DIGI- JA VÄESTÖTIETO-VIRASTO

Kustannus-vaikuttavuus-malli digitaalisen turvallisuuden riskienhallintaan [luonnos]

VAHTI-hyvät käytännöt tukimateriaali

29.5.2023

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

DTYT / Reivo Juho (DVV)

29.5.2023

Sisällysluettelo

DTYT / Reivo Juho (DVV)

29.5.2023

1 Tiivistelmä

Digitaaliseen turvallisuuteen kohdistuvat hallintatoimenpiteet pyrkivät lähtökohtaisesti vähentämään organisaatioon kohdistuvien uhkien vaikutuksia tai niiden todennäköisyyttä, ja täten ehkäistä menetyksiä, joita riskien toteutumisesta saattaisi seurata. Jotta uhkia ja niihin liittyviä riskejä ja menetyksiä voidaan hallita ja vähentää, tulee niiden ympärille luoda järjestelmällinen malli, joka mahdollistaa tämän. Osana tähän soveltuvia hallintamalleja ja johtamisen toimintatapoja kuuluu riskienhallinta, jonka prosesseissa tuotetaan tietoa päätöksenteon tueksi.

Digitaalisen turvallisuuden parantaminen ei ole ilmaista, vaan vaatii toteutuakseen panostuksia ja kustannuksia, jotka on kohdistettava tehokkaasti ja perustellusti. Riskien ja niiden käsittelyn vaihtoehtojen analysoinnin ja arvioinnin eri vaiheissa riskejä tulee kyetä arvottamaan ja suhteuttamaan yhdenmukaisesti - niin digitaalisen turvallisuuden sisällä kuin muihin riskeihin nähden, osana kokonaisriskienhallintaa. Tässä dokumentissa tähän liittyvien arvostusten muodostamisen vaiheet eri tasoilla kokoavaa mallia kutsutaan digitaalisen turvallisuuden kustannus-vaikuttavuusmalliksi.

Käytännön tasolla digitaalisen turvallisuuden riskienhallintatoimille voidaan laskea arvo, tarkastelemalla arvioitua menetystä sekä huomioimalla myös jäännösriskin. Tätä investointien kustannuksiin perustuvaa laskelmaa on kuitenkin rikastettava, mikäli pyritään tunnistamaan suojattavia arvoja[1] sekä eri hallintatoimien merkitystä ja kohdistamaan toimenpiteitä näihin oikealla ja tehokkaalla tavalla. Tämä rikastaminen tapahtuu muodostamalla arvomalli, tuomalla tarkasteluun sopivat luokittelutavat, jotka ovat yhteydessä digitaalisen turvallisuuden johtamiseen ja koordinaatioon. Tässä dokumentissa luotu kustannusluokittelumalli hyödyntää laajasti käytössä olevia ISO27000- ja NIST CSF-malleja. Digitaalisen turvallisuuden arvioinnin kannalta on oleellista, että turvallisuuteen liittyvät kustannukset voidaan tunnistaa ja luokitella riittävän tarkalla tasolla. Samalla tiedonkeräyksen toteutuksen pitää kuitenkin olla suhteessa asiantuntijoiden resursseihin, sillä automaatio ainakaan toistaiseksi kykene riittävällä tarkkuudella omatoimisesti tunnistamaan digiturvan kontekseja.

Kolmannella tasolla riskitietoa vielä käsitellään eteenpäin vaikuttavuuden esiintuomiseksi, jotta arvotuksen merkityksiä voidaan tarkastella strategisessa kontekstissa tarvitulla ja hyödynnettävissä olevalla tavalla. Digiturvallisuuden arvomallin riskit, menetykset ja kustannukset voidaan tuoda osaksi organisaation laajempaa riskienhallinnan kokonaisuutta, toiminnan ohjausta ja strategista johtamista. Ilman tätä vaihetta uhkana on, että arvomallin hyödyntäminen toimintojen kehittämisessä ja riskien hallinnassa jää asiantuntijatasolle eikä integroitu organisaation johtamismalliin.

[1] Suojattavalla arvolla tarkoitetaan tässä dokumentissa sekä konkreettisia järjestelmiä, joilla nähdään rahallista arvoa, arvoa, joka sisältyy tietoon ja sen käyttöön, että laajempia yhteiskunnallisia tai perusarvoja. Nykyaikaisessa ja kompleksisessa maailmassa on huomioitava, että riskit voivat kohdistua useille eri tasoille. Tämä laajentaa niin sanotun suojattavan kohteen määritelmää, sillä esimerkiksi yksittäinen tietovarasto voi olla merkityksetön sen rinnalla, miten varmistetaan palvelukokonaisuuden jatkuvuus, tai miten se ja muut digitaalisen toimintaympäristön sosio-teknisen järjestelmän osaset vaikuttavat mm. ”luottamuksen” muodostumiseen. Strategiset tavoitteet voidaan usein muotoilla laajemmiksi suojattaviksi arvoiksi.

2 Johdanto

Digitaalisella turvallisuudella (lyhyemmin digiturvallisuudella, digiturvalla) pyritään organisaatioissa varmistamaan, että niiden digitaalinen toimintaympäristö on luotettava ja että toiminta siellä on turvallista ja hallittua normaalissa arjessa kaikille käyttäjille. Jotta tämä olisi toteutettavissa, tulee organisaatioiden pystyä tunnistamaan digitaaliseen toimintaympäristöön kohdistuvia uhkia ja varautumaan näistä muodostuviin riskeihin. Organisaatioiden tulisi myös ymmärtää digitaalisen turvallisuuden uhkiin liittyvät potentiaaliset menetykset ja systemaattisesti pyrkiä minimoimaan niitä.

Digiturvallisuuden arvo muodostuu uhkiin liittyvien menetysten arvon tunnistamisesta sekä riskienhallinnallisista toimenpiteistä, joilla menetyksiin pyritään vaikuttamaan.

Keskeinen keino vaikuttaa organisaation digitaaliseen turvallisuuteen on investoida turvallisuuteen liittyviin menetelmiin, palveluihin ja järjestelmiin. Digitaaliseen turvallisuuteen kohdentuvat investoinnit pyrkivät lähtökohtaisesti vähentämään organisaatioihin kohdistuvia digitaalisia uhkia tai niiden todennäköisyyttä. Jotta investointien toimivuutta ja tehokkuutta voidaan seurata ja mitata tulee näihin liittyviä kuluja ja kustannuksia ymmärtää.

Tämän dokumentin tarkoituksena on määritellä lähestymistapa digitaalisen turvallisuuden kustannusten luokitteluun, uhkakuvien myötä muodostuvien mahdollisten menetysten luokitteluun sekä malli organisaatiokohtaiseen digitaalisen turvallisuuden riskienhallintaan edellä mainittuihin liittyvää tietoa hyödyntämällä. Dokumentin tarkoituksena on myös kuvata, miten lähestymistapa tulee integroida osaksi organisaation kokonaisvaltaista riskienhallintaa, strategista johtamista ja hallinnollista vaikuttavuutta. Edellä kuvattu kokonaisuus muodostaa digiturvallisuuden kustannus-vaikuttavuusmallin.

Digiturvallisuuden kustannus-vaikuttavuusmalli on konseptuaalinen malli sille, miten julkisissa organisaatioissa voidaan käsitellä digiturvan kustannuksia. Se on yhteensopiva ISO31000-sarjan mukaisen riskienhallinnan kanssa, sisältyen prosessissa riskien analysointiin ja arviointiin kvantitatiivisesti. Malli ei ota kantaa siihen, miten hallinta toteutetaan käytännön tasolla tai mitä hallintamallia digitaalisessa turvallisuudessa käytetään. Mallin käytäntöön saattamisessa suosittelemme digitaalisia työkaluja ja järjestelmiä, jotka tukevat mallin mukaista tekemistä, tietojen tehokasta käsittelyä sekä mahdollistavat prosessin automaatioasteen nostamisen. Digiturvallisuuteen liittyvän tiedonkeruun osalta voi olla tarpeen kehittää tähän liittyviä taloushallinnon järjestelmiä ja käytänteitä. Myös toimittajayhteistyön kautta voidaan sopia toimintamalleista, jotka edesauttavat kustannusluokittelua, erityisesti sen automatisoinnissa. Nämä on syytä huomioida, kun digiturvallisuuden kustannus-vaikuttavuusmallin käyttöönottoa suunnitellaan.

Kustannusten ja arvon laskeminen osana riskienhallinnan analysointia ja arviointia edellyttää tiettyä maturiteettia organisaatiolta, sen turvallisuuden hallinnalta sekä riskienhallinnalta. Tämä on tunnistettu haaste julkisessa hallinnossa. Valtiontalouden tarkastusviraston vuonna 2017 tekemän selvityksen mukaan, julkisen hallinnon organisaatiot budjetoivat digitaaliseen turvallisuuteen käytettävät varat toimintamenomomentille erittelemättömänä osana organisaation toiminnasta aiheutuvia

kustannuksia[2]. Haasteina ovat olleet sekä julkisen hallinnon toimintaan ja riskien logiikkaan liittyvät erityisyydet, että digitaalisen turvallisuuden alueella sovellettavissa olevan yhtenäisen mallin puuttuminen. Muun muassa näihin on pyritty vastaamaan osana Valtiovarainministeriön Haukka-hanketta[3], jota on toteutettu Digi- ja väestötietovirastossa JUDO-hankkeen[4] osana.

Digitaalisen turvallisuuden kustannus-vaikuttavuusmallin tarkoituksena on tarjota mekanismi, jonka avulla organisaatiot voivat systemaattisesti arvioida riskejä sekä kvantifioida niihin liittyviä hallintatoimenpiteitä (investointeja). Mallin tarkoituksena on myös integroida digiturvallisuuden riskienhallinta organisaation strategiseen päätöksentekoon sekä mahdollistaa digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyväksi saattaminen ja seuranta läpi koko organisaation.

Tämä asiakirja on tarkoitettu ensisijaisesti julkishallinnon eri organisaatioille, näissä toimiville riskienhallinnan ja digitaalisen turvallisuuden asiantuntijoille sekä näiden tehtävien parissa työskenteleville muille tahoille, kuten johdolle, hallinnon kehittäjille ja sisäiselle tarkastukselle. Malli on sovellettavissa myös julkishallinnon ulkopuolella keskeisiltä osin.

[2] *Valtiontalouden tarkastusvirasto. (2017). Kybersuojauksen järjestäminen. Tuloksellisuustarkastuskertomus. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Dnro 185/54/2016*.
(https://www.vtv.fi/app/uploads/2018/05/22102159/kybersuojauksen-jarjestaminen-16-2017.pdf)
[3] *Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka*)
(https://vm.fi/hanke?tunnus=VM174:00/2020)
[4] *Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma* (https://julkaisut.valtioneuvosto.fi/handle/10024/161218)

DTYT / Reivo Juho (DVV)

29.5.2023

3 Digitaalisen turvallisuuden kustannus-vaikuttavuusmallin osat

Digitaalisen turvallisuuden kustannus-vaikuttavuusmalli kokonaisuus pyrkii edesauttamaan ymmärrystä digitaaliseen turvallisuuteen tehtävistä panostuksista ja niiden tuottamista hyödyistä, eli niiden vaikutuksista digitaalisen turvallisuuden uhkien pienemiseen organisaatiossa. Tähän sisältyy neljä tasoa, jotka kattavat riskien analysoinnin ja arvioinnin taloudellisten merkitysten kautta eri tasoilla. Kokonaisuuden tavoitteena on mahdollistaa digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyväksi tekeminen sekä yhdenmukaisuus kokonaisriskienarviota varten.

Digitaaliseen turvallisuuteen kohdistuvat investoinnit pyrkivät lähtökohtaisesti vähentämään julkishallintoon kohdistuvia digitaalisia uhkia tai niiden todennäköisyyttä. Jotta uhkia ja niihin liittyviä riskejä ja menetyksiä voidaan kvantifioida ja seurata tulee niiden ympärille luoda säännönmukainen laskutapa, mikä mahdollistaa tämän. Tätä mallia kutsutaan tässä dokumentissa **riskien laskentamalliksi**. Siinä analysoidaan yksittäisten riskien osalta hallintatoimien merkitystä riskien taloudelliseen vaikutukseen.

Yksittäisiä riskejä laajemman hallittavuuden ja toiminnan koordinoinnin vuoksi on hyvä käyttää yhtenäistä mallia niihin liittyvien investointien kustannusten seuraamiseen, sen osalta, miten riskit kohdistuvat eri osa-alueille tai laajempiin kokonaisuuksiin. Tätä mallia kutsutaan tässä dokumentissa **digitaalisen turvallisuuden kustannusluokitteluksi**. Riskejä käsitellään tiettyjen vakiintuneiden hallintakeinoluokkien ja -kokonaisuuksien kautta, vaikka ne eivät välttämättä kata kaikkia riskin osatekijöitä. Tarkastelemalla, minne investoidut kustannukset kerääntyvät, voidaan analysoida riskien hallintatoimien vaikutuksia.

Lasku- ja kustannusmallien tarkoituksena on tarjota mallit, joiden avulla organisaatiot voivat systemaattisesti arvioida digiturvan konkreettisia suojattavia kohteita ja niihin liittyviä riskejä sekä kvantifioida toimenpiteitä (investointeja) joilla riskejä pyritään hallinnoimaan ja pienentämään. **Digiturvallisuuden menetysluokittelu** tarjoaa mallin tarkastella riskejä laajempien suojattavien arvojen kannalta. Näitä voi myös pitää tavoitteina, joihin hallintamallien toimilla pyritään.

