettisten mittareiden asettamisen toiminnoille ja alakategorioille. Ministeriön digitaalisen turvallisuuden strategiadokumentissa huomautetaan, että useimmat investoinnit ja digitaaliseen turvallisuuteen käytettävät resurssit eivät ole suoraan kohdistettavissa yksittäisiin kustannuslajeihin. Eri kokonaisuudet on näin ollen jaettava eri toimintojen välille tapauskohtaiseen arviointiin pohjautuen (Department of Energy 2018, 27). Ministeriön budjetoinnissa digitaalisen turvallisuuden kustannukset jaetaan kolmeen kategoriaan NIST:n viitekehyksen mukaisesti:

1) Tunnistus ja suojaustoimet – verkkojen ja tietojen suojaaminen (IDENTIFY and *PROTECT—Protecting Networks and Information*). Kategoria sisältää suojaustoimet ja investoinnit, joiden avulla organisaation verkkoja sekä tietoja suojataan riskeiltä. Esimerkiksi informaation suojaukseen käytettävästä teknologiasta ja henkilöstön koulutuksesta aiheutuvat kustannukset sisältyvät tähän kategoriaan.

2) Havainnointi ja reagointi – turvallisuuspoikkeamien tunnistaminen, analysointi ja lieventäminen (*DETECT and RESPOND—Detect, Analyze, and Mitigate Intrusions*). Kategoria sisältää esimerkiksi hyökkäyksentorjuntajärjestelmiin ja niiden ylläpitoon käytetyt resurssit, sekä poikkeamien havainnointiin liittyvät toimenpiteet ja prosessit.

[2]Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11, 2017. Kohta 1. (c). ii.

3) Palautuminen – digitaalisen toimintaympäristön strateginen muotoilu (RECOVER—*Shaping the Cybersecurity Environment Strategic Implementation*). Kolmanteen kustannuskategoriaan sisältyvät toimet käsittävät esimerkiksi riskien arviointiin liittyvät toimet, kriisiviestinnän sekä jatkuvuussuunnittelun.

Jokaiselle kategorialle voidaan määrittää konkreettisia tavoitteita, joiden avulla kustannusvaikuttavuutta seurataan. Sellaisenaan yllä mainitut kustannuskategoriat eivät kuitenkaan mahdollista luotettavaa digitaalisen turvallisuuden kustannus-vaikuttavuusarviointia. Suojaustoimien osalta voidaan määritellä niiden vaikutukset riskien odotusarvoihin, mutta esimerkiksi sisäisen viestinnän ja muiden tukitoimien vaikutuksia riskeihin ei voida suoraan määritellä. Siksi niistä aiheutuvat kustannukset on arvioinnissa kohdistettava konkreettisemmille suojaustoimille.

4.4 Digitaalisen turvallisuuden riskiarviointi

Riskiarviointi on hyvin tärkeää digitaalisen turvallisuuden vaikuttavuuden arvioinnin kannalta, sillä yksi keskeinen digitaaliseen turvallisuuteen panostamalla saavutettava hyöty, on riskien toteutumisesta aiheutuvien menetysten vähentäminen. Riskit voivat realisoituessaan vaikeuttaa julkisen hallinnon organisaatioiden toimintaa ja estää niiden yhteiskuntaa palvelevien tavoitteiden saavuttamisen. Digitaalisen turvallisuuden riskejä tulisikin entistä enemmän lähestyä yksinomaan teknisiä ratkaisuja vaativien teknisten ongelmien lisäksi taloudellisesta näkökulmasta. Siinä lähtökohtana on arvioida riskien potentiaaliset vaikutukset yhteiskunnalliselle arvolle, jota pyritään suojaamaan (OECD 2015, 4). Hyvinvointiteorian mukaisesti taloudellisella hyvinvoinnilla tarkoitetaan kansalaisten hyvinvointia (Puhakka 2017, 20). Riskejä tulisi siis vertailla taloudellisesti huomioimalla niiden potentiaaliset vaikutukset yhteiskunnan kokonaishyvinvointiin, sillä julkiseen sektoriin kohdistuvat menetykset allokoituvat aina lo-

pulta kansalaisille. Näin ollen taloudellinen näkökulma digitaalisen turvallisuuden riskeihin on edellytys sille, että digitaalisen turvallisuuden yhteiskunnallista vaikuttavuutta voidaan arvioida ja resursseja kohdistaa järkevällä tavalla.

Riskialtistuksen lisääntyessä on sekä yksityisellä sektorilla että julkisessa hallinnossa kasvava tarve panostaa digitaaliseen turvallisuuteen ja varmistaa riittävä osaaminen ja resursointi. Yhteiskunnalle tärkeiden tietoteknisten järjestelmien ja rakenteiden toimivuus on merkittävä huoltovarmuuskysymys, ja järjestelmiin kohdistuvien riskien arviointia on tehostettava jo normaalioloissa (TEM 2019, 18). Digitaaliseen turvallisuuteen kohdistuvat riskit ovat dynaamisia, sillä ne ovat usein monimutkaisia, nopeasti muuttuvia ja niiden syy-seuraussuhteet vaikeasti arvioitavissa olevia.

Jotta digitaalisen talouden mahdollistama hyvinvoinnin kasvu saadaan hyödynnettyä, on välttämätöntä ymmärtää digitaalisen turvallisuuden arvo sen mahdollistajana (OECD 2015, 2). Digitaalisen turvallisuuden vaikuttavuus, eli yhteiskunnallinen arvo, on nähtävä voimakkaasti riippuvaisena digitaaliseen toimintaympäristöön kohdistuvien riskien arvosta, ja riskialtistuksen kasvun myötä julkisella sektorilla on kasvava tarve investoida digitaaliseen toimintaan kohdistuviin riskeihin varautumiseen.

4.4.1 Valtiohallinnon riskienhallintamalli

Valtiovarain controller -toiminnon valtionhallinnon riskienhallintapolitiikkamalli on luonteeltaan laadullinen, eikä sen käyttäminen edellytä todennäköisyyksien ja vaikutusten numeerista arvioimista. Mallissa määritellään riskienhallinnan tavoitteet, vastuut ja menetelmät. Valtionhallinnon riskienhallintamallissa edellytetään myös riskeihin liittyvää tiedonvaihtoa toimintaympäristön eri osapuolten välillä.

Mallin mukaan riskienhallintaprosessi sisältää seuraavat viisi vaihetta:

- *Toimintaympäristön määrittely* sisältää päätökset reunaehdoista, joissa riskien vaikutukset arvioidaan. Reunaehtoja ovat esimerkiksi tarkastelussa rajattava aika, toimintaympäristö sekä riskikriteerit.

- *Riskien tunnistaminen* pitää sisällään esimerkiksi tiedon kokoamisen toimintaympäristöön vaikuttavista riskeistä ja riskien jaottelun neljään kategoriaan, jotka ovat strategiset, operatiiviset, taloudelliset sekä vahinkoriskit.

- *Riskianalyysissa* arvioidaan riskien todennäköisyyttä neliportaisella asteikolla, joka sisältää seuraavat tasot: epätodennäköinen, mahdollinen, todennäköinen ja lähes varma. Myös vaikutusten arviointiin malli tarjoaa neliportaisen asteikon: vähäinen, kohtalainen, merkittävä ja kriittinen.

- *Riskien merkityksen arvioinnissa* riskit pyritään järjestämään ja priorisoimaan niiden riskianalyysin tuloksena määritellyn vaikuttavuuden mukaisesti. Tässä voidaan käyttää riskimatriisia, jonka avulla tulosta voidaan myös kommunikoida visuaalisesti.

- *Riskien käsittelyssä* päätetään toimista, joilla riskiin reagoidaan. Riskiä voidaan esimerkiksi pyrkiä torjumaan kokonaan, pienentämään, jakamaan tai se voidaan hyväksyä.

Riskienhallintamallin neliportainen todennäköisyys- ja vaikuttavuusjaottelu ei huomioi kustannus-vaikuttavuus näkökulmaa parhaalla mahdollisella tavalla etenkään digitaalisen turvallisuuden osalta, jossa taloudellinen riskiarviointi on keskeinen tekijä.

4.4.2 Riskien kvantifiominen

Riskejä voidaan pyrkiä arvioimaan myös määrällisesti. FAIR Instituten julkaisema Factor Analysis of Information Security Risk –viitekehyksen avulla digitaalisen turvallisuuden riskien todennäköisyydet ja vaikutukset kuvataan numeerisesti. Viitekehys perustuu Monte Carlo – simulointimenetelmään, joka satunnaislukuja hyödyntäen luo hankkeen tai investoinnin riskiportfoliolle ennalta asetetun määrän skenaarioita, laskee skenaarioiden keskiarvot sekä näin muodostaa todennäköisyysjakauman riskien aiheuttamien menetysten odotusarvoille.

FAIR–viitekehyksessä riskien todennäköisyydelle ja niiden aiheuttamille menetyksille tulee määrittää niiden hajontaa kuvaavat kolmen pisteen estimaatit, jotka ovat pessimistinen, todennäköisin sekä optimistinen arvo. Viitekehyksessä riskit sisältävät seuraavat komponentit:

- Arvioitu frekvenssi: optimistinen, todennäköisin ja pessimistinen; (esimerkiksi 0,05; 1; 3)
- Haavoittuvuus: optimistinen, todennäköisin ja pessimistinen; (esimerkiksi 1% - 5% - 99%)
- Vaikutus, riskin toteutumisesta aiheutuva menetys: optimistinen, todennäköisin ja pessimistinen; (esimerkiksi 1000 - 2000 - 100 000)

Riskien aiheuttamat menetykset on jaoteltu seuraaviin kategorioihin:

- Tuottavuus (productivity). Esimerkkinä tuottavuuteen kohdistuvasta menetyksestä ovat toiminnan keskeytykset.
- Reagointi (response). Tämän kategorian menetykset aiheutuvat esimerkiksi digitaalisen turvallisuuden poikkeaman selvittämiseen käytetyistä resursseista.