Molemmille luokittelumalleille on tässä dokumentissa valittu luokittelukriteerit, jotka mahdollistavat yhdenmukaisen seurannan ja vertailtavuuden organisaatioiden sisällä ja poikkihallinnollisesti niiden välillä.

Kun kustannusluokittelu ja menetysluokittelu yhdistetään, organisaatio voi arvioida digitaalisen turvallisuuden kustannuksia ja menetysten arvoa osana riskienhallintaprosessejaan. Tätä kokonaisuutta on avattu tässä dokumentissa organisaatiokohtaisena **digiturvallisuuden arvomallina**. Koska digitaaliseen turvallisuuteen kohdistuvien investointien vaikutus riskien pienemiseen on ainakin osin riippuvainen organisaation nykytilasta, tulisi myös digitaalisen turvallisuuden nykymaturiteetti huomioida osana näitä analyysejä ja arviointeja.

Kun arvo- ja kustannusmallit yhdistetään organisaation strategiseen päätöksentekoon, voidaan tietoa hyödyntää tavalla, joka luo **digitaalisen turvallisuuden vaikuttavuus -mallin**. Tällä mallilla tulkitaan arvomalliin sisältyvien kustannusten ja luokitteluiden merkitystä organisaation strategisille tavoitteille ja strategisille riskeille.

Oheisessa kuvassa digiturvallisuuden arvo- ja kustannusmalli ja sen eri osa-alueet on kuvattu yleisellä tasolla.

Kuva 1: Kuvassa keltaiset laatikot kuvaavat digiturvallisuuden menetysten luokittelumallia (”menetys-luokittelu”) ja kustannusten seuranta- ja luokittelumallia (”kustannusmalli”) jotka pohjautuvat kansainväli-siin standardeihin. Menetysten luokittelua käytetään organisaation digiturvallisuuden riskien laskenta-mallissa. Mallien pohjalta organisaatio arvioi potentiaalisen menetyksen arvon ja siihen liittyvän riskin, ja yhdistämällä siihen digiturvallisuuden kustannukset se muodostaa näistä digiturvallisuuden arvomallin. Arvomalli tulee integroida organisaation strategiseen johtamiseen ja luoda siitä strategiaa ja hallinnointia tukeva vaikuttavuusmalli. Tämä kokonaisuus on digiturvallisuuden kustannus-vaikuttavuusmalli.

3.1 Digiturvallisuus kattavan turvallisuuden ja riskienhallinnan mallina

Digiturvallisuudella pyritään varmistamaan, että organisaatioiden digitaalinen toimin-taympäristö on luotettava, turvallinen ja saatavilla oleva. Jotta tämä olisi toteutetta-vissa organisaatioiden eri toimijoiden tulisi olla hyvin varautuneita digitaaliseen toi-mintaympäristöön kohdistuviin uhkiin. Organisaatioiden tulisi pystyä kestämään erilai-set häiriötilanteet sekä palautumaan niistä mahdollisimman tehokkaasti. Digiturvalli-suus jaetaan tässä dokumentissa viiteen pääluokkaan.[5]

Kuva 2: Malli perustuu VN:n periaatepäätökseen Dnro VN/1465/2020 ja se ilmentää ns. monen turvalli-suuden mallia, minimiä kattavalle turvallisuudelle digissä + omasta toiminnasta voi koitua tarve huomi-oida myös muita turvallisuuden toteutusalueita

[5] *Digi- ja väestötietovirasto: Mitä on digiturva?* (https://dvv.fi/mita-on-digiturva)

Nämä toteutusalueet ovat keskeisiä kattavan digiturvallisuuden toteuttamiselle:

- Hallinnollisesta näkökulmasta digiturvallisuuden **johtaminen ja riskienhallinta** tulisi olla luonnollinen osa koko organisaation johtamista, hallintoa ja kokonaisturvallisuutta.
- **Jatkuvuudenhallinnalla** tarkoitetaan toimenpiteitä, jotka liittyvät erilaisten häiriötilanteiden ennaltaehkäisemiseen. Häiriötilanteisiin tulisi kyetä varautumaan, hallitsemaan niiden aiheuttamia vaikutuksia, oppimaan niistä palautua sekä varmistaa organisaation toiminnan jatkuvuutta.
- **Kyberturvallisuus** pyritään varmistamaan sähköisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta. Toiminnon tarkoituksena on pyrkiä turvaamaan yhteiskunnan tai organisaation elintärkeät ja kriittiset toiminnot.
- **Tietosuojan** tarkoituksena on suojata yksilöiden yksityisyyden ja siihen liittyvien tietojen suojeleminen kaikissa tilanteissa.
- **Tietoturva** takaa organisaatioiden tietojen luottamuksellisuuden, eheyden ja saatavuuden. Tämän avulla pyritään, että vain oikeutetut tahot pääsevän käsiksi tarvittaviin tietoihin.

Digitaalista turvallisuutta ohjaavana mallina[6] tämä luokittelu on sekä tarpeellinen laajassa kuvassa, mutta samaan aikaan luokittelujärjestelmänä tai taloudellisena ohjaajana organisaatiotasolla haasteellinen Tässä käytetyt luokat eivät määritelmällisesti ole saman tasoisia ja näillä useita päällekkäisyyksiä. Vaikka juuri päällekkäisyyksiä voidaan pitää riskienhallinnallisena syvyytenä puolustuksessa uhkia vastaan, ne eivät sovellu toisensa pois sulkevaan rakenteeseen, jonka tulisi olla käytettävyydeltään kevyt ja helposti ihmiskäyttäjän ymmärrettävissä. Siksi tätä mallia tulee soveltaa laajemmassa tai strategisessa tarkastelussa soveltaen, vaikuttavuus-mallin tasolla.

[6] *Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta, VM/2020/47* (https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f806928f5)

4 Digiturvallisuuden riskien laskenta: menetysten arvioiminen osana riskienhallinnan prosessia

Digitaalisen turvallisuuden tärkeä osa on oikein toteutettu ja toimiva riskien arviointi.[7]

Riskien arviointiprosessia voidaan hyödyntää approksimaationa menetysten laskemiselle, ellei organisaatiolla ole parempaa tapaa arvioida digitalisen turvallisuuden menetyksiä. Riskejä voidaan myös mitata osana organisaation alaprosesseja, esim. hankintaprosessia (kts esimerkiksi ISO31000-standardi[8]).

Yksi monen tuntema tapa on luokitella riskit neljään pääluokkaan: strategiset riskit, operatiiviset riskit, taloudelliset riskit ja vahinkoriskit. Tämä soveltuu kuitenkin vain lähinnä ylätason kokonaisriskienhallintaan, eikä välttämättä kata julkishallinnon organisaation tarpeita. Riskien luokitteluun ei ole yhtä ainoaa kaikille sopivaa mallia tai tapaa, vaan organisaation riskien luokittelu tulee suunnitella ja toteuttaa organisaation toiminnan erityispiirteet huomioon ottaen.

Tukimateriaalit riskienhallinnalle sisältävät yksinkertaisen riskien arviointityökalun, jonka dimensiot (todennäköisyys ja vaikutus, joiden tulona riskin suuruus) ennustavat menetyksiä riskien toteutuessa. Työkalussa voidaan huomioida myös riskien käsittelyn toimenpiteet, sillä dimensioihin voidaan pyrkiä vaikuttamaan. Kuitenkin, vain riskien luonteen tarkempi analysointi ja ominaisuuksien tuntemus kertoo miten riski toimii ja vaikuttaa meihin. Tämä myös auttaa luomaan varsinaisia hallintatoimenpiteitä – toimintaa, jolla merkitystä ja kustannuksia.

Kuten aidossa riskienhallinnassa, käsittely tulee aloittaa riskin tunnistamisesta, eli mitä riskiin sisältyvä epävarmuus uhkaa. Tätä varten meidän on tunnettava toimintaympäristömme sekä organisaatiomme, eli ne kohteet, tavoitteet ja laajemmat arvot joita pyrimme suojaamaan.

4.1 Malli digitaalisen turvallisuuden aiheuttamien menetysten luokitteluun

On tärkeää, että digitaalisen turvallisuuden mahdolliset menetykset arvioidaan jollain tavalla organisaatioissa, jotta uhkien seurauksia ymmärrettäisiin paremmin. Menetykset voivat olla esimerkiksi kustannuksia, jotka muodostuvat aiempaan tilanteeseen palautumisesta, menetyksiä tulevaisuuden ennakoiduista tuloista, maksettavista ulkoisista korvauksista tai kadotetusta varallisuudesta. Menetykset voivat olla tilapäisiä tai pidempiaikaisia. Menetykset riippuvat paljolti digitaalisen turvallisuuden tapahtumatyypistä, kontekstista sekä organisaation tilanteesta.

Koska mahdolliset toteutuvat menetykset voivat olla hyvinkin erilaisia sisällöltään, niitä on luontevaa luokitella tarkemmalle tasolle. Tällaiseen luokitteluun voidaan käyttää

[7] *Tätä on kuvattu esimerkiksi VM:n VAHTI 22/2017 ohjeessa riskienhallinnalle, joka on tätä kirjoitettaessa joiltain osin vanhentunut. Siinä esitetyt asiat pääosin korvautuvat Valtiovarain controller-toiminnon julkaiseman riskikäsikirjan sisällöllä (odotetaan julkaistavan syksyllä 2023), johon nähden tämä on horisontaalisen poikkihallinnollisen erityisaiheen analyysin ja luokittelun sovellusohje. VAHTI-riskienhallintaohjeen päivitystä valmistellaan.*

[8] *Riskienhallintajärjestelmä ISO 31000* (https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-31000-riskienhallinta/)

esim. EU:n SAINT-hankkeessa käytettyä luokittelua[9]. SAINT (Systemic Analyzer In Network Threats) on EU:n rahoittama hanke, jossa tarkasteltiin tietoturvallisuuden kustannuksia. Erilaisia variaatioita mitata menetyksiä löytyy paljon (esim. kaupallisilta toimijoilta), mutta tärkeintä organisaatiolle on valita sellainen malli, joka parhaiten sopii juuri sille (ja tarvittaessa muokata sitä). SAINT-hankkeessa käytetty luokittelu on tähän tarkoitukseen hyvä lähtökohta, koska se huomioi eri menetyksiä laajalti.

Menetykset yhteensä									
			Strategisen tason menetykset						
			Organisatorisen tason menetykset						
			Toiminnallisen tason menetykset						
Immateriaali-oikeudelliset menetykset	Toiminnan keskeytykset	Datan ja ohjelmistojen menetykset	Kiristys-tapauksista ja petoksista aiheutuneet menetykset	Luottamuk-sellisen tiedon vuotamisesta aiheutuvat seuraukset	Korvaus-velvollisuudet kolmansille osapuolille	Vaikutukset maineeseen	Fyysiseen omaisuuteen kohdistuvat menetykset	Henkeen ja terveyteen kohdistuvat menetykset	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset

Kuva 3: Malli digitaalisen turvallisuuden aiheuttamien menetysten luokitteluun. Mallin menetysten luokittelu on alimmalla rivillä. Niitä voidaan tarkastella eri tasoisina, niin kuin kuvassa on esitetty.

Suojattavia asioita (arvoja, kohteita ja muita menetysluokkien kokonaisuuksia) kuvaavan mallin kautta voidaan pohtia menetysten laadullista ulottuvuutta strategisella, organisatorisella ja toiminnallisella tasolla. Alimmalla tasolla menetykset konkretisoituvat helpommin mitattaviin kokonaisuuksiin, jotka saattavat toteutua yksin tai yhdessä muiden menetysten kanssa.

4.2 Menetykset ennen ja jälkeen riskienhallintatoimenpiteiden

Riskienhallinnan perustyökalua käyttäen huomioidaan riskien menetysten arviointi, jossa riskin suuruus saadaan kertomalla todennäköisyys ja vaikutus. Jos käytetään rahallista arviota riskien arvioinnissa, tämä suuruus on parhaimmillaan käypä arvio mahdollisesta menetyksestä. Täten saadaan jokaisessa organisaatiossa itsearvioinnin pohjalta mahdollinen menetyksen suuruus.

Hallintatoimenpiteet aiheuttavat useimmiten kustannuksia (lähinnä ajan, rahan ja resurssien käyttö). Riskien hallintatoimenpiteitä ovat esimerkiksi riskin vähentäminen, ehkäiseminen ja pitäminen.

Kustannuksilla on parhaassa tapauksessa hyvinkin suora syy-yhteys suojattaviin riskeihin, joka jollain karkeustasolla parhaassa tapauksessa voidaan arvioida. Syy-seuraus-yhteys kustannusten ja menetysten välillä (siltä osin kuin sitä on) ei välttämättä ole lineaarista, joten toimenpiteitä on mietittävä tilanteesta riippuen. Syy-seuraus saattaa olla myös epälineaarinen, binäärinen tai joku muu tuntematon yhteys. Kustannukset vaikuttavat eri tavoin eri riskeihin. Jotkut kustannukset vaikuttavat useampaan riskiin, toisaalta saatetaan tarvita investointia useaan eri toimenpiteeseen, jotta saadaan yhtä riski pienemmäksi.

Parhaan näkemyksen asiasta tuovat arviointiin useimmiten organisaation omat asiantuntijat. Organisaatio itse osaa parhaiten tehdä arvioinnin omasta riskiprofiilistaan ennen ja jälkeen riskienhallinnallisten toimenpiteiden.

[9] *EU SAINT: D4.4 Report on Cost-Benefit Analysis of Cyber-security Solutions, Products and Models, sivu 48* (https://project-saint.eu/sites/default/files/d4.4.pdf)

Alla olevassa esimerkissä on hahmotettu riskien arvioiminen ja kuvaaminen ennen ja jälkeen kustannusten käytön riskienhallinnan perustyökalua käyttäen.

Esimerkki: Riskien arviointi ennen ja jälkeen riskienhallinnan toimenpiteiden

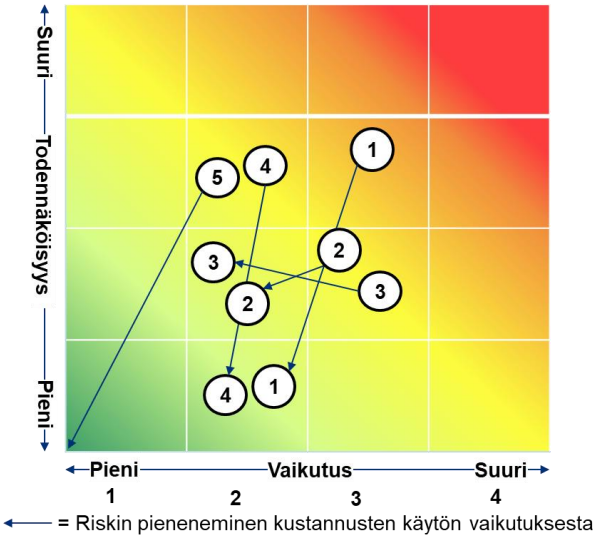
Alla on kuvattu esimerkki, jossa esimerkkiorganisaatio *Roskienhallintavirasto* on tehnyt riskianalyysin 5 keskeisimmästä digiturvallisuusriskistään. *Roskienhallintavirasto* on arvioinut riskin toteutumisen todennäköisyyttä asteikolla 1-4 (epätodennäköinen, mahdollinen, todennäköinen, lähes varma). Riskin vaikutus sen toteutuessa on arvioitu myös asteikolla 1-4, johon on sisältynyt euromääräinen kokoluokka (1 pienin ja 4 suurin).

Keskeisimmät 10 digiturvallisuusriskiä		Todennäköisyys ennen toimenpiteitä	Vaikutus ennen toimenpiteitä	Todennäköisyys toimenpiteiden jälkeen	Vaikutus toimenpiteiden jälkeen
Riski-nro	Nimike				
1	Riski sille, että…	3	3	1	2
2	Riski sille, että…	2	3	2	2
3	Riski sille, että…	2	3	2	2
4	Riski sille, että…	3	2	1	2
5	Riski sille, että…	3	2	Ei ole	Ei ole

Kuva 4: Roskienhallintaviraston riskiarviointi ennen ja jälkeen riskienhallinnallisten toimenpiteiden

Taulukon kahdessa ensimmäisessä sarakkeessa on riskin numero ja kuvaus. Kahdessa keskimmäisessä sarakkeessa on arvioitu riskin todennäköisyys ja vaikutus ennen riskienhallinnan toimenpiteitä (eli nykytila). Kaksi viimeistä saraketta taulukossa kuvaavat arviota jäännösriskiksi, mikäli tehtäisiin tiettyjä riskienhallinnallisia toimenpiteitä.

Sama asia on kuvattu seuraavassa kuvassa, jossa pallot kuvaavat riskejä ennen ja jälkeen riskienhallintatoimenpiteiden, ja nuolet kuvaavat kuinka paljon riskienhallinnan toimenpiteillä arvioidaan voitavan pienentää riskiä (joko todennäköisyyden, vaikutusten tai molempien kautta). Pallot taulukossa kuvaavat riskin riskilukua (kukin ruutu on kokonaisluku).



Kuva 5: Roskienhallintaviraston graafinen riskikuvaus taulukossa esitetyn arvion pohjalta

4.3 Riskienhallintatoimenpiteiden rahallinen vaikutus

Riskejä tarkasteltaessa on ensisijaista arvioida niitä tarvittavien toimenpiteiden kannalta, mutta samalla tulisi huomioida ja tuottaa myös euromääräinen arvio, joka voi täydentää riskin merkityksen ymmärtämistä, mutta etenkin tukea pidemmän aikavälin

ja kokonaisriskienhallinnan arviointitarpeiden kautta taloussuunnittelua. Rahallinen arvio riskien vaikutuksesta on sikäli hyödyllinen, että se on yhteismitallinen digitaaliseen turvallisuuteen liittyvien riskienhallinnan kustannusten kanssa.

Mikäli riskianalyysissä käytetään euromääräisiä arvioita vaikutukselle ja prosentuaalisia arvioita vuosittaiselle todennäköisyydelle, toimija pystyy karkealla tasolla laskemaan euromääräisen odotusarvon riskitoteutumalle vuositasolla kulloisellekin riskille sekä kaikkien riskien kokonaisvaikutukselle. Tällä tavalla saadaan laskettua odotettu digitaalisen turvallisuuden menetysriski mukaan tietylle ajanjaksolle. Erityisesti julkisessa hallinnossa on tosin huomioitava, että menetyksiä on arvioitava myös rahallisia menetyksiä laajemmin, mitä avataan enemmän sekä arvomallin että vaikuttavuuden osioissa tässä asiakirjassa. Menetysten realistisen arvioinnin tulisi toimia motivaattorina ja perusteluna hallintatoimille organisaatiossa.

Tämän jatkeena, toimija voi arvioida riskejä euromääräisesti riskienhallinnan toimenpiteiden jälkeen. Nämä usein vaativat toimenpiteitä, joilla on euromääräisiä kustannuksia ja ne sisältyvät joko aiemmin arvioituun normaalin toiminnan menokehykseen tai niitä varten on tehtävä muita toimia (esim. erilliset hankkeet ja projektit, mahdollisesti osana jatkuvuudenhallinnan varautumista) ja siten varmistettava erillinen rahoitus. Käyttäen odotusarvoa riskien toteutumisen arvolle ennen ja jälkeen (ns. jäännösriski) hallintatoimien kustannuksia, saadaan näiden erotuksena laskettua hallintatoimien vaikutus. Tämä laskennallinen arvioiden erotus antaa suuntaa antavasti turvallisuuteen vaikuttavien toimien euromääräisen arvon.

Laskentakaavana digiturvallisuuden taloudelliseen hyötyarviointiin voidaan myös hyödyntää laskentakaavaa:

$$T=Z-(I+J)$$

jossa digitaalisen turvallisuuden investointien taloudellinen hyöty (T) saadaan vähentämällä riskien euromääräisestä arvosta eli odotetuista menetyksistä (Z) digitaalisen turvallisuuden kustannukset (I) sekä jäännösriski (J).

Mikäli halutaan, kaavassa voidaan huomioida myös arvon diskonttaus jolloin kaavasta tulee:

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

Investoinnin vaikutuksen suuruus suhteessa riskiin pienentämiseen ei tule huomioiduksi tässä laskentakaavassa. Asiaa käsitellään laajemmin maturiteetin yhteydessä.

Esimerkki: Riskien toteutuman odotusarvon pienentäminen kohdistamalla kustannuksia riskiä pienentäviin toimenpiteisiin

Roskienhallintavirasto tunnisti edellisessä esimerkkitaulukossa digitaalisen turvallisuuden riskinsä ennen ja jälkeen riskienhallintatoimenpiteiden. Virasto on tunnistanut riskienhallintatoimenpiteiden kokonaiskustannukseksi 1,2 MEUR, ja tämä investointi kohdistetaan eri toimenpiteisiin. Alla olevassa taulukossa on eritelty tarkemmin kustannusten kohdistaminen ja miten ne vaikuttavat eri riskeihin.

Roskienhallintavirasto on antanut prosentuaalisia arvoja todennäköisyysasteikolle 1 – 4 seuraavasti: 1 = 25%, 2 = 50%, 3 = 75% ja 4 = 100%.

Roskienhallintavirasto on antanut euromääräisiä arvoja vaikutusasteikolle 1 – 4 seuraavasti: 1 = 1 MEUR, 2 = 5 MEUR, 3 = 10 MEUR ja 4 = 15 MEUR

Yllä olevien asteikkojen avulla virasto pystyy laskemaan riskiarvioihin perustuvan riskien teoreettisen toteutuman odotusarvon kertaamalla todennäköisyysluvun vaikutusluvulla (odotettu menetys = todennäköisyys * vaikutus). Nämä laskelmat näkyvät alla olevassa taulukossa odotettuina menetyksinä ennen ja jälkeen riskienhallintatoimenpiteiden.

Keskeisimmät 10 digiturvallisuus-riskiä		Toden-näköisyys ennen toimen-piteitä	Vaikutus ennen toimen-piteitä	Odotetun menetyksen laskelma	Odotettu menetys ennen	Riskien-hallinnan kustannuk-set	Todennäköi-syys kustan-nusten käy-tön jälkeen	Vaikutus kustannus-ten käytön jälkeen	Odotetun menetyksen laskelma	Odotettu menetys jälkeen	Odotettu riskien-hallinnan säästö
Riski-nro	**Nimike**										
1	Riski sille, että…	3	3	75%*10 MEUR	7,5 MEUR	0,2 MEUR	1	2	25%*5 MEUR	1,25 MEUR	6,05 MEUR
2	Riski sille, että…	2	3	50%*10 MEUR	5 MEUR	0,4 MEUR	2	2	50%*5 MEUR	2,5 MEUR	2,1 MEUR
3	Riski sille, että…	2	3	50%*10 MEUR	5 MEUR	0,1 MEUR	2	2	50%*5 MEUR	2,5 MEUR	2,4 MEUR
4	Riski sille, että…	3	2	50%*5 MEUR	2,5 MEUR	0,5 MEUR	1	1	25%*1 MEUR	0,25 MEUR	1,75 MEUR
	Odotettu kokonais-menetys				**20 MEUR**					**6,5 MEUR**	
	Kokonais-kustannus					**1,2 MEUR**					

Menetysten laskeminen Mallin B mukaan:
- Odotettu tappio (Expected loss) = todnäk*vaikutus

Kuva 6: Roskienhallintaviraston odotettu kokonaismenetys ja investointien kokonaiskustannus. Viimeisessä sarakkeessa on laskettu odotettu riskienhallinnan säästö (=odotettu menetys ennen – (riskienhallinnan kustannukset + odotettu menetys jälkeen)).

- *Roskienhallintavirasto* pystyy arvionsa mukaan pienentämään riskin numero 1 odotettua menetystä 7,5 MEUR:sta 1,25 MEURiin panostamalla 0,2 MEUR digitaalista turvallisuutta edistäviin toimenpiteisiin. Riskin numero 2 odotettua menetystä pystytään pienentämään 5 MEUR:sta 2,5 MEUR:iin panostamalla 0,4 MEUR:in edestä riskiä pienentäviin toimenpiteisiin jne.

- *Roskienhallintavirasto* arvioi pienentävänsä odotettua menetystä neljästä suurimmasta digiriskistä 20 MEUR:sta 6,5 MEUR:iin panostamalla 1,2 MEUR riskienhallinnan toimenpiteisiin. Kokonaisuutena *Roskienhallintavirasto* arvioi myös, että sijoittamalla tämän 1,2 MEUR vaikutus muihin kuin suurimpaan neljään riskiin on vielä merkittävämpi. Eli sijoitukset näihin riskeihin pienentävät samalla myös monia muita pienempiä riskejä, jolloin hyöty on vielä suurempi kuin taulukossa huomioidut neljän suurimman riskien vaikutus.

- *Esimerkissä huomioitavia asioita*

  – Riskien vaikutuksia voidaan myös havainnollistaa laadullisilla mittareilla kvantitatiivisen mittareiden (euron) sijaan, jolloin kustannusten määrän vertailu saatuun lopputulemaan on kvalitatiivinen. Yllä olevan esimerkin voisi myös tehdä täysin kvalitatiivisilla oletuksilla, silloin toki suora vertailtavuus riskien

(laadullinen mittaus) ja kustannusten (EUR) välillä hämärtyy. Kvalitatiivisten seurausten ymmärtäminen saattaa kuitenkin olla huomattavan paljon tärkeämpää kuin kvantitatiivisten seurausten ymmärtäminen, joten tätä aspektia ei saa unohtaa menetyksiä arvioitaessa. Euromääräinen mitattavuus ei siten ole riskien arvioinnin ainoa tavoite, lähinnä se helpottaa asian seurantaa, arviointia, yhteismitallisuutta ja kommunikointia.

- Jäännösriskejä hallitaan osana organisaation normaalia riskienhallinnan prosessia, ja niiden koko ohjaa tyypillisesti sitä, millä organisaation tasolla niistä päätetään ja missä niistä otetaan vastuu. Jäännösriski saattaa olla luonteeltaan erilainen kuin alkuperäinen riski. Siten riskin omistajuus saattaa siirtyä organisaatiossa alkuperäiseltä riskin omistajalta toiselle.

- Kustannusten käyttö saattaa vaikuttaa eri tavoin riskeihin. Kustannukset saattavat vaikuttaa todennäköisyyteen, vaikutukseen tai molempiin. Kustannuksen käyttö yhteen kohteeseen saattaa vaikuttaa moneen riskiin, toisaalta kustannusten käyttö moneen kohteeseen saattaa kaikki vaikuttaa yhteen riskiin.