- Korjauskustannukset (replacement). Esimerkiksi vaurioituneiden tai hävinneiden laitteiden korjaamiseen tai korvaamiseen käytetyt resurssit.
- Oikeudelliset seuraukset (fines and judgements). Esimerkiksi sakot.
- Kilpailulliset haitat (loss of competitive advantage). Menetetyt kilpailulliset mahdollisuudet.
- Maine (reputation). Luottamus kansalaisten ja muiden sidosryhmien keskuudessa.

Simuloinnin avulla saadaan määriteltyä riskiportfolion vaikutuksille määritetyllä luottamustasolla todennäköisyysjakauma, jonka perusteella voidaan arvioida järkevää resursointia menetysten välttämiseksi. (Freund ja Jones 2015).

Myös simulointia hyödyntävät riskiarviointimenetelmät perustuvat asiantuntijoiden määrittämään dataan, joten niiden tuloksena saatava informaatio ei välttämättä tuota lisäarvoa verrattuna laadullisiin menetelmiin. Riskiarvioinnin subjektiivisuutta ei siis voida poistaa myöskään simulointiin perustuvia menetelmiä hyödyntämällä. On myös mahdollista, että mallinnuksessa ei riittävästi huomioida erittäin epätodennäköisten, mutta toteutuessaan katastrofaalisten riskien mahdollisuutta.

Organisaatioiden tasolla huomattava osa digitaalisen turvallisuuden toimenpiteiden vaikutuksista on epäsuoria, eikä niiden vaikuttavuutta voida siten mitata suoraan suhteessa tiettyihin riskeihin. Esimerkiksi henkilökunnan koulutukseen käytettyjen resurssien vaikutuksia tiettyjen ennalta määriteltyjen riskien todennäköisyyksiin tai vaikutuksiin on haasteellista arvioida kvantitatiivisesti ennen toimenpiteen suorittamista tai sen jälkeen.

4.5 Lainsäädännössä asetettujen vaatimusten täyttäminen

Digitaalisen turvallisuuden kustannus-vaikuttavuusarviointia voidaan lähestyä myös lainsäädännön asettamien vaatimusten kautta. Yksi keskeisistä digitaalisen turvallisuuden panostuksilla saavutettavista tavoitteista on lainsäädännössä asetettujen velvoitteiden täyttäminen. Konkreettiset vaatimukset asettavat toiminnalle selkeät tavoitteet, joiden täyttämiseen vaadittavien toimien kustannuksia voidaan seurata ja arvioida. Digitaalisen turvallisuuden riskin toteutuminen saattaa aiheuttaa mittavia negatiivisia ulkoisvaikutuksia. Silloin menetykset eivät kohdistu ainoastaan siihen organisaatioon, jonka vastuulla olevan haavoittuvuuden johdosta riski toteutuu. Ulkoisvaikutusten johdosta yksittäisten toimijoiden investoinnit digitaaliseen turvallisuuteen voivat olla liian vähäisiä yhteiskunnan kokonaisedun näkökulmasta (Juuso ja Svento 2018, 194). Ulkoishaitan sisäistäminen tarkoittaa pyrkimystä yhdenmukaistaa yksittäisen organisaation optimaalinen resursointi sekä yhteiskunnan kannalta optimaalinen resursointi digitaaliseen turvallisuuteen. Negatiivisten ulkoisvaikutusten, eli ulkoishaittojen, sisäistämiseksi voidaan käyttää erilaisia ohjauskeinoja.

Digitaalisessa toimintaympäristössä informaation yhteiskunnallinen merkittävyys kasvaa. Näin ollen on entistä tärkeämpää kiinnittää huomiota informaation luotettavuuden, eheyden ja saatavuuden turvaamiseen (Kuusisto 2014, 44). Tietoturvallisuutta ja tiedonhallinnan yhdenmukaistamista kehittävä laki julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki 906/2019) tuli voimaan vuoden 2020 alussa. Lain tavoitteena on selkeyttää tiedonhallintaan liittyviä vastuita ja velvollisuuksia siirtämällä digitaalista turvallisuutta koskevat vaatimukset yhteen sääntelykokonaisuuteen (HE 284/2018, 36). Ennen lain voimaantuloa tiedonhallintaa koskevat säännökset olivat hajallaan eri laeissa. Laissa myös konkretisoitiin säännöksiä hyvästä tietojenhallinnasta, vaikkakin monilta osin säännösten ydinsisältö pysyi muuttumattomana. Lainsäädännön ennakoitavuuden, yksityiskohtaisuuden ja johdonmukaisuuden parantuessa julkisen hallinnon organisaatiot voivat aiempaa helpommin varmistua omien tiedonhallintaprosessiensa lainmukaisuudesta.

Tiedonhallintalain 13 §:ssä mainitaan, että tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava turvallisuustoimenpiteet sen mukaisesti. Digitaalisen turvallisuuden kustannus-vaikuttavuuden kannalta on keskeistä, että turvallisuuspanostukset kohdistetaan tarkoituksenmukaisesti. Tämä voidaan saavuttaa priorisoimalla turvallisuustoimet taloudellisesta näkökulmasta kohdistaen resurssit suojattavien kohteiden arvon, sekä arvoon kohdistuvien uhkien mukaisesti.

Digitaaliseen turvallisuuteen tähtäävät prosessit pyrkivät estämään riskin toteutumista sekä minimoimaan riskin toteutumisesta aiheutuvia menetyksiä. Uuden tiedonhallintalain hyötynä onkin se, että laki pyrkii luomaan tiedonhallintayksiköille aiempaa paremmat edellytykset reagoida muutos- ja häiriötilanteisiin (HE 284/2018, 36). Tiedonhallintalain tavoitteena on myös tehostaa kertaalleen kerätyn tiedon hyödyntämistä, mistä koituu julkisen hallinnon organisaatioille kustannushyötyjä (HE 284/2018, 36).

Vaikka lainsäädännön vaatimustenmukaisuus on oltava lähtökohtana digitaaliselle turvallisuudelle, ei sitä kuitenkaan tulisi nähdä ainoana tavoitteena. Vaatimustenmukaisuus ei takaa tehokasta riskien hallintaa tai hyvää turvallisuuden tasoa organisaatioissa. Pelkästään vaatimustenmukaisuuden tavoitteekseen ottavat organisaatiot voivat suhtautua turvallisuuteen mekanistisesti ja jättää huomiotta toimintaympäristönsä erityispiirteet ja muut relevantit seikat, joita ei ole huomioitu lainsäädännössä.

4.6 Keskitetty kokonaiskuvapalvelu ja tiedon jakaminen

Vahvasti verkottuneessa julkisen hallinnon tieto- ja viestintäteknisessä ympäristössä toimintavarmuuden varmistamiseksi ja kustannustehokkuuden kehittämiseksi on tärkeää ylläpitää ajankohtaista tilannekuvaa ja jakaa tietoa.
Tämä huomioidaan seuraavalla tavalla myös valtiovarain controller- toiminnon

riskienhallintapolitiikkamallin suosituksessa: ”*Valtionhallinnon virastojen toiminta kytkeytyy toisten virastojen sekä muiden yhteistyökumppaneiden ja sidosryhmien toimintaan. Virastojen tehokas riskienhallinta edellyttää riittävää tiedonvaihtoa näiden kanssa. Merkittävistä riskeistä ja riskienhallintatoimista tulee viestiä tulosohjaavalle ministeriölle.”*

Tällä hetkellä Suomessa esimerkiksi Kyberturvallisuuskeskus ylläpitää ja tuottaa digitaalisen turvallisuuden tilannekuvaa organisaatioiden ja kansalaisten käyttöön. Kyberturvallisuuskeskus tuottaa tietoa esimerkiksi digitaalisen turvallisuuden haavoittuvuuksista, uhkista ja toteutuneista poikkeamatilanteista.

Digitaalisen turvallisuuden riskeihin ja resursointiin liittyvän informaation niukkuutta pidetään yhtenä suurimmista ongelmista digitaalisen turvallisuuden tason arvioinnin kannalta (Moore, Dynes ja Chang, 2016, 2). Digitaalisen turvallisuuden kustannustehokkuuden parantamiseksi julkisen hallinnon toimijat voisivat hyötyä tehokkaammasta digitaalisen turvallisuuden riskeihin, suojaustoimiin, käytäntöihin ja ajankohtaisiin asioihin liittyvän tiedon jakamisesta. Taloudelliset päätökset investoinneista digitaaliseen turvallisuuteen tehdään aina epätäydellisen tiedon pohjalta, ja alati muutoksessa olevien digitaalisen turvallisuuden riskikuvien ylläpitäminen on haasteellista. Ei siis voida olla varmoja siitä, kuinka tehokkaasti turvallisuuteen käytettävät resurssit synnyttävät hyötyjä, joista keskeisimpiä on turvattaviin kohteisiin kohdistuvien riskien väheneminen ja niiden vaikutusten pienentyminen. Näin ollen riskeihin liittyvän tiedon määrällä ja laadulla on paljon vaikutusta kustannustehokasta ja tarkoituksenmukaista digitaalisen turvallisuuden resursointia tavoiteltaessa (Juuso ja Svento 2018, 195). Tiedon avulla muut julkisen hallinnon toimijat kykenevät paremmin havaitsemaan toimintaansa vaikuttavia digitaalisen turvallisuuden riskejä, ja näin varautumaan niihin paremmin. Riskitiedon lisäksi tietojen jakaminen eri suojaustoimien ja –menetelmien toimivuudesta hyödyttävät muita organisaatioita, vaikuttaen siten koko yhteiskunnan digitaaliseen turvallisuuteen.

5 YHTEENVETO HAASTATTELUISTA

Selvitystyön yhteydessä toteutettujen haastatteluiden tavoitteena oli kartoittaa julkisen hallinnon organisaatioiden käytäntöjä digitaalisen turvallisuuden kustannus-vaikuttavuusarvioinnissa. Haastatteluiden keskeiset havainnot, havaintojen kuvaukset ja tunnistetut kehitystoimenpiteet on esitelty teemoittain tässä kappaleessa.

5.1 Riskien arviointi julkisessa hallinnossa

Haastateltavien mukaan julkisen hallinnon organisaatioissa ei arvioida digitaaliseen turvallisuuteen kohdistuvia riskejä irrallaan muista toiminnan riskeistä. Riskejä arvioidaan useimmiten järjestelmähankintojen yhteydessä erillisenä hankintaprosessin vaiheena tai osana tieto- ja viestintäteknologian operatiivisia riskejä. Haastateltavat arvioivat digitaaliseen turvallisuuteen liittyvien riskien erittelemisessä haasteeksi etenkin riskien eriyttämisen muista riskeistä ja niiden systemaattisen kategorisoinnin puutteet.

Haastatelluilla organisaatioilla ei ole yhteisesti käytössä olevaa digitaalisen turvallisuuden riskien arviointimallia. Monissa julkisen hallinnon organisaatioissa riskienarvioinnissa hyödynnetään valtiovarain controller -toiminnon valmistelemaa riskienhallintamallia tai VAHTI-ohjeiden riskienhallintapolitiikkaa. Haastateltavien mukaan heidän organisaatioissaan riskienhallintaa toteutetaan ja dokumentoidaan erilaisten kaupallisten ohjelmistojen avulla.

Riskien osalta havainnot ovat pääosin yhteneväisiä vuonna 2019 Valtiovarainministeriön toteuttaman riskienhallintakyselyn tulosten kanssa. Kyselyn tulosten mukaan suurin osa kyselyyn osallistuneista valtion virastoista ei verrannut riskienhallinnan toimenpiteiden avulla saavutettavia hyötyjä niistä aiheutuneisiin kustannuksiin (Valtiovarainministeriö 2019, 35).

Luokittelu	Havainto	Kehitystoimenpiteet
Digitaalisen turvallisuuden riskien arviointi	Haastatteluiden perusteella digitaalisen turvallisuuden riskejä arvioidaan pääsääntöisesti osana organisaatioiden kokonaisturvallisuudenhallintaa.	Digitaalisen turvallisuuden riskien arviointiin olisi suositeltavaa laatia yleinen luokittelumalli, jota julkisen hallinnon organisaatiot voisivat hyödyntää sekä hankkeiden, että toiminnan digitaalisen turvallisuuden riskien tunnistamisessa ja arvioinnissa
	Osa organisaatioista on eriyttänyt tieto- ja viestintäteknologian omaksi riskikategoriakseen.	
	Riskejä arvioidaan uusien hankintojen yhteydessä.	
	Osa haastatelluista organisaatioista arvioi digitaalisen turvallisuuden riskejä toiminnallisten ja rahamääräisten vaikutusten, sekä sidosryhmiin kohdistuvien vaikutusten perusteella.	
Riskienhallintamalli	Riskiarvioinnissa hyödynnetään valtiovarain controller -toiminnon valmistelemaa riskienhallinnan mallia	
	Riskiarvioinnissa hyödynnetään VAHTI:n julkaisemien ohjeiden riskienhallintapolitiikkaa käsittelevää osiota.	
	Riskien todennäköisyydet ja vaikutukset luokitellaan kriittisyyden mukaisesti neliportaiselle asteikolle.	
Vaikutusten arviointi	Turvattavia kohteita arvioidaan sanallisesti, ei rahamääräisesti.	
	Riskien toteutumisen seurauksia sidosryhmiin ei ole arvioitu.	

Taulukko 4. Riskien arviointiin liittyvät havainnot ja kehitystoimenpiteet

5.2 Kustannusten seuranta

Haastateltavien mukaan digitaalisen turvallisuuden kustannukset eivät ole oma kustannuserä julkisen hallinnon organisaatioissa. Digitaalisen turvallisuuden

kustannukset tunnistetaan organisaatioissa olevan osittain päällekkäisiä muiden kustannuserien kanssa, eikä niitä sen vuoksi käsitellä erikseen. Päällekkäisyyksiä nähtiin erityisesti muiden turvallisuuskustannusten, hankintojen ja henkilöstökulujen kanssa. Julkisen hallinnon organisaatiot saavat lisäksi monet käyttämistään palveluista valtion yhteisten keskitettyjen palveluiden kautta, eikä organisaatioilla täten ole itsellään tarkkaa tietoa näihin hyödyntämiinsä palveluihin tehdyistä turvallisuustoimenpiteistä tai niiden kustannuksista.

Julkisen hallinnon organisaatioissa ei ole haastateltavien mukaan arvioitu systemaattisesti tehtyjen digitaalisen turvallisuuden toimenpiteiden rahamäärällisiä vaikutuksia. Vaikutusten rahamäärällisen arvioinnin koettiin perustuvan epävarmoihin ennusteisiin, joiden laatimiseksi vaadittaisiin merkittävästi enemmän vertailukelpoista dataa. Haastateltavat arvioivat toiminnan katkoksista johtuvien kustannusten arvioinnin mahdolliseksi, mutta epäsuorien kustannusten ja vaikutusten arvioimisen erittäin hankalaksi.

Luokittelu	Havainto	Kehitystoimenpiteet
Digitaalisen turvallisuuden kustannukset	Digitaaliseen turvallisuuteen kohdistettuja resursseja ei eritellä toimintamenomomenteilla.	Kustannusten jaotteluun olisi suositeltavaa olla yksityiskohtainen ja yleistettävä malli, jota jokainen julkisen hallinnon organisaatio voisi hyödyntää.
	Riskien pienentämistoimenpiteiden tuottamaa arvoa ei arvioida kvantitatiivisesti niiden ennustettavuuden epävarmuuden vuoksi.	
Suojaustoimenpiteiden kustannukset	Turvattavien kohteiden suojausta parantavia toimenpiteitä kartoitetaan ja priorisoidaan riskiarvioinnin perusteella.	Suojaustoimenpiteiden kustannuksia ja niistä mahdollisesti seuranneita vaikutuk-

	Suojaustoimenpiteiden vaikuttavuutta ei arvioida suhteessa toimenpiteiden kustannuksiin.	sia olisi suositeltavaa dokumentoida tarkemmin ja arvioida toimien avulla saavutettuja hyötyjä suhteessa arvioituihin riskeihin.
	Turvattavien kohteiden suojaustoimenpiteiden vaatimia työmääriä ei arvioida toimenpiteittäin.	
	Epäsuorien vaikutusten rahallista arvoa on vaikea määritellä.	
	Organisaatioilla ei ole asiakkaan roolissa ollessaan tietoa palveluntarjoajien tai niiden käyttämien yksityisten palveluntuottajien turvallisuuden toimenpiteiden kustannuksista tai niiden vaikuttavuudesta.	
Toteutuneiden riskien aiheuttamat menetykset	Pienemmistä digitaalisen turvallisuuden poikkeamista aiheutuneista menetyksistä ei tällä hetkellä kerätä systemaattisesti tietoa.	
	Riskin realisoitumisesta aiheutuneita taloudellisia menetyksiä kartoitetaan usein vain rikosilmoitusten yhteydessä.	

Taulukko 5. Kustannusten seurantaan liittyvät havainnot ja kehitystoimenpiteet

5.3 Tunnistetut kehityskohteet

Haastattelujen perusteella julkisen hallinnon organisaatioilla on tarve yhtenäiselle ja selkeälle tavalle tunnistaa, luokitella ja arvioida digitaaliseen turvallisuuteen liittyviä riskejä, turvaamiseen liittyvien suojaustoimenpiteiden kustannuksia, sekä tehdyistä toimenpiteistä saavutettavia hyötyjä. Tätä varten olisi suositeltavaa laatia selkeä toimintamalli, jota kukin organisaatio voisi hyödyntää suojaustoimenpiteiden kustannusten ja vaikuttavuuden arvioimisessa toimialasta ja organisaation toiminnan luonteesta riippumatta.

Digitaalisen turvallisuuden toimenpiteiden vaikuttavuuden arvioimiseksi haastatteluissa nousi esiin tarve kerätä ja jakaa organisaatioiden välillä systemaattisesti tietoja digitaaliseen turvallisuuteen kohdennetuista toimenpiteistä, toimenpiteiden kustannuksista ja niiden vaikutuksista. Erityisesti toimenpiteiden vaikutusten rahamääräiseen arvioimiseen kaivattiin nykyistä enemmän taustatietoa ennusteiden laatimisen tueksi. Tiedon systemaattista keräämistä ja jakamista varten olisi suositeltavaa laatia julkisen hallinnon organisaatioille keskitetty tilannekuvapalvelu, jota organisaatiot voisivat hyödyntää arviointiensa tukena. Tilannekuvapalvelu mahdollistaisi myös koko julkisen hallinnon digitaalisen turvallisuuden kustannusten yhtenäisen kartoittamisen.

6 SUOSITUKSET KUSTANNUS-VAIKUTTAVUUDEN ARVIOINNIN KEHITTÄMISEKSI

Tässä kappaleessa on esitetty ehdotus julkisen hallinnon digitaalisen turvallisuuden kustannus-vaikuttavuuden arvioinnin kehittämiseksi. Kappaleessa kuvataan malli digitaalisen turvallisuuden rahamääräisen vaikuttavuuden arviointiin, sekä digitaalisen turvallisuuden kustannusten jaotteluun ja malli laadullisen vaikuttavuuden mittaamiseen.