5 Digitaalisen turvallisuuden kustannusluokittelumalli

Digitaalisen turvallisuuden kustannus-vaikuttavuuden arvioinnin kannalta on oleellista, että turvallisuuteen liittyvät kustannukset voidaan tunnistaa ja luokitella julkishallinnon organisaatioissa yhteneväisellä tavalla. VTV:n vuonna 2017 tehdyn selvityksen mukaan julkisen hallinnon organisaatiot budjetoivat digitaaliseen turvallisuuteen käytettävät varat toimintamenomomentille erittelemättömänä osana organisaation toiminnasta aiheutuvia kustannuksia.[10]

Jotta digiturvallisuuteen liittyviä kustannuksia voidaan seurata, mitata ja hyödyntää osana digitaalisen turvallisuuden kustannus-vaikuttavuusanalyysiä on välttämätöntä pyrkiä erottamaan digitaaliseen turvallisuuteen liittyvät kustannukset muista tietohallinnon, palveluhankintojen sekä muista organisatorisista kustannuksista. Tämä edellyttää kustannusten tunnistamista ja siitä seuraavaa kustannusten luokittelua.[11]

Kustannusten tunnistaminen ja luokittelu on toisistaan riippuvaisia. Kustannusten tunnistaminen edellyttää, että organisaatioilla on yhtenäinen käsitys siitä mitä digitaalisen turvallisuuden kustannuksiin sisältyy. Yhtenäinen tapa luokitella kustannuksia edesauttaa kehittämään yhtenäistä ymmärrystä kustannusten sisällöstä ja rakenteesta ja auttaa täten myös kustannusten seurannassa sekä optimoimaan paremmin resurssien käyttöä.

Kustannuksia voidaan luokitella monin eri tavoin. Ohjaavana tekijänä tulee pitää, että kustannukset luokitellaan tavalla, joka on:

- Ymmärrettävä eli merkitykset ja tarkkuudet ovat sopivia
- Toteutettavissa oleva (tehokkaasti) eli hyöty suhteessa vaivaan on sopiva
- Hallintomallia eli toimintaa, koordinaatiota ja kehittämistä tukeva
- Linkitettävissä (potentiaalisiin) menetyksiin eli riskiperusteista

Ymmärrettävällä luokittelulla tarkoitetaan sitä, että luokkien määrittely on niin selkeää, että kustannuksia käsittelevät henkilöt pystyvät yhtenäisellä tavalla luokittelemaan kulut oikeisiin kululuokkiin ja hahmottamaan niiden merkityksen. Toteutettavissa olevalla luokittelulla tarkoitetaan sitä, että luokiteltavassa aineistossa (esim. laskut) tulee olla (tai siihen voidaan liittää) riittävästi tietoa, jotta kulu osataan ohjata oikeaan luokkaan. Myös tämän tiedon kerääminen tulee tapahtua käytännössä toteutettavissa olevalla tavalla, minkä haasteellisuuteen vaikuttaa kulujen käsittelyprosessi ja järjestelmien integraatio. Asia on merkittävä, sillä hienojakoisemman tiedon tarve, automatisointi sekä reaaliaikaisuus tulevat korostumaan tulevaisuudessa.

---

[10] *Valtiontalouden tarkastusvirasto. (2017). Kybersuojauksen järjestäminen. Tuloksellisuustarkastuskertomus. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Dnro 185/54/2016*. (https://www.vtv.fi/app/uploads/2018/05/22102159/kybersuojauksen-jarjestaminen-16-2017.pdf)

[11] *Digitaalisen turvallisuuden kustannus- vaikuttavuusarviointi julkishallinnossa – selvitystyöraportti 2020, Valtiovarainministeriö*. (https://vm.fi/documents/10623/306832/Digitaalisen+turvallisuuden+kustannus-vaikuttavuusarviointi+julkisessa+hallinnossa+%28selvitysty%C3%B6n+raportti+1.6.2020%29/c79cab0d-ba57-1d20-1e17-772cd24a9d62/Digitaalisen+turvallisuuden+kustannus-vaikuttavuusarviointi+julkisessa+hallinnossa+%28selvitysty%C3%B6n+raportti+1.6.2020%29.pdf)

Hallintomallia tukevalla luokittelulla tarkoitetaan sitä, että luokittelumalli on julkishallinnon organisaation toimintaa ohjaavaan hallintomalliin soveltuvaksi todettu luokittelumalli, siten, että luokittelu kuvaa sen osa-alueita riittävän uskottavasti. Kulujen ja kustannusten vaikutuksia arvioitaessa on myös oleellista, että kustannusluokat ovat yhdistettävissä riskienarvioinnissa käytettäviin menetysluokkiin, jotta mahdollistetaan digitaalisen turvallisuuden kustannuksiin liittyvien hyötyjen mittaaminen.

5.1 Malli kulujen luokitteluun

Kulujen luokitteluun on kaksi lähtökohtaista mallia: datalähtöinen malli ja toimintalähtöinen malli. Mallit yhdistämällä voidaan pyrkiä hyödyntämään molempien parhaat puolet sekä tuottamaan tehokas toteutus. Molemmat mallit edellyttävät julkishallinnon organisaatioilta käytännön toimenpiteitä kulujen käsittelyssä ja merkitsemissä. Tarkoituksena on erottaa ”IT-kuluista” turvallisuuteen keskeisesti liittyvät menot riittävällä tarkkuudella ja systemaattisuudella, jotta kohdistuksen merkitystä voidaan arvioida ja siten ohjata.

Mallien tukena on syytä käyttää sellaisia rakenteita, jotka mahdollisuuksien mukaan ovat jo organisaatioissa eri tavoin käytössä, todettu käyttöön toimiviksi turvallisuuden hallinnassa sekä ovat sovellettavissa yhteiseen yhdenmukaiseen käyttöön. Näiden viitekehysten rakennetta (niiden osa-alueiden määrittelyä ja niissä käytettyjä otsikointeja, jotka kuvaavat alaosioita eri tarkkuuksilla) voidaan soveltaa käytettäväksi luokitteluina. Näillä ei ole tarkoitus korvata olemassa olevia prosesseja vaan organisaatio voi käyttää niitä myös turvallisuusprosessien lisäksi tai rinnakkaisena prosesseina, vaihtoehtoisena mallina/luokitteluna hallintatoimissa tai näiden analysoinnissa. Erityisesti digitaalisten ja automatisoitujen hallinta-, toiminnanohjaus- ja raportointijärjestelmien (mm. koontinäkymät ja mittaristot) kehittyessä on mahdollista hyödyntää useita tapoja käsitellä ja tarkastella myös digiturvallisuuden ja riskienhallinnan tietoja. Systemaattisen tarkastelun myötä voidaan määritellä mittareita ja raja-arvoja, joilla tuetaan priorisointia, erityiseen tarkasteluun nostamista ja strategisia valintoja, ohjaamista ja päätöksiä.

5.1.1 Datalähtöinen tai toimintalähtöinen luokittelumalli

Datalähtöisellä mallin kehittämisellä tarkoitetaan lähestymistapaa, jossa kustannusluokkien muodostaminen on datalähtöistä eli luokkien muodostumista ohjaavat esimerkiksi ne tiedot, joita voidaan tunnistaa laskuista ja muista kustannusasiakirjoista.

Mallin hyviin puoliin kuuluu, että luokittelusta tulee käytännönläheinen. Parhaimmillaan data saadaan jo olemassa olevien prosessien sivutuotteena, mutta tavallista on, että niitä pitää täydentää. Hankintojen kohdalla voidaan jo esimerkiksi tehdä suuntaa antavia päätelmiä siitä, mistä hankinta on tehty, ketkä sitä ovat käsitelleet ja mitä avainsanoja siinä on tunnistettavissa. Mikäli luokittelu halutaan kytkeä johonkin viitekehykseen “data kertoo” mihin se parhaiten sopii.

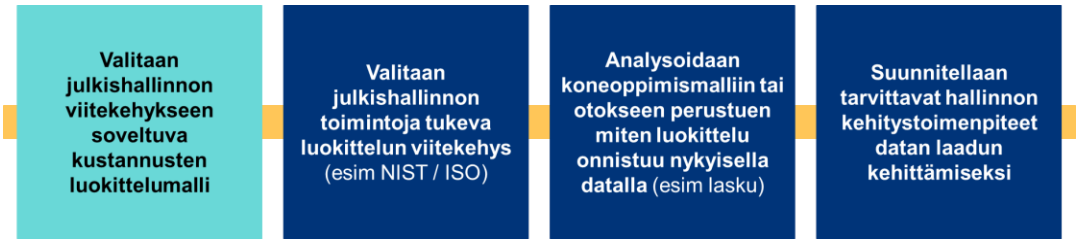
Mallin heikkoudet liittyvät data-aineiston (esim. laskujen) laadulliseen selkeyteen. Mikäli laskut eivät ole riittävän selkeitä ja yksilöityjä luokittelusta voi tulla hyvin geneerinen, jolloin esimerkiksi luokittelun kytkentä toimenpiteisiin sekä niiden menetyksiin ja hyötyihin voi vaikeutua. Liian yksinkertainen luokittelu ei palvele kustannus-vaikuttavuuden arvioinnin käyttötarkoitusta, eikä siten tuota riittävästi lisäarvoa riskienhallinnan analyysien tueksi suhteessa vaivaan ja kustannuksiin, vaikka joillekin

organisaatioille jo turvallisuuteen pääosiltaankin liittyvien kustannusten tunnistaminen on askel eteenpäin.

Kuva 7: Datalähtöinen luokittelumalli: Luokittelumallissa huomioidaan mitä "data mahdollistaa" ja kehitystoimenpiteet keskittyvät matalalla roikkuviin hedelmiin.

Toimintalähtöisen luokittelumallin lähtökohtana on valmiit viitekehykset, kuten ISO2700-sarjan tai NIST Cybersecurity Framework (NIST CSF), joita hyödynnetään organisaatiossa digitaalisen turvallisuuden hallinnan tukena.[12] Valmiin viitekehyksen hyödyntäminen palvelee julkishallinnon hallintoperiaatteita. Ne ovat jatkuvan kehityksen ansiosta pääsääntöisesti selkeitä ja ymmärrettäviä sekä yleisesti tunnettuja ja hyväksyttyjä. On myös oletettavaa, että yleisesti käytössä olevaan rakenteeseen perustuva luokittelumalli on selkeämmin kytkettävissä riskien ja menetysten määrittelyssä käytettävään malliin.

Heikkoutena kyseisen mallin luokittelussa on, että vaikka malli yleisesti tunnettu, sen käytännön toteutus, eli esimerkiksi laskuissa tunnistettavan datan käyttö sen mukaisesti, ei useinkaan ole yhtä suoraviivaista, saati jo valmiiksi olemassa. Kustannusten luokittelun käytännön haasteet voivat vääristää mallin vertailukelpoisuutta. Esimerkiksi tulkintaerot luokittelussa voivat merkittävästi vinouttaa tuloksia. Lisäksi mallien mahdollistaman yksityiskohtaisuuden tason suhteen on löydettävä tasapaino riittävän tiedon tarkkuuden ja käytännön toteutettavuuden välillä. Tämä ongelma tosi muuttuu merkityksettömäksi, mikäli toiminnanohjaus- tai maksujärjestelmät kykenevät automatisoidusti oikean kontekstin tunnistamiseen.



Kuva 8: Toimintalähtöinen luokittelumalli: Luokittelumallissa huomioidaan julkishallinnon hallintomallin tarpeet.

[12] *Muun muassa ISO27000-sarja ja NIST CSF toimivat esimerkkeinä ja suuntaviivoina monille organisoitumisen ja koordinaation rakenteille, eikä edellytyksenä tai oletuksena ole virallisen standardoidun mallin käyttö.*

5.1.2 NIST CSF kustannusluokittelun perustana

NIST Cybersecurity Framework -viitekehys[13] (NIST CSF) toimii työkaluna, jolla organisaatiot voivat järjestää sekä parantaa omaa digiturvallisuuden hallintaansa erityisesti käytännön tasolla. Se ohjaa organisaatioita rakentamaan tehokkaampaa ja organisoidumpaa digiturvallisuutta perustuen häiriöiden ilmenemiseen ja tämän ennakointia tukevaan prosessirakenteeseen (ns. alhaalta-ylös tai toimintalähtöinen rakenne). Malli on sovellettavissa myös turvallisuusarkkitehtuuriin[14].

Viitekehys antaa erilaisia suosituksia ja selkeitä ohjeita, kuinka kyberhäiriöihin tulisi ennaltaehkäistä, reagoida onnettomuuden tapahtuessa ja palautua ongelman sattuessa. Toimintojen avulla katetaan mm. organisaation data, ohjelmat, infrastruktuuri ja työntekijät. Sen käytöllä kaiken kokoiset organisaatiot pystyvät paremmin ymmärtämään, hallitsemaan ja vähentämään heihin kohdistuvaa kyberturvallisuuden riskiä. Viitekehyksen käyttö vaatii sen käyttäjiltä osaamista ja kokemusta digitaalisesta turvallisuudesta laajasti, vaikka sen taksonomia erityisesti ohjaa kohti uhkiin liittyviä relevantteja riskienhallintatoimia.

NIST CSF sisältää 5 avaintoimintoa, joilla on 23 kategoriaa ja 108 alakategoriaa:

- Tunnistaminen
- Suojautuminen
- Havainnointi
- Reagoiminen
- Palautuminen

5.1.3 ISO /IEC 27001 ja 27002 kustannusluokittelun perustana

ISO/IEC 27000 -sarja on joukko kansainvälinen standardointijärjestön International Electrotechnical Commission (ISO) luomia tietoturvastandardeja, jotka liittyvät informaatioteknologiaan. Se tarjoaa parhaat käytännöt tietoturvariskien hallintaan ISMS:n (Information Security Management System) avulla. Näihin liittyvät myös muut hallintajärjestelmät, kuten laadunvarmistus ja ympäristönsuojelu. Se tukee organisaatioita rakentamaan tehokkaampaa ja organisoidumpaa digiturvallisuutta hallinta- ja koordinointitoimenpiteitä järjestelmällisesti ohjaavalla hallintarakenteen kehittyvällä prosessilla (ns. ylhäältä-alas rakenne). ISO27000:ssä noudatetaan ISO31000-sarjassa kuvattua standardoitua riskienhallinnan prosessia ja se on yhteensopiva erilaisten muiden johtamisen-, laadun kehittämisen- ja hallinnoinnin standardien kanssa.