Selvityksen perusteella julkisen hallinnon organisaatioiden olisi suositeltavaa arvioida organisaation digitaalisen turvallisuuden vaikuttavuutta säännöllisesti. Tämä mahdollistaa eri toimenpidevaihtoehtojen kannattavuuden vertailun digitaalisen turvallisuuden toimenpiteitä suunniteltaessa. Turvallisuuspanostusten vaikuttavuutta tulisi seurata systemaattisesti jälkitarkastelun kautta.

6.1 Suositus digitaalisen turvallisuuden rahamääräiseen arviointiin

Julkisen hallinnon organisaatioiden tulisi tunnistaa organisaation toimintaan kohdistuvat riskit, sekä kohteet, joita riskeiltä halutaan suojella. Suojaustoimenpiteitä suunniteltaessa tulisi tunnistaa myös vuosittainen odotusarvo riskien realisoitumisesta aiheutuville kustannuksille, mikäli suojattaville kohteille ei toteuteta lainkaan digitaalisen turvallisuuden suojaustoimenpiteitä. Riskien arvioinnissa tulee huomioida kriittiset riippuvuudet, joiden johdosta riskien toteutumisen vaikutukset aiheuttavat seurauksia myös muille kuin organisaatiolle itselleen. Tätä kustannusta voidaan käyttää vertailtaessa teoreettisena maksimihyötynä, joka suojaustoimenpiteillä voidaan saavuttaa.

6.1.1 Turvattavien kohteiden määrittely ja menetysten odotusarvon laskeminen

Turvattavien kohteiden arvo tulisi arvioida. Turvattavia kohteita ovat esimerkiksi tiedonhallintalain tarkoittaman tiedonhallintayksikön merkittävimmät tietovarannot, sekä keskeiset palvelut. Kunkin turvattavan kohteen merkittävimmät riskit tulisi tunnistaa. Tunnistetulle riskille tulisi laskea rahamääräinen odotusarvo perustuen riskin realisoitumisen todennäköisyyteen ja realisoitumisen potentiaalisesti aiheuttamiin kustannuksiin. Koska kustannusten odotusarvojen laskeminen on viitteellistä arvioiden laatimisen epätarkkuuden vuoksi, voitaisiin arvio esittää karkeasti suuruusluokassa, joka suhteutetaan tiedonhallintayksikön vuosittaiseen talousarvioon. Kustannuksia voitaisiin arvioida esimerkiksi toiminnan katkoksista aiheutuvien menetysten, ongelman korjaamiseksi tarvittavien työtuntien tai luottamuksellisen tiedon menetyksistä aiheutuvien kulujen avulla. Arvioon tulisi pyrkiä sisällyttämään myös laadulliset kustannukset ja asiakkaille tai kolmansille osapuolille riskin realisoitumisesta aiheutuvat kustannukset, vaikka niiden vaikutus näkyykin usein epäsuorasti.

6.1.2 Suojaustoimien vaikuttavuus ja nettoarvo

Digitaalisen turvallisuuden riskien potentiaalisilta menetyksiltä suojaavien toimenpiteiden vaikuttavuutta tulisi arvioida tunnistettujen riskien rahamääräisiin odotusarvoihin verrattuna. Pääsääntöisesti tiedonhallintayksikön asiantuntijoiden tulisi tehdä vaikuttavuuden arviointi. Ulkoisesti tuotettujen palveluiden osalta palveluntoimittajalta olisi suositeltavaa pyrkiä selvittämään palveluun tehtyjen digitaalisen turvallisuuden toimenpiteiden kustannuksia. Näiden palveluiden digitaalisen turvallisuuden toimenpiteiden vaikuttavuutta tulisi arvioida myös virastoissa.

Toteutettavien suojaustoimenpiteiden tarkoituksena on pienentää suojattaviin kohteisiin kohdistuvien riskien aiheuttamien kustannusten odotusarvoa ja saattaa jäännösriski hyväksytylle tasolle. Toimenpiteiden taloudellinen nettoarvo

(T) saadaan laskettua vähentämällä suojaustoimenpiteistä aiheutuneet kustannukset (I) riskien aiheuttamien kustannusten odotusarvosta eli potentiaalisista menetyksistä (Z), eli T = Z – I. Tätä taloudellista nettoarvoa voidaan hyödyntää julkisen hallinnon digitaalisen turvallisuuden kustannusten vaikuttavuuden arvioimisessa.

Tiedonhallintayksikön riskien ja suojaustoimenpiteiden dokumentoinnin ohjeellinen malli on seuraava:

Riski	Kuvaus	Todennäköisyys	Arvioitu frekvenssi	Vaikutukset	Menetykset	Hallinta	Vastuu	Kustannus	Vaikuttavuus	Seuranta
Nimi	Riskin kuvaus ja lähde	Riskien toteutumisen todennäköisyys arvioidulla ajanjaksolla, esim. asteikolla 1-4	Riskien esiintyvyys arvioidulla ajanjaksolla	Riskin vaikutus; riskien kriittisyyden perusteella, esim. asteikolla 1-4.	Arvioidut menetykset (U) jos riski toteutuisi.	Valittavat suojaustoimet	Riskin hallinnasta vastuullinen taho	Valittujen suojaustoimien kustannukset (I)	Digitaalisen turvallisuuden vaikuttavuus (T). T=Z-I jossa Z=menetysten pieneneminen	Suojaustoimien vaikuttavuuden seuranta

Taulukko 6. Malli vaikuttavuuden dokumentointiin

Mallia ja sen kuvausta on tarkoitus täsmentää digitaalisen turvallisuuden kustannus-vaikuttavuusarvioinnin ohjeistuksen laadinnan aikana. Liitteessä 5 on malliin liittyvä esimerkkilaskelma.

6.1.3 Suositus digitaalisen turvallisuuden kustannusten suunnitteluun ja seurantaan

Tiedonhallintayksiköiden olisi suositeltavaa ottaa käyttöön yhteinen menetelmä digitaalisen turvallisuuden menetysten arviointiin sekä resurssien budjetointiin ja seurantaan. Näin saataisiin digitaalisen turvallisuuden johtamisen tueksi ajantasaista tilannekuvaa digitaalisen turvallisuuden riskeistä sekä toimenpiteiden kustannuksista ja vaikuttavuudesta koko julkisessa hallinnossa.

Potentiaalisten menetysten arvioinnissa tarkastelu voisi tapahtua esimerkiksi luvussa 3.2. kuvatussa SAINT-projektissa käytetyllä tavalla, seuraavat näkökulmat huomioiden: immateriaalioikeudelliset menetykset, toiminnan keskeytykset, datan ja ohjelmistojen menetykset, rikoksisista aiheutuvat tappiot, luottamuksellisen tiedon vuotamisesta aiheutuvat seuraukset, korvausvelvollisuudet kolmansille osapuolille, vaikutukset maineeseen, fyysiseen omaisuuteen kohdistuvat menetykset, terveyteen kohdistuvat haitat ja poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset.

Digitaalisen turvallisuuden menetysten rahamääräiseen arviointiin, sekä menetysten pienentämiseksi tehtävien digitaalisen turvallisuuden toimenpiteiden kustannusten suunnitteluun ja seurantaan hyödynnettävän viitekehyksen tulisi mahdollistaa sekä määrällisten että laadullisten kustannusten seurannan ja sen tulisi mahdollistaa yhdenmukainen vertailtavuus tiedonhallintayksiköiden toiminnan luonteesta riippumatta. Kappaleessa 4.3.2 kuvattua NISTin kyberturvallisuuden arvioinnin viitekehystä tai siitä sovellettua mallia voitaisiin hyödyntää digitaalisen turvallisuuden toimenpiteiden kustannusten seurantaan tiedonhallintayksiköissä. Käytännössä tämä tarkoittaisi sitä, että määritetäisiin oheisen taulukon mukaisesti jokaiselle käsiteltävälle asialle olennaisen osa-alueen rahamääräinen arvo.

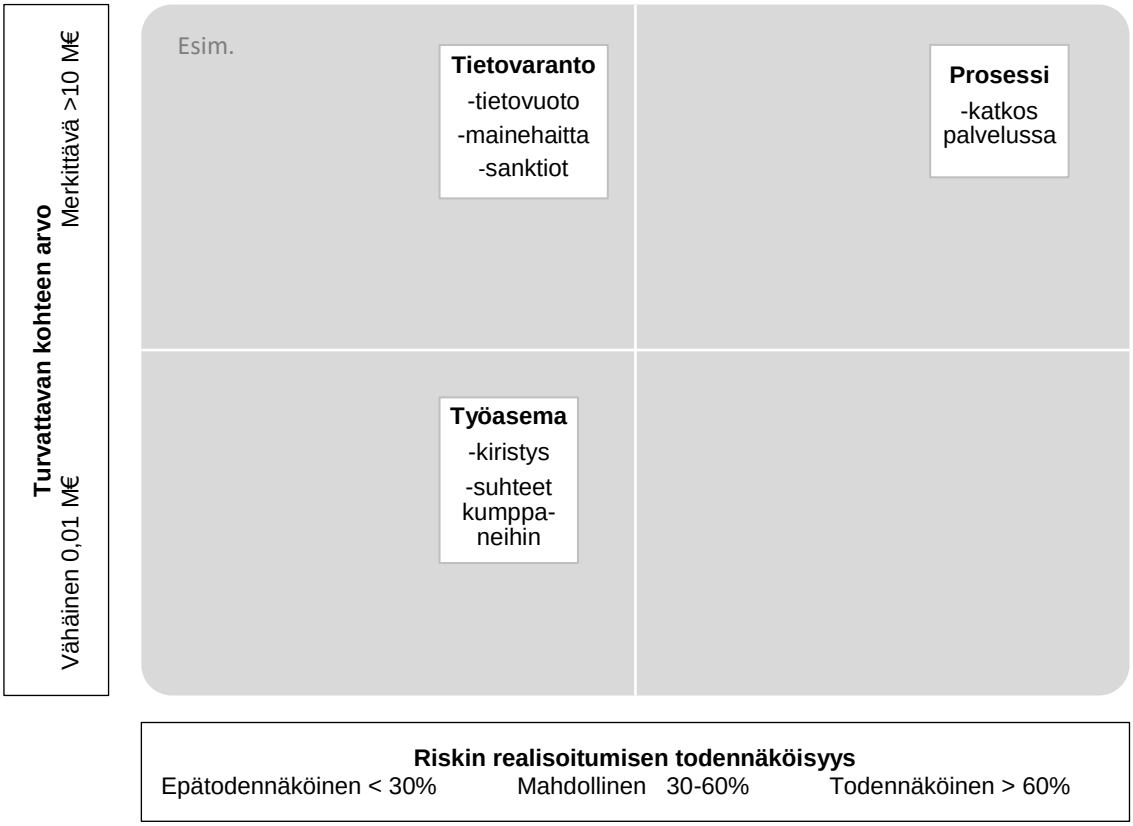
Tunnistus	Omaisuuden hallinta
	Liiketoimintaympäristö
	Hallinto
	Riskiarviointi
	Riskienhallintastrategia
Suojaus	Kulunvalvonta
	Tietoisuus & koulutus
	Tietoturvallisuus
	Tietosuojaprosessit ja – menettelyt
	Ylläpito
	Suojausteknologia
Havainnointi	Poikkeamat ja tapahtumat
	Turvallisuuden jatkuva seuranta
	Havaitsemisprosessit
Reagointi	Reagointisuunnittelu
	Viestintä
	Analysointi
	Lievennys
	Parannukset
Palautuminen	Toipumissuunnitelma
	Parannukset
	Viestintä

Taulukko 7. NIST Cyber Security Framework

NIST:n viitekehyksen soveltumista ajateltuun tarkoitukseen on tarkoitus selvittää tarkemmin mallin tarkentamisen yhteydessä.

6.2 Digitaalisen turvallisuuden kustannusten säännöllinen arviointi

Digitaalisen turvallisuuden riskien tunnistaminen ja niistä aiheutuvien kustannusten arviointi on suositeltavaa sitoa osaksi organisaation säännöllistä riskiarviointia. Säännöllisen riskiarvioinnin avulla voidaan laatia organisaatiolle digitaalisen turvallisuuden riskiportfolio, jossa riskit jaotellaan niiden vaikutusten mukaisesti. Riskien vaikutukset tulisi luokitella suojattavan kohteen arvon ja riskin realisoitumisen todennäköisyyden perusteella. Alla olevassa kuviossa on esitelty ehdotus riskien luokittelulle.



Kuva 4. Riskien arviointi

Suojattaville kohteille kohdistuvien riskien luokittelun avulla voidaan arvioida ja vertailla toteutettavien suojaustoimenpiteiden kustannuksia. Vertailussa tulisi huomioida

1) arvio turvallisuuspoikkeamien aiheuttamista menetyksistä, mikäli toimintaa jatketaan käytössä olevilla suojaustoimenpiteillä, sekä

2) arvio turvallisuuspoikkeamien aiheuttamista menetyksistä, mikäli toteutetaan suunniteltuja digitaalisen turvallisuuden lisätoimenpiteitä, sekä arvio näiden lisätoimenpiteiden kustannuksista esimerkiksi seuraavan JTS-kauden aikana. Lasketaan menetysten nettoarvio lisäämällä lisätoimenpiteiden arvioidut kustannukset arvioon menetyksistä.

Näiden kahden arvion erotuksella saadaan laskettua digitaalisen turvallisuuden rahamääräinen vaikuttavuus määritellyllä aikavälillä. Tehtyjen arvioiden toteutumista tulisi seurata systemaattisesti tulevien arvioiden parantamiseksi.

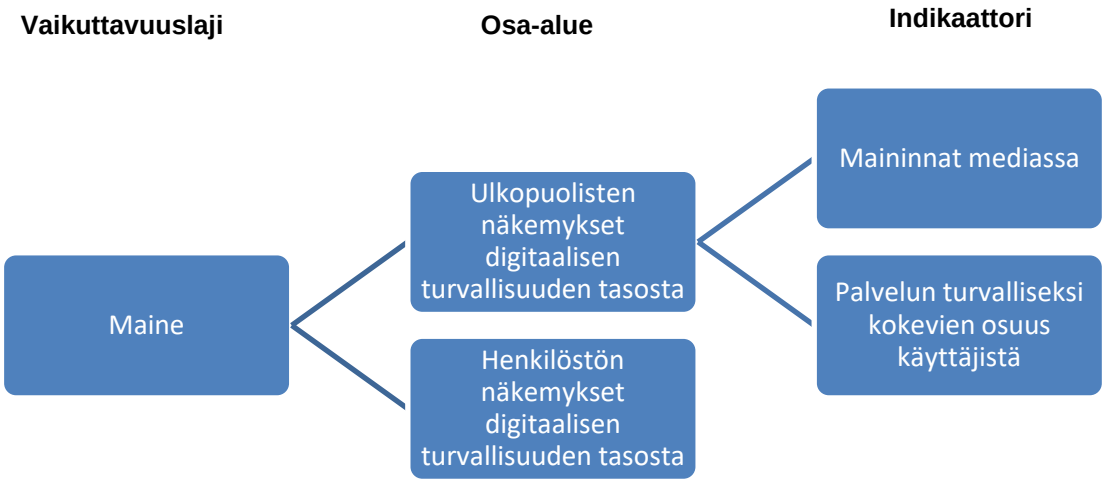
6.3 Laadulliset vaikuttavuusindikaattorit

Digitaalisen turvallisuuden toimenpiteiden vaikuttavuutta tulisi arvioida määrällisten indikaattoreiden lisäksi myös laadullisten indikaattoreiden kautta. Digitaalisen turvallisuuden toimenpiteillä on usein vaikutusta myös esimerkiksi kansalaisten tai henkilöstön luottamukseen tiedonhallintayksikön toiminnan turvallisuudesta. Laadullisten indikaattoreiden tavoitteena on mahdollistaa suojaustoimenpiteiden vaikuttavuuden mittaaminen osana kustannus-vaikuttavuusarviointia.

Laadullista vaikuttavuutta tulisi mitata esimerkiksi tiedonhallintayksikön henkilöstölle tai sidosryhmille toteutettavalla kyselyllä. Kyselyssä pyydetään vastaajia arvioimaan subjektiivisesti digitaalisen turvallisuuden toimenpiteiden vaikutuksia tunnistettuihin indikaattoreihin. Kysely tulisi toteuttaa säännöllisesti osana muuta digitaalisen turvallisuuden riskien arviointia. Tämän lisäksi laadullisia indikaattoreita voitaisiin arvioida esimerkiksi säännöllisen mediaseurannan avulla.

Selvitystyön perusteella on laadittu liitteessä 4 esitetyt indikaattorit mittaamaan digitaalisen turvallisuuden laadullisia vaikutuksia. Indikaattorit voidaan kytkeä osaksi alla esiteltyä vaikutuskarttaa, jonka avulla laadullisia vaikutuksia voidaan luokitella systemaattisesti (Goebel ja Metsäranta 2007, 27).

Käytettävät mainetta ja turvallisuuskulttuuria seuraavat (tietoisuus, asenne, osaaminen) mittarit kannattaa valita harkiten, niiden seurantaa tulee toteuttaa pitkäjänteisesti ja niiden perusteella tulee tehdä digitaalisen turvallisuuden ohjaus- sekä resursointipäätöksiä.



Kuva 5. Esimerkki laadullisen vaikuttavuuden indikaattoreista

6.4 Kehityshankkeiden digitaalisen turvallisuuden vaikuttavuuden arvioinnista

Digitaalisen turvallisuuden kustannus-vaikuttavuusanalyysimallin mukaista arviointia suositellaan myös tiedonhallintalain mukaiseen lausuntomenettelyyn sisältyville digitalisoitumista edistäville hankkeille. Erityisen tarpeen tämä on turvallisuutta edistäville hankkeille. Tarkastelun avulla voidaan vertailla eri toimenpidevaihtoehtojen kannattavuutta. On syytä huomioida, että riskien arvottamiseen perustuvan kustannus-vaikuttavuusanalyysin tulokset ovat aina suuntaa-antavia, eivätkä ne voi olla täysin vertailukelpoisia tiedonhallintayksiköiden välillä. Epävarmuuden hahmottamiseksi tulee tarkastella skenaarioita, joissa oletetaan erilaisia arvoja keskeisille tekijöille.

Suojattaviin kohteisiin kohdistuviin riskeihin suunniteltuja toimenpiteitä tulisi arvioida toimenpiteistä aiheutuvien kustannusten kautta. Suorien kustannusten lisäksi tiedonhallintayksikön tulisi huomioida myös suojaustoimenpiteestä ai-

heutuvat epäsuorat kustannukset, kuten esimerkiksi toimenpiteeseen käytettävä työaika tai järjestelmän käytön mahdolliset katkokset. Suojaustoimenpiteiden vaikutusten vertailemiseksi toimenpiteistä aiheutuvat kustannukset tulisi jaotella kustannuslajeittain kussakin tiedonhallintayksikössä. Alla olevassa taulukossa on esitelty ehdotus suojaustoimenpiteiden kustannuslajeista, jonka avulla tiedonhallintayksikkö voisi valmistella digitaalisen turvallisuuden kustannus-vaikuttavuuden osana riskiarviointia ja koko hankkeen kustannus/hyöty-analyysiä.

Kustannuslaji	Esimerkki
Suunnittelukustannukset	Markkinatutkimus ja suunnittelu
Investointikustannukset	Laitteet, palvelut ja ohjelmistot
Ylläpito- ja käyttökustannukset	Työaika, laadunvalvonta, lisenssimaksut ja konsulttipalkkiot
Haittakustannukset	Investointi digitaalisen turvallisuuteen hidastaa toimintaa, vaikuttaa negatiivisesti tehokkuuteen tai mukavuuteen
Muut	Käytöstä poistamisen kustannukset, laitteiston kierrättäminen.