ISO 27000-sarja kattaa useita kokonaisuuksia. Siinä ISO27002 standardi on tarkoitettu organisaatioiden käyttöön standardiin ISO/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toteuttamisprosessissa tai ohjeistukseksi organisaatioille, jotka toteuttavat yleisesti hyväksyttyjä tietoturvallisuuden hallintakeinoja. Standardi on suunniteltu organisaatioille, jotka aikovat valita hallintakeinoja standardiin ISO/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toteuttamisprosessin

[13] *Tässä viitataan CSF versioon 1.1 (2023):* (https://www.nist.gov/cyberframework)

[14] *DVV:* (https://wiki.dvv.fi/display/DTARK)

puitteissa, huomioiden, että jokaisen organisaation on itse määriteltävä oma toimintaympäristönsä, tarpeensa ja riskinsä.

ISO 27002 sisältää 14 pääkohtaa, joiden alla on 35 pääturvallisuusluokkaa ja 135 hallintakeinoa:

1. Tietoturvapolitiikat
2. Tietoturvallisuuden organisointi
3. Henkilöstöturvallisuus
4. Suojattavan omaisuuden hallinta
5. Pääsynhallinta
6. Salaus
7. Fyysinen turvallisuus ja ympäristön turvallisuus
8. Käyttöturvallisuus
9. Viestintäturvallisuus
10. Järjestelmien hankkiminen, kehittäminen ja ylläpito
11. Suhteet toimittajiin
12. Tietoturvahäiriöiden hallinta
13. Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia
14. Vaatimustenmukaisuus

5.1.4 NIST CSF- ja ISO- viitekehyksien hyödyntäminen kustannusten seurantaan

NIST CSF- mallin käsittelytapa häiriöprosessin suunnasta, yhdistettynä ISO27001:n malliin yleisesti käytetystä johtamisrakenteesta, luovat yhdessä kattavan tavan luokitella digitaalisen turvallisuuden ja siihen liittyvien riskien kuluja. Tässä esiteltävässä digiturvallisuuden kustannusten luokittelumallissa kulut luokitellaan lisäksi organisaatiolliselle tasolle ja toiminnalliselle tasolle. Organisaatiollinen taso koostuu digiturvallisuuden hallinnointiin liittyvistä kuluista kuten palkat, tietoisuuden kasvattaminen, koulutukset ja vastaavat yleisluontoiset menot, jotka rakentavat pohjaa tai mahdollistavat, kun taas toiminnalliset kulut liittyvät, suorempiin, digiturvallisuuden kohdistettavampiin kustannuksiin käytännön tasolla.

Sekä organisaatiollisten että toiminnallisten kulujen seurantaan ja luokitteluun käytetään NIST CSF:n pääluokkia (5 luokkaa) sekä pääluokkien alle soveltuvia ISO 27002 hallintastandardin pääkohtia (14 kohtaa).

Koska osa digiturvallisuuteen liittyvistä yleisemmistä kustannuksista, kuten henkilökulut, on vaikea kohdistaa NIST CSF:n pääluokkien alle, on kustannusten luokittelua jatkettu lisäämällä kaksi kustannusluokkaa: Henkilökulut sekä Muut kulut. Henkilökuluiksi voidaan luokitella sekä organisaation omia henkilökuluja että ulkopuolisia digiturvallisuuteen liittyviä henkilökuluja, mikäli nämä eivät suorasti liity esimerkiksi tiettyyn toimenpiteeseen. Muihin digiturvallisuuskuluihin voidaan luokitella yleisiä hallinnollisia (koulutus, tiedottaminen, seminaarikulut jne.) jotka eivät ole suoraan luokiteltavissa ISO2700 tai NIST CSF luokkien mukaan.

Kustannusten luokittelumallista tulee näin matriisi, jossa olisi teoreettisesti 98 kustannusluokkaa. Käytännössä kustannusluokkia on kuitenkin vähemmän, sillä ISO27002 ja NIST CSF luokat ovat osin sisäkkäisiä: esimerkiksi ISO27002 Jatkuvuuden hallintaan liittyvät kulut ja NIST CSF Palautuminen pääluokka.

Luokittelu on myös luonteeltaan suuntaa antava ja kuvastaa enemmän kustannusten seurannan tavoitetilaa. On oletettavaa, että kulujen seurannan luokittelun käytännön pilotit ja testit vaikuttavat luokittelun käytännön granularisuuteen. Tällä tarkoitettaan, että käytäntö ja tietotarpeet (jotka ovat kehittyneet hienovaraisemman tiedon suuntaan) osoittavat minkälainen tasapaino on löydettävä tiedon tarkkuuden ja toteuttamisen vaivan välillä, huomioiden myös tieto tuottavien järjestelmien kehityksen tätä tukemaan. Luokittelu itsessään siis vain indikoi sen muodostamaa lisätyötä, sillä järjestelmien ja prosessien toiminnan muotoilulla on merkittävä vaikutus lopputulokseen. Keskeinen tekijä luokittelun liittyen on tunnistaa kuluun liittyvä konteksti.

Toiminnallinen ja organisaatiollinen taso DIGITURVALLISUUDEN KUSTANNUKSET							
ISO27002 / NIST CSF	Tunnista-minen	Suojau-tuminen	Havain-nointi	Reagointi	Palau-tuminen	Henkilö-kulut	Muu
Tietoturvapolitiikat							
Suojattavan omaisuuden hallinta							
Vaatimustenmukaisuus							
Tietoturvallisuuden organisointi							
Henkilöstöturvallisuus							
Pääsynhallinta							
Salaus							
Fyysinen turvallisuus ja ympäristön turvallisuus							
Käyttöturvallisuus							
Viestintäturvallisuus							
Järjestelmien hankkiminen, kehittäminen ja ylläpito							
Suhteet toimittajiin							
Tietoturvahäiriöiden hallinta							
Jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia							

Kuva 9: NIST CSF luokat (vaaka-akseli) sekä ISO27002 (pystyakseli) muodostaa mallin kululuokittelu-matriisista. Jokaisen kulun osalta tulee siis valita kaksi muuttujaa: esim. kulu liittyy Salaukseen ja Suojautumiseen. Koska kaikki NIST CSF / ISO27002 yhdistelmät eivät ole loogisia, esim. tietoturvapolitiikat liittyvät tyypillisesti tietoturvauhkien tunnistamiseen, suojautumiseen ja havainnointiin mutta ei reagointiin tai palautumiseen, ei matriisiin kaikkiin soluihin kirjaudu kustannuksia. Kuvassa harmaat solut kuvaavat esimerkinomaisesti epätodennäköisiä kululuokkia, joita ei todennäköisesti tarvitse käyttää.

Yllä oleva kuva havainnollistaa esimerkkiorganisaation erilaisia kululuokkia, jaettuna vaakatasolla NIST CSF luokkiin (sekä henkilö-/hallinnointi ja muihin kuluihin) sekä pystytasolla ISO 27002 mukaiseen 14 pääkohtaan. Koska kaikki ISO luokat eivät kohdistu kaikille NIST CSF toiminnoille on kuvassa esimerkinomaisesti muutettu harmaaksi sellaisia yhdistelmiä, jotka eivät ole todennäköisiä.

Luokittelu on, käytettyjen mallien johdosta yleiseen käyttöön soveltuva, mutta sikäli suuntaa antava, että siihen voi kohdistua poikkeuksia. Muiden, hallinnollisten kustannusten, luokittelun osalta organisaatio voi lisätä tarvittaessa malliin uusia kategorioita. Lisäksi on mahdollista, että joillain organisaatioilla on poikkeavia järjestelyitä, jolloin jokin yksittäinen ruutu jää merkityksettömäksi.

Mallissa esimerkkiorganisaatio kohdistaa itse digiturvallisuuteen liittyviä kustannuksia ja kuluja valmiiksi määritellyn matriisin mukaisesti sen mukaan mihin luokkaan kulun arvioidaan kuuluvan. Lopputuloksena on kulurakenne yrityksen digiturvallisuuteen rahallisista panostuksista. Malli auttaa organisaatioita sekä seuraamaan digitaaliseen turvallisuuteen liittyviä kuluja yhdenmukaisesti että yhdistämään ne riskien- ja menetystenhallinnan prosesseihin, nähden niiden vaikutukset.

5.1.5 Malli kulujen kohdistamiseen

Digitaaliseen turvallisuuteen liittyviä kustannusten luokittelua, eli yksittäisten kuluerien kohdistamista eri kustannusluokkiin, voidaan tehdä eri tavoin. Kulujen luokitteluun voidaan hyödyntää esimerkiksi laskussa tai hankintapäätöksessä olevia tietoja kuten: toimittajatietoja, viitetietoja ja muuta informaatioita.

Operatiivisella tasolla, eli yksittäisen kulun luokittelua voidaan tehdä:

- Osana laskujen tarkastus ja hyväksyntäprosessia: jolloin laskun tarkastanut / hyväksynyt henkilö subjektiivisen näkemyksen mukaan luokittelee kulun oikeaan luokkaan.
- Kulujen luokitteluun voidaan myös hyödyntää tekoälyyn pohjautuvia oppivia järjestelmiä, jotka mahdollistavat kulujen automaattisen tunnistamiseen ja luokitteluun.

Takautuvasti tehtävä kulujen luokittelu voi olla työläs tehtävä, mikäli kuluja tulee luokitella usean vuoden ajalta. Massaluokittelua voidaan helpottaa joko otokseen perustuvalla luokittelulla tai hyödyntäen oppivia järjestelmiä:

- Massaluokittelua eli takautuvasti laskettavaa kulujen arviointia voidaan tehdä otokseen perustuvalla selvitystyöllä, jolloin esim. ICT-kustannuksista otokseen pohjautuvan arvioidaan kulujen jakautuminen eri luokkiin. Otokseen perustuvassa luokittelussa on omat ongelmansa. Jos otos tehdään organisaatiokohtaisesti mutta rajataan ajallisesti (esim. tutkitaan 6kk:n kulut) on mahdollista, että harvemmin toteutuvat kuluerät vääristyvät. Jos taas otos rajataan organisaatio näkökulmasta (tarkastellaan muutamaa organisaatioita ja oletetaan että näiden kulujakauma on samanlainen, kun muilla) voi taas organisaatiokohtaiset erovaisuudet jäädä piiloon.
- Toisena vaihtoehtona myös takautuvasti tapahtuvaan kulujen luokitteluun on hyödyntää tekoälyä ja oppivia järjestelmiä, jolloin voidaan tarkastella ja luokitella isompia tapahtumamääriä. Vaikka tämänkaltainen lähestymistapa mahdollista kaikkien kulujen tarkastelun isona massana voi lähestymistapa kuitenkin edellyttää mittavaa järjestelmän opettamistyötä.

Luokiteltuja kuluja voidaan kirjata seurannan alkuvaiheessa, esimerkiksi taulukkolaskentajärjestelmään mutta pidemmällä aikavälillä voi seuranta vaatia tilikarttamuutoksen, jonka avulla digiturvallisuuden kustannukset voidaan luokitella suoraan organisaatioiden talousjärjestelmiin.

6 Digiturvallisuuden arvomalli - riskienhallintatoimenpiteiden vaikutus eri riskeihin

Digitaalisen turvallisuuden kustannusmallissa on monta eri kustannuserää, jotka vaikuttavat eri tavalla digitaalisen turvallisuuden menetyksiin ja eri riskeihin. Näiden yhteys on tärkeä hahmottaa, jotta saadaan kohdistettua kustannukset optimaalisesti. Kustannusten käyttö vaikuttaa usein useampaan riskiin. Mallia, joka sisältää organisaation arvion menetyksen arvosta, riskin todennäköisyydestä, sekä näistä johdetusta odotetusta menetyksestä kutsutaan tässä dokumentissa digiturvallisuuden arvomalliksi. Malli huomio myös organisaation digiturvallisuuden maturiteetin sekä digiturvallisuuden kustannukset

Mikäli käytetään kustannuksia esimerkiksi tietoturvahenkilöstön palkkaukseen, se useimmiten vaikuttaa useisiin riskeihin. Toisaalta tietyt kustannuserät vaikuttavat selkeästi enemmän tiettyihin menetyksiin, kuten salaukseen investoiminen vaikuttaa mm. luottamuksellisen tiedon vuotamisesta aiheutuviin seurauksiin, mutta ei välttämättä ollenkaan esim. ihmisten henkeen ja terveyteen kohdistuviin menetyksiin.

Oheiseen kuvaan on hahmoteltu tätä syy-yhteyttä. Kustannukset on digitaalisen turvallisuuden kustannusmallin mukaisesti hahmoteltu pystysuoraan sarakkeeseen, kun taas menetykset digitaalisen turvallisuuden arvomallin mukaisesti on hahmotettu vaakasuoralle riville.