Taulukko 8. Suojaustoimenpiteiden kustannuslajit

Digitaalisen turvallisuuden kustannus-vaikuttavuuden arviointiin on hankkeidenkin osalta perusteltua sisällyttää myös laadullista arviointia. Tätä on kuvattu kappaleessa 6.2.

7 Johtopäätökset

Selvityksessä laadittiin haastattelujen ja kirjallisuuskatsauksen perusteella ehdotus digitaalisen turvallisuuden kustannus-vaikuttavuuden arviointiin. Ehdotus sisältää menetelmän riskien arvottamiseen sekä kustannusten budjetoinnissa ja arvioinnissa hyödynnettävän kehikon, ja laadullisen vaikuttavuuden indikaattoreita. Ehdotuksen tarkoituksena on saada aikaan digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyvöittäminen. Ehdotus siten tukisi digitaaliseen turvallisuuteen käytettyjen resurssien ja niiden avulla saavutettavien hyötyjen vertailua. Ehdotuksen avulla digitaalisen turvallisuuden taloudellista ja laadullista vaikuttavuutta voitaisiin arvioida sekä verrata käytettyihin resursseihin nykyisiä käytänteitä paremmin.

Digitaalisen turvallisuuden kustannus-vaikuttavuuden arvioinnin tulee perustua mitattavissa oleviin hyötyihin, joita digitaaliseen turvallisuuteen tehtävillä panostuksilla voidaan saavuttaa. Kaikkea digitaaliseen turvallisuuteen tehdyillä panostuksilla saavutettavaa vaikuttavuutta ei voida mitata rahamääräisesti. Näin ollen ehdotuksessa on myös laadullisia indikaattoreita, joiden avulla myös esimerkiksi tiedonhallintayksikön maineeseen liittyviä tekijöitä pystytään mittaamaan ja seuraamaan. Ehdotusta on tarkoitus pilotoida vuoden 2020 aikana valtiovarainministeriössä.

Selvityksen jatkotehtävänä on ehdotuksen tarkentaminen sekä soveltaminen sekä valtionhallinnossa että kuntasektorilla. Julkisen hallinnon digitaalisen turvallisuuden kustannus-vaikuttavuusarvioinneissa on huomioitava laajasti riskien toteutumisesta aiheutuvat yhteiskunnalliset vaikutukset, eivätkä ne voi rajoittua vain yksittäisen viraston sisäisiin kustannuksiin ja hyötyihin. Tulee siis huomioida myös asiakkaille, yhteistyökumppaneille sekä muualla yhteiskunnassa riskin realisoitumisesta aiheutuvat menetykset. Julkisen hallinnon perustietotekniikkapalvelujen tuotanto on pitkälti keskitetty valtion osalta Valtion

tieto- ja viestintätekniikkakeskus Valtoriin sekä kuntien osalta kuntien ja kuntayhtymien ICT-yhtiöihin. Tällöin keskiöön nousee keskinäisriippuvuudet ja keskitettyjen palvelujen merkittävyyden erilaisuus eri asiakkaille. Palvelutuottajien ja asiakkaiden tulisi yhdessä arvioida palveluiden keskinäisriippuvuuksien synnyttämiä riskejä, huomioiden kasautumisriskit, sekä riskit myös poikkeusoloissa normaaliolojen lisäksi. Palveluiden merkittävyys kullekin asiakkaalle, sekä asiakkaan kanssa arvioitujen riskien hallinta sekä normaali- että poikkeusoloissa tulisi huomioida asiakkaiden ja tuottajien välisissä sopimuksissa.

Digitaalisen turvallisuuden kustannus-vaikuttavuudessa on huomioitava myös digitaalisen turvallisuuden riskien dynaaminen luonne, minkä johdosta riskien todennäköisyyksien ja vaikutusten ennustaminen on usein haasteellista. Riskien dynaamisesta luonteesta johtuen myös historiallisen riskidatan arvo on usein vähäinen. Tämän johdosta riskien arvioinnissa on usein hyödynnettävä esimerkiksi useita vaihtoehtoisia skenaarioita.

Yhteiskunnallisten vaikutusten arvioimista varten suunnitelmana on muodostaa virastoissa laadittavien digitaalisen turvallisuuden kustannus-vaikuttavuusarviointien perusteella strateginen kokonaisarvio osana Valtiokonttorin Tietokiri-kokonaisuutta.

LÄHDELUETTELO

Adar E., Blobner C., Hutter R., Pettersen K., (2012), An extended Cost-Benefit Analysis for evaluating Decisions on Security Measures of Public Decision Makers, CRITIS 2012, 7th Int. Conf. on Critical Inf. Infrastruct, Security, September 17-19, Lillehammer.

Euroopan Unioni. (2019). Challenges to effective EU cybersecurity policy Briefing Paper. March 2019.

Fischer, L., Uslar, M., Morrill, D., Döring, M & Haesen, E. (2018). Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector. Ecofys 2018 by order of: European Commission.

Flores, W, R, Sommestad, T, Holm, H and Ekstedt, M. (2011*). Assessing Future Value of Investments in Security-Related IT Governance Control Objectives – Surveying IT Professionals*. The Electronic Journal Information Systems Evaluation Volume 14 Issue 2 2011, (pp216-227).

Franklin, C. & Chee, B. (2019). Securing the Cloud: Security Strategies for the Ubiquitous Data Center. 10.1201/9780367259433.

Freund, J. & Jones, J. (2015). Measuring and managing information risk: A FAIR approach. Oxford, UK: Butterworth-Heinemann.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. Npj Digital Medicine (2019) 2:98.

Gilligan, J. (2013). The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment," October 2013. Armed Forces Communications and Electronics Association (AFCEA).

Goebel, A. ja Metsäranta, H. (2007) Tienpidon vaikutuskartta. Tiehallinto, Asiantuntijapalvelut. Tiehallinnon selvityksiä 1/2007.

Gordon, L. & Loeb, M. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), pp. 438-457.

Green, S. L. (2002). Rational Choice Theory: An Overview. Baylor University Faculty Development Seminar on Rational Choice Theory

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. Managerial Auditing Journal, 34(7), 808-834.

Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi. HE 284/2018.

Hulthén, R. (2009). Communicating the Economic Value of Security Investments; Value at Security Risk.

ISACA 2012. Introduction to Return on Security Investment. Helping CERTs assessing the cost of (lack of) security. [Deliverable – December 2012]

Jajodia, S. Cybenko, G., Liu, P., Wang, C. & Wellman, M. (2019). Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Control- and Game-Theoretic Approaches to Cyber Security. Springer Nature.

Juuso, A., & Svento, R. (2018). Tietoturvainvestoinnit ja uhkatiedon jakaminen taloustieteellisestä näkökulmasta. Kansantaloudellinen aikakauskirja – 114. vsk. – 2/2018

Kaplan, S. and Garrick, B.J. (1981) On the quantitative definition of risk. Risk Analysis 1, 11-27.

Krausz, M., & Walker, J. (2013). The True Cost of Information Security Breaches and Cyber Crime. ITGP.

Kuusisto, T. (2014). Kybertaistelu 2020. Maanpuolustuskorkeakoulu. Julkaisusarja 2, No. 1/2014

Lamothe, D., ja Görlach, B. (2005). Evaluation of the impact of floods and associated protection policies. Final Report. European commission.

Liikenne- ja viestintävirasto Traficom. Kyberturvallisuuskeskus. (2020). Kyberturvallisuus ja yrityksen hallituksen vastuu. Traficomin julkaisuja 2/2020.

Moore, T., Dynes, S. & Chang, F. (2016). Identifying how firms manage cybersecurity investment. Workshop on the Economics of Information Security (WEIS), Berkeley, CA, June 13-14, 2016.

Mänttäri-van der Kuip, M., Tammelin, M., & Anttila, T. (2018). Organisaatioiden isomorfismi : julkiset organisaatiot ja yhdenmukaisuuden paine. Yhteiskuntapolitiikka, 83 (3), 233-244.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://doi.org/10.6028/NIST.CSWP.04162018. (Linkitetty 6.5.2020)

OECD. (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris.

OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris.

Opetusministeriö. (2009). Vaikuttavuusindikaattorit kulttuuripolitiikan tietopohjan vahvistajina. Opetusministeriön julkaisuja 2009:57.

Panou, Angeliki & Ntantogian, Christoforos & Xenakis, Christos. (2017). RiSKi: A Framework for Modeling Cyber Threats to Estimate Risk for Data Breach Insurance. 10.1145/3139367.3139426.

Puhakka, A. (2017). INVESTOIMALLA HYVINVOINTIA. Hyvinvointitaloutta rakentamassa. Suomen sosiaali ja terveys ry. SOSTEn julkaisuja 3/2017.

Radanliev, P., Roure, C., Cannady, S., Montalvo, R.M., Nicolescu, R., Huth, M., (2018). Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. Living in the Internet of Things: Cybersecurity of the IoT - 2018. Institution of Engineering and Technology, London.

Ristimäki, P. (2015). VAHTI Ohjejaosto - vuosi toimintaa. 10.12.2015 VAHTI päivä. Valtiovarainministeriö.

Rodewald, G. (2005). Aligning information security investments with a firm's risk tolerance. In Proceedings of the 2nd annual conference on Information security curriculum development (InfoSecCD '05). Association for Computing Machinery, New York, NY, USA, 139–141.

Rokkas, Neokosmidis ja Xydias. (2018). Report on Cost-Benefit Analysis of Cyber-security Solutions, Products and Models. Work Package 4: Cyber-security, Cyber-crime Market and Regulatory Analysis. Systemic Analyser in Network Threats – with the support of the European Commission and the Horizon 2020 Program, under Grant Agreement No 740829.

Rousku, K. ja Mellin, L. (2018). Henkilöstön ja johdon tietoturvabarometri 2017. Valtiovarainministeriön julkaisu 19/2018.

Schneier, B. (2013). Economics of Information Security and Privacy III. Springer-Verlag New York.

Shim, W. (2011). Vulnerability and Information Security Investment Under Interdependent Risks: A Theoretical Approach.

Su, X. (2006). An Overview of Economic Approaches to Information Security Management. (CTIT Technical Report Series; No. 06-30). Enschede: Centrum voor Telematica en Informatie Technologie.

Valtiontalouden tarkastusvirasto. (2017). *Kybersuojauksen järjestäminen. Tuloksellisuuskertomus*. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Dnro 185/54/2016.

Valtiovarainministeriö. (2020a). Julkisen hallinnon digitaalinen turvallisuus. Valtiovarainministeriön julkaisuja 2020:23.

Valtiovarainministeriö. (2020b). Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka). Valtiovarainministeriön julkaisuja 2020:33.

Valtiovarainministeriö. (2019). Riskienhallinnan järjestämisen nykytila valtion virastoissa, rahastoissa ja liikelaitoksissa. Valtiovarainministeriön julkaisuja 2019:64. Toim. Taavitsainen, P.

Valtiovarainministeriö. (2017). Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Toim. Rousku, K.

Valtiovarainministeriö. (2014). Tietoturvallisuuden arviointiohje. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. 2/2014. Juvenes Print - Suomen Yliopistopaino Oy

Valtiovarainministeriö. (2012). Kohti strategisempaa, kevyempää, poikkihallinnollisempaa ja yhtenäisempää tulosohjausta. Valtiovarainministeriön julkaisuja 21/2012

Vuorinen, S. (2019). Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019:14.

Su, X. (2006). An Overview of Economic Approaches to Information Security Management", Technical Report TR-CTIT-06-30, University of Twente, June 2006

Työ- ja elinkeinoministeriö (2019), *Kasvua digitaalisesta turvallisuudesta*. Tiekartta 2019–2030. Valmistelutyön loppuraportti. Helsinki 2019.

Zhang, Y. (2016). Research on Cost-benefit Evaluation Model for Performance-based fire Safety Design of Buildings. Procedia Engineering, 135(C), pp. 537-543.

Liite 1. Haastatellut henkilöt

Autero Ville, Alitalo Sirpa ja Jokela Jaakko. Työ- ja elinkeinoministeriö.

Liikamaa Marko ja Veli-Matti Lammentausta. Istekki Oy.

Merta Jaana, Nummikoski Jukka ja Vertanen Antti. Maa- ja metsätalousministeriö.

Mäntylä Harri ja Saarimaa Elina. Puolustusministeriö.

Naumanen Hannu ja Simula Tommi. Valtion tieto- ja viestintätekniikkakeskus.

Puhakainen Petri. Valtioneuvoston kanslia.

Rinne Tapani. Kaarinan kaupunki.

Tallinen Juha. Pääesikunta.

Uusikartano Ari. Ulkoministeriö.

Ylikangas Marke. Verohallinto.

Liite 2. Haastatteluiden kysymykset

- Millainen digitaalisen turvallisuuden riskiarviointimalli on käytössä organisaatiossanne? Mitkä ovat nykyisen mallin hyödyt ja puutteet?
    - Mitä mahdollisia laadullisia arviointeja riskiarviointimalliin sisältyy? Miten arvioisitte liitteenä olevan laadullisen vaikuttavuuden arvioinnin hyödyntävän organisaatiota?
- Miten arvioitte riskien mahdollisen realisoitumisen todennäköisyyttä, ja sen aiheuttamia menetyksiä?
- Arvioidaanko riskien toteutumisen todennäköisyyttä esimerkiksi neliportaisella asteikolla tai prosentuaalisesti, ja niiden potentiaalisesti aiheuttamia menetyksiä euromääräisesti?
- Miten arvioitte riskejä pienentäviä toimia?
    - Miten riskejä pienentävien toimien kustannuksia arvioidaan?
    - Miten riskejä pienentävien toimien vaikuttavuutta riskin toteutumisesta aiheutuvan menetyksen odotusarvoon arvioidaan?
- Miten riskiltä suojattavan kohteen, eli esimerkiksi prosessin, palvelun tai tietovarannon arvoa yhteiskunnalle arvioidaan? (Esimerkiksi suoritteiden arvon kautta).
    - Arvioitteko riskiä pienentävien toimien kustannuksia suhteessa turvattavan kohteen arvoon? Entä mahdollisten menetysten suuruutta suhteessa turvattavan kohteen arvoon? Eli riskiä pienentävien toimien välttämättömyyttä?

- Gordon-Loeb –mallin mukaan optimaalinen resursointi digitaaliseen turvallisuuteen saavutetaan investoimalla n. 37% menetyksen odotusarvosta. Mitä ajattelet tämän kaavan soveltamisesta arvioitaessa panostuksia digitaaliseen turvallisuuteen julkisessa hallinnossa.

- Kerätäänkö riskien toteutumisesta aiheutuneista menetyksistä dataa?
  - Miten keräätte dataa riskien toteutumisesta aiheutuneista menetyksistä?
  - Kerätäänkö dataa aktiivisesti, ja onko siihen olemassa selkeä ohjeistus?
- Mitä ohjelmistoa käytätte riskien ja riskejä pienentävien toimien tunnistamiseen ja ylläpitoon?
- Muita näkökulmia digitaalisen turvallisuuden kustannusten ja hyötyjen arvioimiseen?

Liite 3. Käsitteistö

Digitaalinen turvallisuus
Digitaalisen turvallisuuden viitekehys koostuu viidestä osa-alueesta, jotka ovat riskienhallinta, jatkuvuudenhallinta, tietosuoja, tietoturvallisuus ja kyberturvallisuuden. Termi on vakiintumaton, ja sitä käytetään usein kyberturvallisuuden synonyymina. Esimerkiksi OECD käyttää englanninkielistä termiä *digital security*, koska se on yhteneväinen esimerkiksi digitalisaation ja digitaalisen talouden kanssa. [1]

Riskiarviointi
Riskin merkityksen arvioinnin kokonaisprosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin. [2]

Riski
Kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutusten yhdistelmä. Riski lasketaan tapahtuman todennäköisyyden ja vaikutuksen tulona. Riskit voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön tai yhteisöllisiin arvoihin. [3]

Menetys
Tappio, vahinko. Esimerkiksi tehokkuuden, työajan, maineen, hyvinvoinnin tai varojen vähentyminen riskin toteutumisen seurauksena. [4]

Kustannus
Suoritteiden aikaansaamiseksi tehty taloudellinen uhraus, joka aiheutuu tuotannontekijöiden käytöstä tai kulutuksesta. [5]

Riskejä pienentävä toimi
Riskiä muuttava toimenpide. Hallintakeinoja ovat kaikki riskiä muuttavat prosessit, toimintaperiaatteet, laitteet, käytännöt tai muut toimenpiteet. Hallintakeinoilla ei aina välttämättä ole haluttua tai oletettua muutosvaikutusta. [6]

Ulkoisvaikutus
Yrityksen toiminnan vaikutukset yrityksen ulkopuolella. Ulkoisvaikutukset voivat olla positiivisia (esim. tutkimus- ja kehitysyhteistyö) tai negatiivisia (esim. ympäristön saastuttaminen). Positiivinen ulkoisvaikutus, ulkoishyöty; negatiivinen ulkoisvaikutus, ulkoishaitta. [7]

Suojattava kohde
Yhteiskunnan tai organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata riskien varalta. Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema. [8]

Lähteet termien määritelmille:

[1] Pilkahduksia tulevaisuuteen, Tietopolitiikka, tekoäly ja robotisaatio hyvinvoinnin ja taloudellisen menestyksen mahdollistajana Suomessa, Valtiovarainministeriön julkaisuja – 2019:22

[2] Valtiokonttori. Riskienhallinta ja turvallisuus –forum 17.10.2012

[3] Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)

[4] Iate. European Union terminology. https://iate.europa.eu/search/standard/result/1582806100716/1

[5] Sanastokeskus TSK TEPA-termipankki. Kiinteistösanasto (TSK 4, 1984)

[6] Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI). 22/2017 Ohje riskienhallintaan – LIITTEET 1 – 6

[7] Iate. European Union terminology. https://iate.europa.eu/entry/result/750521/all.

[8] Sanastokeskus TSK ry. KYBERTURVALLISUUDEN SANASTO. 2018.

Liite 4. Laadulliset indikaattorit

Määrällisten mittareiden lisäksi tarvitaan laadullisia mittareita, esimerkiksi luottamus, tai henkilön subjektiivinen arvio, täydentämään digitaalisen turvallisuuden vaikutusten arviointia. Laadullinen arviointi voi sisältää esimerkiksi oheisen kyselyn. Kyselyssä esitetään digitaalisen turvallisuuden sisäisiin ja ulkoisiin tekijöihin liittyviä väittämiä. Väittämiä arvioidaan neliportaisella asteikolla, jossa

- 1 = olen täysin eri mieltä väitteen kanssa
- 2 = olen osittain eri mieltä väitteen kanssa
- 3 = olen melko samaa mieltä väitteen kanssa
- 4 = olen täysin samaa mieltä väitteen kanssa

Sisäiset

1) Organisaatiossani käytetään riittävästi resursseja digitaalisen turvallisuuden kehittämiseen ja ylläpitoon.
2) Tiedän, kuinka paljon organisaationi käyttää resursseja digitaalisen turvallisuuden kehittämiseen.
3) Organisaationi digitaalinen turvallisuus paranisi, jos sen kehittämiseen käytettäisiin nykyistä enemmän resursseja (esim. turvallisuuspoikkeamat vähentyisivät ja riskit vähenisivät).
4) Organisaatiossani digitaaliseen turvallisuuteen käytetyt resurssit on kohdennettu oikeisiin asioihin parhaalla mahdollisella tavalla.
5) Organisaatiossani seurataan digitaalisen turvallisuuden poikkeamia (esim. tietoturvahäiriöt) ja arvioidaan niiden aiheuttamia vahinkoja [taloudelliset vahingot, mainehaitat, palveluiden saatavuus].
6) Koen, että työni kannalta tärkeät tiedot ovat turvassa palveluntarjoajan tietovarastoissa.