Menetykset / Toimenpiteet	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	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
Tietoturvapolitiikat	●	●	●	●	●	●	●	●	●	●
Suojattavan omaisuuden hallinta	●	●	●	●	●	●	●	●	●	●
Vaatimustenmukaisuus	●	●	●	●	●	●	●	●	●	●
Tietoturvallisuuden organisointi	●	●	●	●	●	●	●	●	●	●
Henkilöstöturvallisuus	●	●	●	●	●	●	●	●	●	●
Pääsynhallinta	●	●	●	●	●	●	●	●	●	●
Salaus	●	●	●	●	●	●	●	●	●	●
Fyysinen turvallisuus ja ympäristön turvallisuus	●	●	●	●	●	●	●	●	●	●
Käyttöturvallisuus	●	●	●	●	●	●	●	●	●	●
Jne…										

Kuva 10: Toimenpiteiden ja niihin liittyvien kustannusten vaikutus riskeihin ja niihin liittyviin menetyksiin

Ensimmäinen sarake ”Toimenpiteet” kuvaa organisaation investointeja erilaisiin mahdollisiin toimenpiteiseen, jotka on kuvattu digitaalisen turvallisuuden kustannusmallin mukaisesti. Ne koostuvat erilaisia kustannuseristä, joihin organisaatiot voivat investoida saavuttaakseen mahdollisia menetyksien vähennyksiä, joita kuvataan ensimmäisellä ”Menetykset” rivillä. Nämä koostuvat mahdollisista menetyksistä, joita organisaatio voi kokea. Taulukko siis kuvaa palloilla investointien vaikutuksia mahdollisiin menetyksiin kategorioittain.

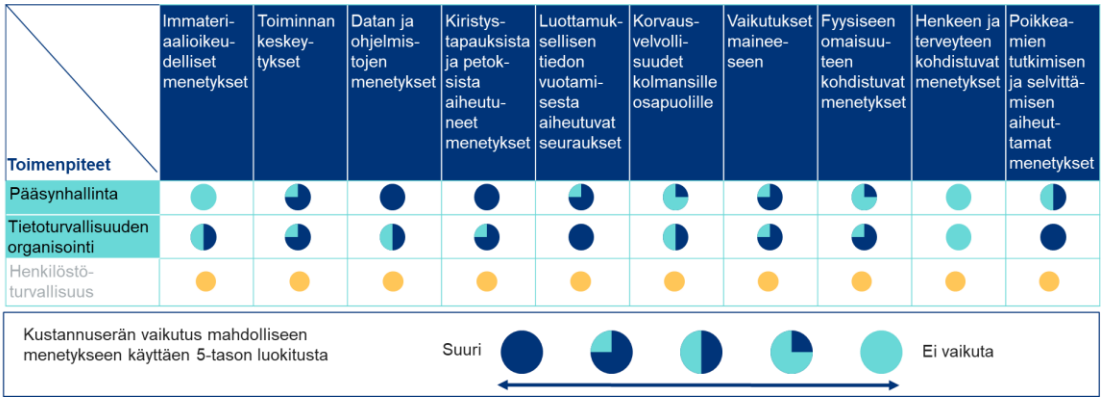
Taulukolla voidaan hahmottaa miten erilaiset toimenpiteet vaikuttavat organisaatioon kohdistuviin mahdollisiin menetyksiin esimerkiksi kuvan oikeassa alalaidassa kuvatuilla palloilla. Pallot on jaettu viiteen suuruusluokkaan pienimmästä (”ei vaikuta”) suurimpaan (”suuri”), ja määrittelevät millainen vaikutus toimenpiteellä on kuhunkin menetysluokkaan. On huomioitavaa, että vaikutukset vaihtelevat organisaation mukaan monista eri muuttujista riippuen. Yllä olevassa kuvassa asiaa on havainnollistettu yleisellä tasolla, mutta jokaisen organisaation on itse pohdittava miten kustannukset vaikuttavat mihinkin riskiin ja kuinka paljon.

6.1 Arvomallin riskienhallintatoimenpiteiden käytännön esimerkkejä

Alla on kuvattu muutama esimerkki siitä, miten digiturvallisuuden arvomallia voi hyödyntää käytännössä.

Esimerkki investoiminen pääsynhallintaan:

Roskienhallintavirasto on todennut tarpeen investoida kyberturvallisuuden toimenpiteisiin, jotta se pystyy pienentämään mahdollisia menetyksiä mahdollisen riskin toteutuessa. Tässä esimerkissä (Kuva 11) virasto investoi pääsynhallintaan sekä tietoturvallisuuden organisointiin, jotta se saisi seuraavat vaikutukset mahdollisiin menetyksiin kustannus-vaikuttavuusmallin mukaisesti:



Kuva 11: Roskienhallintaviraston arvio toimenpiteiden ja investointien vaikutuksista menetyksiin

Roskienhallintaviraston investoiminen toimenpiteeseen *”Pääsynhallinta*” nähdään vaikuttavan eniten datan ja ohjelmistojen menetyksiin sekä kiristystapauksista ja petoksista aiheutuneet menetyksiin. Vaikutukset ovat kohtuullisen suuret myös toiminnan keskeytyksen aiheutuviin menetyksiin, luottamuksellisen tiedon vuotamisesta aiheutuviin menetyksiin, vaikutukseen organisaation maineeseen ja poikkeamien tutkimisen ja selvittämisen aiheutuviin menetyksiin. Investoinneilla nähdään olevan

pienempi vaikutus fyysiseen omaisuuteen kohdistuviin menetyksiin sekä mahdollisiin korvausvelvollisuuksiin kolmansille osapuolille. Investoinnilla ei nähdä olevan vaikutusta lainkaan immateriaalioikeudelliset menetyksiin eikä henkeen ja terveyteen kohdistuvissa menetyksissä.

Investointi toimenpiteeseen *”Tietoturvallisuuden organisointi”* vaikuttaa eniten luottamuksellisen tiedon vuotamisesta aiheutuviin menetykseen sekä poikkeamien tutkimisen ja selvittämisen aiheutuviin menetyksiin. Vaikutusten nähdään olevan kohtuullisen suuret myös toiminnan keskeytyksen aiheutuviin menetyksiin, fyysiseen omaisuuteen kohdistuviin menetyksiin, organisaation maineeseen ja kiristyksistä ja petoksista aiheutuviin menetyksiin. Investoinnilla nähdään olevan keskinkertainen vaikutus datan ja ohjelmiston menetyksistä kohdistuviin menetyksiin sekä mahdollisiin korvausvelvollisuuksiin kolmansille osapuolille ja immateriaalioikeudellisiin menetyksiin. Investoinnilla ei nähdä olevan vaikutusta lainkaan henkeen ja terveyteen kohdistuviin menetyksiin.

Investoinnit eri toimenpiteisiin voidaan hyvin tehdä riskiperusteisesti, eli toisaalta digitaalisen turvallisuuden suurimmat riskit kannattaa jollain tavalla vähentää, oli se tapa sitten riskin poistaminen, vähentäminen, siirtäminen tai jotain muuta. Samalla on hyvä pohtia mihin kaikkiin riskeihin yksi investointi itse asiassa vaikuttaa, sillä usein investointi yhteen alueeseen vaikuttaa moneen eri riskiin.

Esimerkki: Investoiminen pääsynhallintaan ja sen vaikutus useampaan riskiin; kustannus-vaikuttavuusmalli käytännössä

Edellisen esimerkin mukaisesti pääsynhallintaan tehty investointi vaikuttaa *Roskienhallintavirastossa* eniten Datan ja ohjelmistojen menetyksiin, Kiristystapauksista aiheutuneisiin menetyksiin, mutta myös moniin muihin riskeihin.

Roskienhallintavirasto on päättänyt riskiperusteisesti investoida niihin digiturvallisuuden asioihin, joissa riskit ovat olennaisimmat. Riski datan ja ohjelmistojen menetyksiin heikon pääsynhallinnan takia on Roskienhallintavirastossa koettu isona riskinä (kts kuva 12), joten siksi virasto investoi pääsynhallinnan kehittämiseen 0,5 MEUR. Tällä investoinnilla virasto uskoo pystyvänsä pienentämään teoreettista odotettua riskitoteuman arvoa Datan ja ohjelmistojen menetysten osalta 2,5 MEUR:sta 0,5 MEUR:iin.

Menetykset / Toimenpiteet	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	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
Ei tehdä mitään			2,5 MEUR							
versus			↓ Riskin toteutuman odotusarvon pienennys							
Pääsynhallinta-investointi 0,5 MEUR			0,5 MEUR							

Kuva 12: Datan ja ohjelmistojen menetysten riski ennen ja jälkeen pääsynhallintaan tehdyn investoinnin

- Samalla *Roskienhallintavirasto* laskee että tällä yhdellä investoinnilla pystytään pienentämään odotettua riskitoteutumaa muidenkin riskien osalta. *Roskienhallintavirasto* arvioi, että muut riskit pienenevät alla olevan taulukon (kuva 13) mukaan pääsynhallintainvestoinnin kautta.

Menetykset / Toimenpiteet	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	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
Ei tehdä mitään		0,5 MEUR	2,5 MEUR	0,5 MEUR	1,0 MEUR		1,0 MEUR			
versus		↓	↓	↓	↓		↓			
Pääsynhallinta-investointi 0,5 MEUR		0,3 MEUR	0,5 MEUR	0,2 MEUR	0,2 MEUR		0,3 MEUR			

Kuva13: Kaikki merkittävimmät digiriskit ennen ja jälkeen pääsynhallintaan tehdyn investoinnin

Eli kokonaisuutena investoinnin pääsynhallintaan (0,5 MEUR) uskotaan pienentävän useiden riskien jäännösarvoa. Osoittautuu, että 0,5 MEUR investointi pääsynhallintaan itse asiassa pienentää useita riskejä kokonaisodotusarvosta 5,5 MEUR (kuvan 13 ylemmän rivin summa) tasolle 1,5 MEUR (kuvan 13 alemman rivin summa).

6.2 Organisaation digitaalisen turvallisuuden maturiteetin vaikutus saatavaan kustannushyötyyn

Digiturvallisuuden riskienhallintamalli on rakenteeltaan lähtökohtaisesti samankaltainen eri organisaatioille, mutta organisaation maturiteetti digitaalisen turvallisuuden hallinnassa olisi hyvä huomioida investointeja tehtäessä.

Organisaatio, joka on hyvin kypsällä maturiteettitasolla digitaalisessa turvallisuudessa, ei luultavasti saa yhtä paljon hyötyä lisäinvestoinneista kuin organisaatio, joka on hyvin alkeellisella tasolla. Esimerkiksi organisaatio, jolla on vähäinen määrä salauksia tänään, saa hyvin kohdistettuina investoinneilla merkittäviä hyötyjä luottamuksellisen tiedon vuotamisesta aiheutuvien seurausten osalta. Toisaalta organisaatiolla, jossa jo on investoitu salauksiin, ei välttämättä saada samaa hyötyä lisäinvestoinneista.

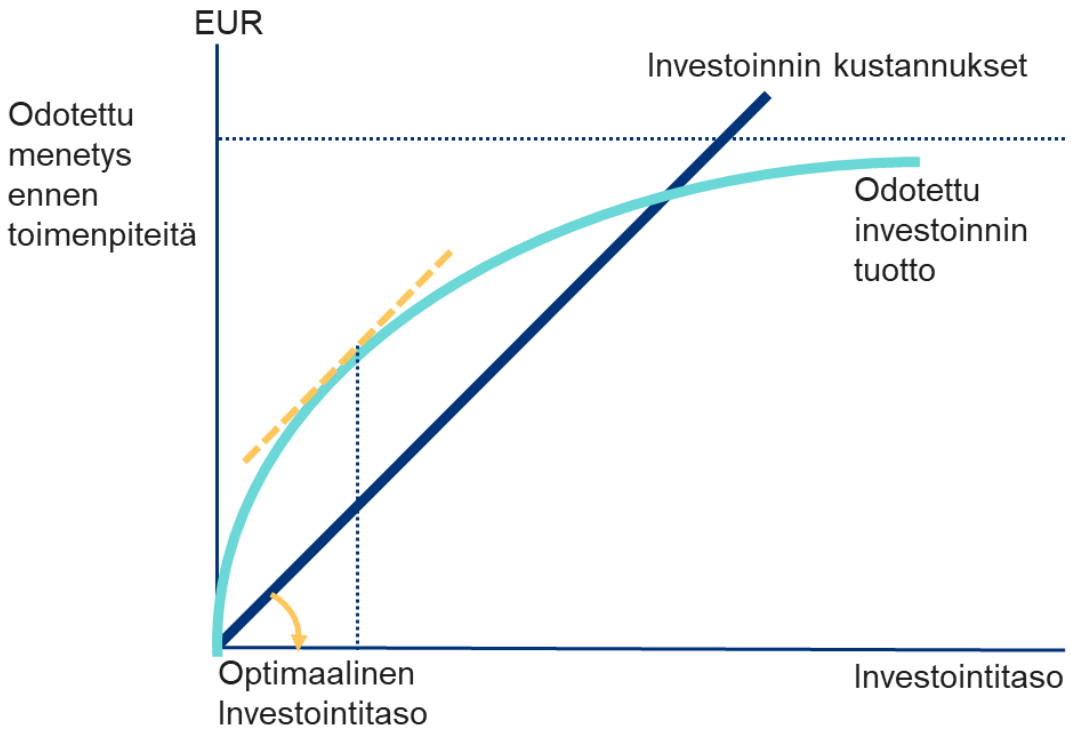
6.2.1 Tietoturvainvestointien hyöty ja Gordon-Loeb -malli

Organisaation maturiteetti vaikuttaa mallin mukaan siihen, kuinka paljon hyötyä eri investoinneilla saadaan aikaiseksi. Gordon-Loeb-mallissa[15] tämä asia on kuvattu oikealla olevan kuvan mukaan epälineaarisena funktiona, jossa marginaalinen lisähyöty investoinneista jossain vaiheessa rupeaa pienenemään. Optimaalinen kohta investoinneille löytyy (katkoviiva kuvassa), jonka jälkeen lisäinvestoinnit tuovat vähemmän ja vähemmän marginaalihyötyä organisaatiolle

[15] *Investing in Cybersecurity: Insights from the Gordon-Loeb Model* (https://www.scirp.org/journal/paperinformation.aspx?paperid=64892)

Gordon-Loeb -mallin mukaan ei kannata investoida tietoturvaan enempää kuin karkeasti 1/3 odotetun tappion arvosta. Investointia, joka on yli 37% odotetun tappion arvosta, ei Gordon-Loebin mukaan kannata tehdä ollenkaan.