Seuraavassa on lueteltu toimenpiteitä, joiden avulla organisaatiot pyrkivät parantamaan digitaalista turvallisuuttaan. Kuinka merkittävästi arvioit näiden toimenpiteiden parantavan organisaatiosi digitaalista turvallisuutta? Arvioi parannusta neliportaisella asteikolla, jossa

- 1 = hyvin vähäinen vaikutus, tai ei lainkaan vaikutusta
- 2 = melko vähäinen vaikutus
- 3 = jonkin verran vaikutusta
- 4 = erittäin merkittävä vaikutus

1) Johdon tietoisuuden lisääminen
2) Henkilöstön perehdytysohjelman kehittäminen tai laajentaminen
3) Lisäinvestoinnit laitteisiin (mm. tekninen valvonta, tietojärjestelmien seuranta ja valvonta, viestintä)
4) Lisäinvestoinnit ohjelmistoihin (mm. tietoturvaohjelmistot, koulutusalustat)
5) Palvelutoimittajien ohjauksen ja valvonnan tehostaminen
6) Vaatimustenmukaisuuden kehittäminen (esimerkiksi standardointi ja sertifiointi)

Ulkoisille sidosryhmille kohdistettavat kysymykset

Jos arvioidaan palveluntarjoajia kollektiivisesti, saattavat vastaajat painottaa arvioissaan eri palveluntarjoajia. Jos arvioidaan nimettyjä palveluntarjoajia (esim. Valtori, Tieto, Fujitsu, jne.), voi ongelmaksi muodostua palveluntarjoajien liian suuri lukumäärä. Vastaajaa voisi pyytää keskittymään yhteen tai kahteen merkittävimpään digitaalisia palveluja tarjoavaan organisaatioon.]

1) Koen, että omat [henkilö]tietoni ovat turvassa palveluntarjoajan tietovarastoissa.
2) Luotan palveluntarjoajan digitaalisen turvallisuuden tasoon.
3) Uskon, että palveluntarjoaja pystyy huolehtimaan digitalisoituvien palvelujen riskeistä riittävän hyvin.
4) Uskon, että palveluntarjoaja ottaa digitaaliseen turvallisuuteen liittyvät kysymykset vakavasti.
5) Palveluntarjoaja tuottaa minulle riittävästi digitaalista turvallisuutta koskevaa tietoa.

Liite 5. Kuvitteellinen esimerkki kustannus-vaikuttavuuden arvioinnista

Tässä liitteessä esitetään esimerkkilaskelma ehdotuksen mukaisesta kustannus-vaikuttavuusanalyysistä. Esimerkkinä käytetään tiedonhallintalain tarkoittamassa merkityksessä tiedonhallintayksikön kuvitteellisesti tunnistamia merkittävimpiä turvattavia kohteita. Niistä on valittu tarkemman tarkastelun kohteeksi tiedonhallintayksikön merkittävin palvelu. Käsitellään siihen kohdistuvia kuvitteellisia riskejä, ja niiden pienentämiseksi tehtäviä suojaustoimia. Riskien arvioinnissa tulee huomioida kriittiset riippuvuudet, joiden johdosta riskien toteutumisen vaikutukset aiheuttavat seurauksia myös muille kuin tiedonhallintayksikölle itselleen.

Havainnollistava esimerkki, jossa käytetyt tiedot ovat kuvitteellisia: Tiedonhallintayksikön kuvitteellisesti tunnistamat tärkeimmät turvattavat kohteet, sekä arviot niiden arvosta:

Turvattava toiminta	**Kriittisyys**	**Turvattavan kohteen arvo**
Tiedonhallintayksikön merkittävin tietovaranto sidosryhmävaikutuksineen	Erittäin kriittinen (5)	Mittaamattoman arvokas kansallisomaisuus
Tiedonhallintayksikön keskeisin palvelu sidosryhmävaikutuksineen, hankinta ja ylläpito 4 vuoden ajan	5	25 000 000 €
Tiedonhallintayksikön ulkoinen verkkosivusto, hankinta ja ylläpito 4 vuoden ajan	3	500 000 €

Tiedonhallintayksikön kansalaisille tarjoama sähköinen ajanvarausjärjestelmä, hankinta ja ylläpito 4 vuoden ajan	3	250 000 €

Taulukko 8. Esimerkki turvattavien kohteiden arvioinnista

Merkittäviä tiedonhallintayksikön keskeisimpään palveluun kohdistuvia kuvitteellisia digitaalisen turvallisuuden riskejä:

Palveluun kohdistuva riski ja vaikutukset	**Riskiskenaarion todennäköisyys**
Toiminnan katkos	Poikkeamatilanteista johtuvat katkokset ovat harvinaisia. Nykyisin suojaustoimin niitä kohdistuu palveluun noin 2 – 4 kertaa vuosittain. Katkoksen toteutuessa kustannuksia aiheutuu katkoksen syyn selvittelystä sekä mahdollisista korjaustoimenpiteistä. Jos kyseessä on laaja toiminnallinen häiriö, joita on ehkä kaksi kertaa vuodessa, niin selvittelyyn voi kulua usean henkilötyövuoden verran, eli noin 180 000 – 240 000 € kustannukset. Lisäksi tulisivat mahdolliset haitat sidosryhmien toimintaan, noin 300 000€. Näin ollen riskin aiheuttamien menetysten vuosittainen odotusarvo on 960 000 € – 1 080 000 €.
Rikoksista aiheutuvat tappiot	Rikoksista aiheutuvat tappiot ovat melko harvinaisia. Nykyisin suojaustoimin niitä kohdistuu palveluun noin kerran vuodessa. Rikoksen toteutuessa kustannuksia aiheutuu tapahtumisen selvittelystä poliisin kanssa sekä mahdollisista korjaustoimenpiteistä. Selvittelyyn voi kulua usean henkilötyövuoden ver-

	ran, eli noin 180 000 – 240 000 € kustannukset. Rikokset aiheuttavat harvoin haittaa sidosryhmien toimintaan. Näin ollen riskin aiheuttamien menetysten vuosittainen odotusarvo on 180 000 € – 240 000 €.

Taulukko 9. Esimerkki riskien arvioinnista

Esimerkin mukaisessa arvioinnissa tulisi huomioida toiminnan katkoksista aiheutuvat suorat taloudelliset menetykset, tiedonhallintayksikön sisäiset työajan menetykset ja korjauskustannukset. Näiden lisäksi tulisi arvioida myös asiakkaille ja muille julkisen hallinnon toimijoille kohdistuvia menetyksiä.

Riskin pienentämiseen vaadittavat resurssit:

Tavoitteena on tiedonhallintayksikön keskeisen palvelun toiminnan sekä käytettyjen tietojen luottamuksellisuuden, saatavuuden ja eheyden turvaaminen. Esimerkiksi palvelunestohyökkäyksistä johtuvat toiminnan katkokset vaikuttavat ennen kaikkea palvelun ja sen sisältämien tietojen saatavuuteen. Riskiarvioinnin yhteydessä voidaan esimerkiksi todeta tarve parantaa järjestelmän suojausta toiminnan katkosten ehkäisemiseksi. Katkosten todennäköisyyttä arvioidaan voitavan pienentää panostamalla valvonta- ja reagointijärjestelmään, sekä teknologioita että valvontahenkilöstön osaamista kehittämällä. NIST:n viitekehyksen mukaisesti tulisi lisätä resursseja kategorioihin *tietoisuus ja koulutus* (50 000 €) ja suojausteknologia (100 000 €) vuosittain yhteensä 150 000 € vuodessa, eli neljän vuoden aikana yhteensä 600 000€.

Tunnistus	Omaisuuden hallinta
	Liiketoimintaympäristö
	Hallinto
	Riskiarviointi
	Riskienhallintastrategia
Suojaus	Kulunvalvonta
	Tietoisuus & koulutus **+**50 000 €/v 4 vuoden ajan
	Tietoturvallisuus
	Tietosuojaprosessit ja – menettelyt
	Ylläpito

	Suojausteknologia +100 000 €/v 4 vuoden ajan
Havainnointi	Poikkeamat ja tapahtumat
	Turvallisuuden jatkuva seuranta
	Havaitsemisprosessit
Reagointi	Reagointisuunnittelu
	Viestintä
	Analysointi
	Lievennys
	Parannukset
Palautuminen	Toipumissuunnitelma
	Parannukset
	Viestintä

Taulukko 10.Esimerkki NIST-viitekehyksen käytöstä

Nykyisin järjestelmään kohdistuvien katkosten arvioidaan aiheuttavat vuosittain 960 000 € – 1 080 000 € menetykset. Investointien arvioidaan puolittavan vuosittaiset menetykset, eli menetykset pienenisivät vuosittain 480 000€ - 540 000€. Digitaalisen turvallisuuden investointien vuosittaiset kustannukset olisivat 150 000 €, ja arvioitu digitaalisen turvallisuuden vaikuttavuus siten 330 000€ - 390 000€ vuodessa.

Vaikuttavuuden seuranta ja raportointi:

Riskin pienentämiseksi käytettyjen resurssien tehokkuutta tulee seurata toimenpiteiden toteuttamisen jälkeen, jotta vaikuttavuusarviointia voitaisiin jatkossa kehittää. Seurattavana tavoitteena tulisi siis tämän esimerkin osalta olla se, että toteutuvatko arviot realisoituvien toiminnallisten katkosten määrän vähenemisestä.