Alla on kuvattu esimerkkinä Gordon-Loeb -malli, joka on pyrkinyt mallintamaan maturiteetin vaikutusta investoinneista saatavaan hyötyyn.



Kuva 14: Gordon-Loeb -malli: Digitaalisen turvallisuuden investoinnin hyötyfunktio. Investointien kasvaessa niistä saatava rajahyöty pienenee, jolloin voidaan tunnistaa laskennallisesti optimaalisin investointitaso. Investointien kohdistamiseen kohdistuu usein muita vaatimuksia, esimerkiksi lainsäädännöstä tai sopimuksista johtuen, jotka ohjaavat poikkeamaan mallissa esitetystä laskennallisesta optimista.

Marginaalinen lisähyöty investoinnista digitaaliseen turvallisuuteen vaihtelee organisaation tämän hetken maturiteetin perusteella. Jo paljon investoivalle yritykselle lisäinvestoinnit saattavat tuoda marginaalista lisähyötyä riskienhallintamielessä, kun taas alkeellisille organisaatioille kaikki investoinnit tuovat suhteessa enemmän hyötyä.

Koska digitaaliseen turvallisuuteen voi panostaa monella eri tavalla, on syytä pohtia myös oman organisaation maturiteettia digitaalisen turvallisuuden riskienhallinnan osalta. Alla olevassa esimerkissä on kuvattu kahden eri organisaation investointia ja sen riskiä pienentävä vaikutus viestintäturvallisuuteen.

6.2.2 Digiturvallisuuden maturiteetti arvomallissa - käytännön esimerkkejä

Seuraavassa on kuvattu muutama esimerkki organisaation digiturvallisuuden maturiteetin vaikutuksesta riskienhallintatoimenpiteiden hyötyihin.

Esimerkki: Tietoturvainvestointien tuoma rajahyöty kahdessa eri organisaatiossa

Roskienhallintavirasto ja *Riskienhallintavirasto* panostavat kukin 0,3 MEUR viestintäturvallisuuden kehittämiseen. Organisaatiot ovat muuten hyvin samankaltaiset, mutta *Riskienhallintavirastossa* on jo vuosia panostettu viestintäturvallisuuteen, kun taas *Roskienhallintavirastossa* ollaan aika lailla lähtökuopissa. Täten investoinnin tuoma rajahyöty on pienempi *Riskienhallintavirastossa* kuin *Roskienhallintavirastossa*. Samalla 0,3 MEUR:in investoinnilla *Roskienhallintavirasto* saattaa pienentää riskiään esim 50%, kun taas *Riskienhallintavirastossa* sama riski pienenisi vain esim. 10% (fiktiivinen esimerkki Gordon-Loebin mukaellen).

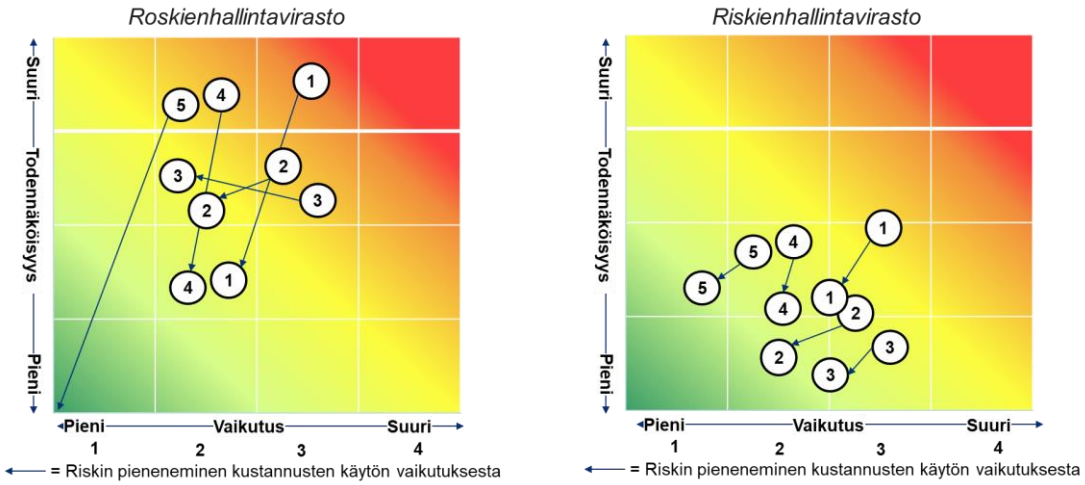
Ylläkuvatun tarkastelun pohjalta organisaatio voisi luokitella itsensä eri maturiteettitasoihin (esim. luokat 1-5) jokaisen kustannusmallin osa-alueen osalta. Kuinka kattava digiturvallisuuden organisaatio meillä on, mikä meidän henkilöstöturvallisuudentaso on, millä tasolla olemme pääsynhallinnassa, entä salausten osalta, jne. Esimerkki tällaisesta itsearvioinnista on kuvattu alla olevassa taulukossa.

Organisaation itse arvioima maturiteetti	Menetykset / Toimenpiteet	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	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
Maturiteetti 2	Tietoturvapolitiikat	●	●	●	●	●	●	●	●	●	●
Maturiteetti 4	Suojattavan omaisuuden hallinta	●	●	●	●	●	●	●	●	●	●
Maturiteetti 2	Vaatimustenmukaisuus	●	●	●	●	●	●	●	●	●	●
Maturiteetti 3	Tietoturvallisuuden organisointi	●	●	●	●	●	●	●	●	●	●
Maturiteetti 5	Henkilöstöturvallisuus	●	●	●	●	●	●	●	●	●	●
Maturiteetti 3	Pääsynhallinta	●	●	●	●	●	●	●	●	●	●
Maturiteetti 1	Salaus	●	●	●	●	●	●	●	●	●	●
Maturiteetti 2	Fyysinen turvallisuus ja ympäristön turvallisuus	●	●	●	●	●	●	●	●	●	●
Maturiteetti 3	Käyttöturvallisuus	●	●	●	●	●	●	●	●	●	●
	Jne…										

Kuva 15: Itsearvioinnin kautta voidaan saada tuntumaa investointien vaikuttavuudesta.

Yllä olevassa esimerkissä on kuvattu yhden fiktiivisen organisaation maturiteettia digitaalisen turvallisuuden eri aspekteissa (vasemmalla oleva numerointi 1-5, jossa 1=kehittymätön ja 5=hyvin kehittynyt). Mitä kehittyneempi organisaatio jo on jossain aspektissa, sen vähemmän rajahyötyä lisäinvestointi tuo riskin määrässä (todennäköisyyden ja/tai vaikutuksen kautta). Tämä pohdinta on hyödyllistä, kun pohditaan seuraavien investointien kohdistamista digitaalisen turvallisuuden parannuksiin.

Esimerkki: Samankokoisen kustannuksen käyttö kahdessa muuten samanlaisessa organisaatiossa, jossa toinen on maturiteetiltaan pidemmällä digitaalisen turvallisuuden hallinnan osalta kuin toinen



Kuva 16: Investointien vaikutus matalamman ja korkeamman maturiteetin organisaatiossa (Roskienhallintavirasto ja Riskienhallintavirasto)

Roskienhallintavirasto ja *Riskienhallintavirasto* ovat digitaalisen turvallisuuden osalta eri maturiteettitasoilla. Riskienhallintavirastolla on mallikkaasti hoidettu kokonaisuus, kun taas Roskienhallintavirastoilla on paljon kehitettävää.

Yllä olevassa kuvassa on kuvattu muuten identtisten organisaatioiden samankokoinen investointi digitaaliseen turvallisuuteen.

Sama asia pätee samaan yritykseen eri ajankohtina. Mitä pidemmälle yritys kehittää digitaalista turvallisuuttaan, sen vähemmän marginaalihyötyä uusi investointi aihepiiriin teoriassa tuo. Toki käytännössä maailmaa muuttuu koko ajan, ja siksi jo paikallaan pysyäkseenkin pitää allokoida kustannuksia.

7 Kustannus-vaikuttavuusmalli

Jotta organisaatio kykenisi turvaamaan arvoa strategisella tasolla, arvomalli tulee integroida strategiseen johtamiseen oikealla tavalla. Muuten riskinä on, että arvomallin hyödyntäminen toimintojen kehittämisessä ja riskien hallinnassa jää asiantuntijatasolle eikä integroitu organisaation johtamismalliin.

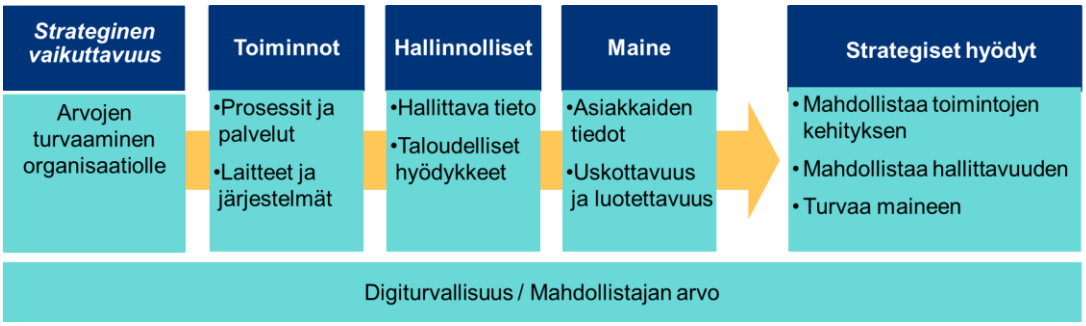
7.1 Digitaalisen turvallisuuden integrointi operatiiviselta tasolta strategiselle tasolle

ISO 31000-standardissa korostetaan ylimmän johdon roolia ja riskienhallinnan sisällyttämistä organisaation johtamisjärjestelmään. Riskienhallinta on osa hallintotapaa ja johtajuutta, ja se on keskeinen tekijä siinä, kuinka organisaatiota johdetaan kaikilla tasoilla. Riskienhallinta edesauttaa siten johtamisjärjestelmän kehittämistä. Keskeinen osa ISO 31000-standardia on organisaation arvon luominen ja säilyttäminen sisällyttämällä riskienhallinta organisaation johtamisjärjestelmään. Tämä tavoite on sovellettavissa myös julkisen hallinnon organisaatioihin.

Kustannus-vaikuttavuusmallin merkitys johtamiselle ja organisaation digiturvallisuuden kustannusten optimoinnille ei tapahdu ilman siihen tarkoitettua prosessia ja metodiikkaa. Vaikuttavuuden arvioinnin kannalta on ratkaisevaa, että prosessit ja tulokset yhdistellään eikä tarkastella vaan jompaakumpaa[16]. Mikäli arvomallia ei hyödynnetä strategisessa johtamisessa, kustannusten kohdentaminen ja niistä saatava hyöty riskien käsittelyssä eivät toteudu optimaalisella tavalla. Riskinä on, että panostetaan sinänsä hyviin asioihin, jotka eivät kuitenkaan strategisesta näkökulmasta ole keskeisimpiä ja merkittävimpiä. Panostuksen pitää myös olla oikeassa suhteessa siitä saatavaan hyötyyn; julkisen hallinnon puolella on huomioitava, että optimointi ja oikeansuuntaisuus rakentuu toisella tavalla kuin yksityisellä sektorilla johtuen julkisen hallinnon toisenlaisista olemassaolon tarkoituksesta. Julkisella puolella, toisin kuin yksityisellä puolella, ei voida hyväksyä tiettyjen riskien toteutumista (esim. turvaluokitellun tiedon paljastuminen) ja niiden käsittelyn on tapahduttava lainsäädännön asettamissa reunaehdoissa (mikä vaikuttaa esim. riskin siirtoon muualle yhteiskunnassa).

Digiturvallisuuden vaikuttavuus on sitä, että organisaation prosessit, palvelut, laitteet, järjestelmät, hallittava tieto ja taloudelliset hyödykkeet ovat turvattuja, ja täten myös esim. organisaation maine, luotettavuus ja lainsäädännöllisten tehtävien toteuttaminen on varmistettu. Digitaalinen vaikuttavuus mahdollistaa toimintojen kehityksen, tiedon ja taloudellisten hyödykkeiden hallittavuuden sekä turvaa maineen (kts kuva alla). Arvomallista päästään vaikuttavuustasolle varmistamalla, että arvomalliin sisältyvä analyysi otetaan osaksi organisaation strategisen tason suunnittelua ja johtamista. Tämä tapahtuu käytännössä huomioimalla johtamisen ja tiedon tarpeet paremmin käsittelytason muuttuessa.

[16] *Peter Dahler-Larsen: Vaikuttavuuden arviointi, Hyvät käytännöt-käsikirja, Stakes 2005* (https://www.julkari.fi/handle/10024/77071)



Kuva 18: Digiturvallisuuden strateginen vaikuttavuus: Kuvassa on yleisellä tasolla esitetty strategista tasoa ja strategisen tason organisaatiolle merkittäviä johtamisalueita, joita digitaalinen turvallisuus mahdollistaa, turvaa ja suojaa. Kun toiminnot, hallinto ja maine -kysymykset ovat riittävällä tavalla hoidettu, digiturvallisuus omalta osaltaan tukee strategisten hyötyjen muodostumista. Tätä hyötyjen muodostumista pyritään osaltaan optimoimaan hyvällä riskienhallinnalla ja sen sisällä käytettävällä vaikuttavuusmallilla.

7.2 Arvomallin muuntaminen vaikuttavuuden käsittelytasolle

Kun digitaalisen turvallisuuden arvomalli integroidaan osaksi organisaation strategista suunnittelua ja riskienhallintaa on huomioitava, että informaatio on kokonaisuudessa sovitettava johtamis- ja riskienhallintatarpeeseen soveltuvaksi. Analyysiä ja arviointia on kehitettävä strategiseen näkökulmaan (johtamisen ja päätöksenteon näkökulmaan ja työtapaan) soveltuvaksi ja siinä tehokkaasti hyödynnettäväksi. Tätä tehtäessä on hyvä huomioida muun muassa alla esitetyt käsittelytavat:

- Digitaalisen turvallisuuden riskejä suhteutetaan digitaalisen turvallisuuden kontekstissa eri tasoilla, myös digitaalisen turvallisuuden strategisena näkökulmana. Tässä dokumentissa kuvatut NIST CSF, ISO27000, SAINT, VAHTI-ohje ym. ovat keskiössä malleissa ja näissä on tunnistettava eri tasot erityyppisille riskikokonaisuuksille. Tällöinkin ylemmän tason digitaalisia riskejä suhteutetaan myös toisiinsa. Tällä tasolla digitaalisen turvallisuuden laajempien riskien käsittelyä tulisi pitää vähimmäisvaatimuksena organisaation vertikaalisesti läpäisevälle riskientarkastelulle ja sen tulisi tuottaa syötteitä organisaation päätöksenteon käyttöön[17].

- Digitaaliset riskit tulisi käsitellä osana organisaation muita riskejä, jolloin ne voivat olla esim. osa palveluiden tai prosessien riskikokonaisuuksia. Mallin integroinnissa riskitietoa käsiteltäessä seuraavalle kontekstuaaliselle tasolle digiturvallisuuden näkökulma muuttuu, laajenee, kun digiturvallisuudesta tulee kiinteämmin osa organisaation kokonaisriskienhallintaa. Yleisesti johtotasolla näkökulma riskeihin perustuu tyypillisesti COSO-ERM[18]-tyyppiseen luokitteluun, eli strategiset, operatiiviset ja taloudelliset riskit sekä vahinkoriskit. Tässä kontekstissa digiturvallisuuden riskit suhteutetaan muihin riskeihin ja strategian painopisteisiin sekä tavoitteisiin ja mahdollisuuksiin, mikäli ne ovat nousseet omina riskeinään tarpeeksi näkyviksi.

[17] *Kts. esim. Traficom: Kyberturvallisuus ja yrityksen hallituksen vastuu* (https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf).

[18] *COSO-ERM* (https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf)

Menetykset (EU SAINT) vs. COSO ERM riskiluokat	Immateriaali-oikeudelliset menetykset	Toiminnan keskeytykset	Datan ja ohjelmistojen menetykset	Kiristys-tapauksissa ja petoksista aiheutuneet menetykset	Luottamuk-sellisen tiedon vuota-misesta aiheutuvat seuraukset	Korvaus-velvollisuudet kolmansille osapuolille	Vaikutukset maineeseen	Fyysiseen omaisuuteen kohdistuvat menetykset	Henkeen ja terveyteen kohdistuvat menetykset	Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
Strategiset riskit										
Taloudelliset riskit										
Operatiiviset riskit										
Vahinkoriskit										

Kuva 19: EU SAINTin digiturvallisuuden mukaiset menetykset suhteutettuna COSO ERM:n riskiluokitteluun

- Tietosisältöjen viestiminen tehokkaasti edellyttää visuaaliseen ulkoasuun ja ymmärrettävyyteen panostamista. Riskitiedosta on siis tehtävä organisaation strategisen johtamisen ja päätöksentekoprosesseja tukevaa[19]. Informaation tulee olla siinä muodossa, että informaatiota hyödyntävä johto pystyy ymmärtämään sitä sekä tekemään sen perusteella päätöksiä ja hallintatoimia joiden avulla informaatio pystytään muuttamaan toiminnaksi. Digiturvallisuuden arvomalli integroidaan näin osaksi päätöksentekoprosessia ja hyvää hallintotapaa.

On hyvä huomioida, että digitaalinen turvallisuus ja siihen liittyvä riskien hallinta voi toimia myös joidenkin strategisten valintojen mahdollistajana. Ilman hyvää digitaalista turvallisuutta muu kehittäminen voi vaarantua. Tietyt organisaation kehityshankkeet tai suunnanvalinnat, esim. digitaalisen kehityksen saralla, vaativat että digitaalisen turvallisuuden valmiudet ovat tarpeeksi hyvällä tasolla. Esimerkiksi automaatio, datan hallinta, ulkoistukset, pilvipalvelut yms. vaativat asianmukaista digitaalisen turvallisuuden riskien käsittelyä. Tulevien tarpeiden riskien tarkastelu on usein yhteydessä tulevaisuuden ennakointityöhön ja organisaation strategityöhön.

[19] *NCSC: Questions for the board to ask about cyber security* (https://www.ncsc.gov.uk/files/NCSC_Board-Toolkit-Questions-for-Boards.pdf)

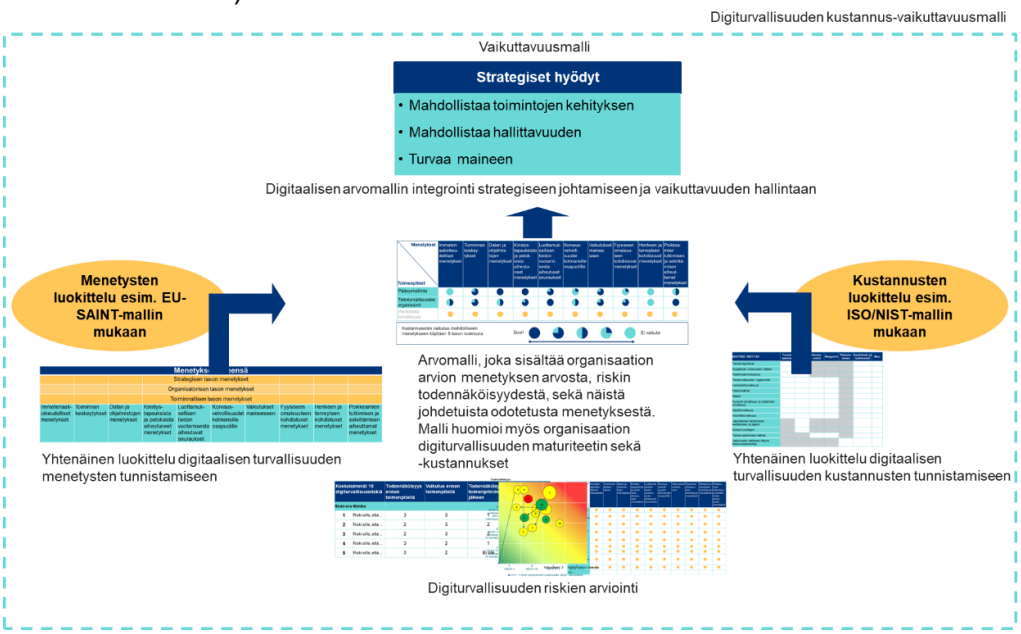
8 Digiturvallisuuden kustannus-vaikuttavuusmallin merkitys

Digitaalisen turvallisuuden kustannus- ja vaikuttavuus -mallin tarkoituksena on tarjota toimintatavat, joiden avulla organisaatiot voivat systemaattisesti arvioida suojattavia kohteita ja niihin liittyviä riskejä sekä kvantifioida toimenpiteitä (investointeja) joilla riskejä pyritään hallinnoimaan ja pienentämään. Mallien tavoitteena on mahdollistaa digitaalisen turvallisuuden vaikuttavuuden ja kustannusten näkyväksi tekeminen sekä varmentaa että toimenpiteet kohdistetaan oikeisiin kohteisiin.

Digiturvallisuuden kustannus-vaikuttavuusmalli pyrkii edesauttamaan ymmärrystä digitaaliseen turvallisuuteen tehtävistä panostuksista ja niiden tuottamista hyödyistä eli niiden vaikutuksista digitaalisen turvallisuuden uhkien pienemiseen. Mallin integraatio organisaation strategiseen johtamiseen, riskienhallintaan ja hallintamalliin auttaa kasvattamaan ymmärrystä digitaalisesta turvallisuudesta ja kytkee toiminnallisen ja organisaatiollisen tason digiturvallisuuden kehittämisen osaksi kokonaisriskienhallintaa.

Tämä kokonaisvaltainen digitaalisen turvallisuuden tunnistaminen, ymmärtäminen ja systemaattinen hallinta ja kehittäminen mahdollistaa sen, että organisaatioiden digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla oleva. Yhteenvetona voidaan siis sanoa, että digitaalisen turvallisuuden kustannus-vaikuttavuusmalli ja sen mahdollistavat hyödyt perustuvat kokonaisuuteen, jossa organisaatio osaa riskin arvioinnin ja hallintatoimen rahallisen arvon laskemisen lisäksi:

- tunnistaa ja digitaalisen turvallisuuden uhat ja näihin yhdistettävät menetykset (”Menetysluokittelu”)
- tunnistaa ja seurata digitaaliseen turvallisuuteen liittyviä kuluja ja kustannuksia (”Kustannusluokittelu”)
- määritellä arvon uhkaan liittyvälle menetykselle sekä riskin uhan toteutumisesta (”Arvomalli”)
- integroida edellä mainitut mallit osaksi organisaation strategista johtamista ja hallintomallia ja täten mahdollistaa digiturvallisuuden strateginen vaikuttavuus (”Vaikuttavuusmalli”)



Kuva 20: Digitaalisen turvallisuuden kustannus-vaikuttavuusmalli ja sen osaset yhteen koottuna

Termistöä

Alla on kuvattuna tässä raportissa käytetyt keskeiset termit. Digiturvallisuuden riskienhallinnan käsitteiden ylläpidetty sanasto on VAHTI-riskienhallintasanasto osoitteesta: http://uri.suomi.fi/terminology/digiriski/

Arvo: Arvo on tässä kontekstissa omaisuuden, tavaran tai palvelun rahallinen, aineellinen tai arvioitu arvo (kts. myös suojattava arvo)

Digitaalinen turvallisuus: tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa ja toiminta sekä siellä että siihen liittyen on turvallista ja hallittua, myös häiriötilanteissa

Digitaalisen toiminnan riski: digitaalisessa toimintaympäristössä vaikuttava, digitaali-seen toimintaympäristöön kohdistuva tai siitä johtuva riski

Kulu: Kulu on vastaanotetun tuotannontekijän hankintamenosta tilikaudelle jaksotettu osa (Lähde: www.tilisanomat.fi)

Kustannus: Kustannuksella tarkoitetaan tuotannontekijän rahassa mitattua käyttöä tai kulutusta. (Lähde: www.tilisanomat.fi)

Jäännösriski: riskin käsittelyn jälkeen jäljellä oleva riski

Menetys: Menetys on tässä kontekstissa arvon (kts yllä) menetys

Riski: Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.

Riskienhallinta tarkoittaa koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Se on systemaattista ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan riskejä.

Riskienhallintapolitiikka: organisaatiokohtainen kuvaus riskienhallintaperiaatteista ja keskeisinä pidetyistä riskienhallinnan puitteista

Riskienhallintaprosessi on menettely riskien arviointiin (tunnistamiseen, analysointiin, merkityksen arviointiin), käsittelyyn, seurantaan ja viestintään

Riskien arviointi: riskien toteutumisen todennäköisyyden ja niiden mahdollisten vaikutusten selvittäminen

Riskienhallinnan läpinäkyvyys: riskienhallinnan arvioinnin mahdollistaminen sidosryhmille ja sisäisille toimijoille siten, että siihen liittyvät tiedot välitetään niiltä osin, kuin tietojen välittäminen ei itsessään tuota merkittäviä riskejä

Riskien luokittelu: riskien tehokasta arviointia ja käsittelyä varten tehtävät ryhmittelyt, joiden ansiosta samankaltaisia tai samaan vastuualueeseen kuuluvia riskejä tai niiden osia voidaan tarkastella yhtenä kokonaisuutena

Strateginen taso: organisaation päätöksenteon taso, jolla tehdään toimintaympäristöön ja toiminnan rahoittamiseen liittyvät, koko organisaation toimintaa ja kehittämistä koskevat päätökset

Suojattava arvo: Suojattavalla arvolla tarkoitetaan tässä dokumentissa sekä konkreettisia järjestelmiä, joilla nähdään rahallista arvoa, arvoa, joka sisältyy tietoon ja sen käyttöön, että laajempia yhteiskunnallisia tai perusarvoja. Nykyaikaisessa ja kompleksisessa maailmassa on huomioitava, että riskit voivat kohdistua useille eri tasoille. Tämä laajentaa niin sanotun suojattavan kohteen määritelmää, sillä esimerkiksi yksittäinen tietovarasto voi olla merkityksetön sen rinnalla, miten varmistetaan palvelukokonaisuuden jatkuvuus, tai miten se ja muut digitaalisen toimintaympäristön sosioteknisen järjestelmän osaset vaikuttavat mm. ”luottamuksen” muodostumiseen. Strategiset tavoitteet voidaan usein muotoilla laajemmiksi suojattaviksi arvoiksi.

Toiminnallinen taso: organisaation päätöksenteon taso, jolla strategisen tason ja koordinointitason päätökset huomioiden tehdään toteutusta ja toimeenpanoa koskevat päätökset

Uhka: mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku