
# Liiketoiminnan hyötyjen huomiointi tietoturvallisuuden hallinnollisessa toteuttamisessa

Oulun Yliopisto
Tietojenkäsittelytieteiden laitos
Kandidaatintyö
Karri Maijanen
8.7.2015

# Tiivistelmä

Tutkimuksessa käydään läpi tietoturvallisuuden hallinnoinnin toteuttamista liiketoiminnan hyötyjen näkökulmasta. Tietoturvallisuuden toteuttamisessa on tärkeä ymmärtää liiketoiminnallisia hyötyjä, jotta siihen tehty investointi tukisi liiketoimintaa ja hyödyttäisi parhaiten liiketoiminnan arvon tuotantoa. Tutkimuksessa tehtiin kirjallisuustutkimus, missä tutkittiin tietoturvallisuuden hallinnolliseen toteuttamiseen vaikuttavia osa-alueita ja miten ne tulisi huomioida liiketoiminnan osana.

Kirjallisuustutkimuksen tuloksena löytyi useita alueita, joilla voidaan vaikuttaa tietoturvallisuuden tasoon organisaatiossa. Tutkimuksessa löydettiin liiketoimintaetuja tietoturvallisuuden nostamisesta strategiselle tasolle. Oikein toteutettuna tietoturvatoiminta tuo liiketoiminnalle runsaasti hyötyjä organisaation eri tasoille.

Ihmisen toiminnan vaikutus tietoturvallisuuden tasoon organisaatiossa on yhä merkittävin. Tämän vuoksi organisaation henkilöstöhallinnon tulisi ottaa suurempi rooli tietoturvallisuuden kehityksessä ja ylläpitämisessä. Tietoturvallisuuden hallinnoinnista on tullut osa yrityskulttuurin rakentamista ja se on näin lähentynyt johtamisen keinoin hallittavaa kokonaisuutta. Tietoturvallisuus on kasvanut liiketoiminnan estäjästä ajan saatossa sen mahdollistajaksi ja turvaajaksi. Liiketoiminnassa tietoturva on noussut kilpailutekijäksi ja osaksi tietointensiivisen yrityksen arkipäivää.

Tiedon turvaamisen keinoilla säilytetään liiketoiminnalle tärkeän tiedon arvo luomalla turvallinen tietojenkäsittely-ympäristö. Yrityksen päätöksenteon käytössä olevan tiedon arvostus kasvaa, mitä paremmin sen turvaominaisuuksia pystytään suojaamaan. Tietoturvallisuus on panostamista luotettavaan päätöksentekoon.

Tietoturvallisuuden keinoin voidaan helposti luoda näennäisesti tietoturvallinen ympäristö, mikä huonon käytettävyyden vuoksi huonontaa tietoturvan tasoa. Liiketoiminnalle on pystyttävä perustelemaan saavutettavien hyötyjen vaikutus liiketoiminnalle ja liiketoiminnan johdon on seurattava, sekä vaadittava hyötyjä kaikilta tietoturvallisuuden investoinneilta. Tämä yhteistyömalli tuo tietoturvallisuuden hyödyt myös johtoryhmän ulottuville ja näin tärkeä tieto on käytettävissä näin myös liiketoiminnan strategisessa suunnittelussa.

Liiketoiminnan hyödyt näkyvät toiminnallisissa, taktisissa, strategisissa ja organisatorisissa organisaation toiminnan osissa. Mitä paremmin tietoturvallisuus yrityksessä toteutetaan, sitä paremmat edellytykset yrityksellä on menestyä. Tämän vuoksi tietoturvallisuuden strateginen merkitys on liiketoiminnalle hyvin merkittävä.

## Avainsanat

tietoturvallisuus, tietoturvallisuuden liiketoiminnallinen hyödyntäminen, tietoturvallisuuden strateginen kilpailuetu, tietoturvallisuuden johtaminen, inhimilliset tekijät tietoturvallisuudessa

## Ohjaaja

Tutkijatohtori Mari Karjalainen

# Sisällysluettelo

Tiivistelmä ..... 2
Sisällysluettelo ..... 3
Käytetyt lyhenteet ja termit ..... 4
1. Johdanto ..... 6
2. Tietoturvallisuus organisaation tietojen turvaamisessa ..... 8
   2.1 Tietoturvallisuus muutoksessa ..... 9
   2.2 Tiedon turvaominaisuudet ..... 11
   2.3 Tiedon turvaaminen organisaatiossa ..... 13
3. Tietoturvallisuuden hallinta tietoturvallisuuden ylläpitämisessä ..... 15
   3.1 Sosiaalisten tekijöiden vaikutus tietoturvallisuuden hallintaan ..... 16
   3.2 Riskien hallinta ..... 19
      3.2.1 Liiketoimintaan liittyvät tekijät riskianalyysissä ..... 23
   3.3 Tietoturvallisuuden hallinnan formalisointi ..... 24
4. Strategisen tietoturvallisuusjohtamisen hyötynäkökulma ..... 28
5. Pohdinta ..... 31
   5.1 Tietoturvallisuus organisaatiossa ..... 31
   5.2 Tiedon turvaominaisuudet ja tiedon arvo ..... 32
   5.3 Inhimilliset tekijät tietoturvallisuudessa ..... 34
   5.4 Riskien hallinta ..... 35
   5.5 Tietoturvallisuuden hallinnan formalisointi ..... 35
   5.6 Strateginen tietoturvallisuusjohtaminen ..... 38
6. Johtopäätökset ..... 39
7. Lähteet ..... 40

# Käytetyt lyhenteet ja termit

Seuraavat lyhenteet ja termit on koottu VAHTI ohjeistuksesta ja niitä on käytetty työssä yleisen selkeyden vuoksi (*Valtionhallinnon tietoturvasanasto*2008).

| **Englanninkielinen lyhenne** | **Englanninkielinen termi** | **Suomenkielinen termi, sekä lyhyt selite** |
|---|---|---|
| ISMS | Information Security Management System | *”Tietoturvallisuuden johtamis- ja hallintajärjestelmä”*, järjestelmä millä toteutetaan määritelty tietoturvataso kohdeorganisaatioon.<br><br>*"osa yleistä toimintajärjestelmää, joka luodaan ja toteutetaan toimintariskien arviointiin perustuen ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus.*<br><br>*Sisältää organisaatiorakenteen, politiikat, suunnittelu- ja kehittämistoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit, mittarit ja resurssit."* |
| IA | Information Assurance | *Tiedon turvaaminen* on kokoelma menettelyitä, joilla pyritään säilyttämään tiedon turvaominaisuudet.<br><br>*”tietoturvallisuuteen tähtäävä toiminta”* |
| | (protected) asset | *”turvattava kohde”*<br><br>*"turvattava kohde on organisaatiolle arvokas kohde, kuten ihmiset, resurssit, toiminta ja palvelut*<br><br>*Tiedon käsittelyn osalta turvattavia kohteita voivat olla esimerkiksi tiedot (eri muodoissaan), inhimilliset resurssit, tietojärjestelmät, käyttöympäristö, fyysinen ympäristö, ulkoiset palvelut, hankinnat, edellä mainittuja palvelevat prosessit."* |
| IS policy | Information security policy | *”Tietoturvapolitiikka”* on kokonaisdokumentaatio tietoturvallisuuden hallinnoimiseksi organisaatiossa. Se jaetaan tavoitteiden mukaisesti eri osiin, jotta se olisi helpommin käytettävissä tietoa tarvitsevilla tahoilla.<br><br>*"1) valtakunnan tasolla tietoturvanormien ja niiden täytäntöönpanon muodostama kokonaisuus*<br><br>*2) organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta* |

| | | |
|---|---|---|
| | | *Voidaan puhua myös tietoturvaperiaatteista. Tietoturvapolitiikka ja -strategia ovat osa organisaation toiminta- ja tietohallintopolitiikkaa ja -strategiaa."* |
| | threat | *"haitallinen tapahtuma, joka voi mahdollisesti toteutua, tai useampi mahdollinen häiriö, joka tapahtuessaan voi aiheuttaa sen että tiedoille, muulle omaisuudelle tai toiminnalle tapahtuu ei-toivottua "* |
| | risk | *"1) todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon*<br><br>*2) uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo (= arvo x todennäköisyys)*<br><br>*Riski voi olla myös mahdollisuus menettää päämääräksi asetettu seikka."* |
| | vulnerability | *"tietojärjestelmän tai sen osan heikkous, joka vaarantaa tietoturvan*<br><br>*Haavoittuvuus voi olla seurausta ohjelmavirheestä tai siitä, että jotakin erityistapausta ei ole otettu huomioon. Haittaohjelmat hyödyntävät levitessään tietoturvahaavoittuvuuksia."* |

# 1. Johdanto

Koska tietoa pidetään nykyaikaisten organisaatioiden tärkeimpänä varantona (de Oliveira Albuquerque, García Villalba, Sandoval Orozco, Buiati, & Kim, 2014), tietoturva kuuluu olennaisena osana tekniikan kehitykseen. Koko yhteiskunnan ollessa yhä enemmän riippuvainen tiedosta, tulee tietoturvallisuuden rooli yrityksien tärkeänä toimintona ymmärtää organisaation kaikilla tasoilla. Organisaation johdon tulee osata hyödyntää tietoturvallisuuden tuomia hyötyjä liiketoiminnassa ja varmistaa sen riittävä taso liiketoimintaetujen näkökulmasta. Liiketoiminnan tulee pitää huoli siitä, että tietoturvaan investoiminen tuottaa haluttua tulosta liiketoiminnassa. Tämän yhteyden muodostaminen tietoturvallisuudesta nähdään usein organisaatioissa haasteelliseksi. Tästä syystä tietoturvallisuus jätetään organisaatioissa helposti tukifunktioksi, vaikka se voitaisiin valjastaa osaksi yrityksen strategista menestystä liiketoiminnan turvaajana ja uuden liiketoiminnan mahdollistajana. Tietoturvallisuuden toteutuksen jäädessä liiketoiminnan strategian ulkopuolelle, siitä muodostuu tukitoimintojen uusi kuluerä, minkä arvo liiketoiminnalle tällöin helposti hukataan. Tämä voi johtaa riittämättömien resurssien käyttöön, sekä suuriin rahallisiin menetyksiin, kun tietoturvallisuuden taso laskee riittämättömän alhaiseksi (S. H. Von Solms, 2005).

Strategisen tietoturvallisuusjohtamisen tärkeys kasvaa tietointensiivisissä organisaatioissa (Sipior & Ward, 2008). Tämä on olennaista huomioida, kun tietoturvallisuuden kriteeristöjen vaatimuksia toteutetaan organisaatioiden tietovarantojen suojaamisessa. Tietoturvallisuuden lähestymistapa suojauskeinoihin tulisikin olla kokonaisvaltainen läpi koko organisaation kaikkien toimintojen keskittyen liiketoimintojen varantoihin.

Tämä työ on kirjallisuuskatsaus, jossa tarkastellaan strategista tietoturvallisuuden johtamista ja siihen liittyviä taustatekijöitä organisaatioissa. Tarkoituksena on ymmärtää sitä, miten strateginen tietoturvallisuuden johtaminen tulisi toteuttaa organisaatioon maksimoiden samalla myös liiketoiminnan hyödyt. Tietoturvan peruskäsitteiden ja tietoturvallisuuden johtamisen määrittelyn kautta siirrytään tarkastelemaan tietoturvallisuuden strategista toteuttamista.

Tutkimuksen ytimessä on halu ymmärtää tietoturvallisuuden ja liiketoiminnan yhtymäkohtia, sekä määritellä niiden synergiaetuja. Tutkimuksessa tarkastellaan hallinnollisten tietoturvavaatimusten toteuttamista osaksi yrityksen liiketoimintaprosesseja. Tietoturvallisuuden hallinta tulisi toteuttaa osana tietoturvallisuuden ja liiketoiminnan prosesseja, jotta yritys aidosti täyttäisi tietoturvallisuuden kriteeristöjen vaatimukset ja maksimoisi samalla tehdyn tietoturvatyön hyödyt liiketoiminnassaan. Tietoturva on parhaimmillaan tukemassa liiketoimintaa aina strategiasta asti kattaen kaikki toiminnot koko organisaatiossa. Oikein toteutettuna sillä parannetaan työntekijöiden tehokkuutta ja yrityksen mahdollisuuksia levittäytyä uusille markkina-alueille, sekä liiketoimintamuotoihin (Ezingeard, McFadzean, & Birchall, 2005).

Työssä käsitellään myös miten tietoturvallisuus voidaan upottaa liiketoimintaan osaksi yrityksen kulttuuria, hallinnollisia menettelytapoja, sekä osaksi hyväksyttävää työskentelytapaa organisaation alimmillakin tasoilla. Työssä kuitenkin rajataan esitetyt toimintatavat vain hallinnollisen toteutuksen osalle.

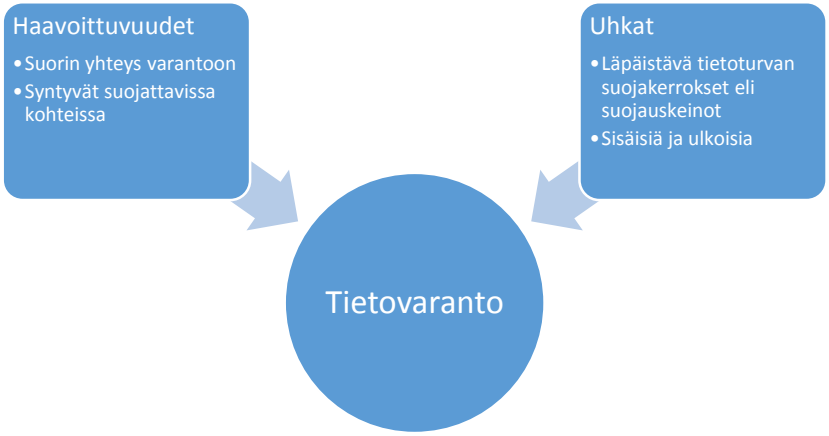
Kirjallisuustutkimuksen perusteella havaittiin, että Suomen kansallista auditointikriteeristöä KaTaKria ei ole tutkittu monipuolisesti tieteellisesti. Sen sijaan

ISO27000–sarjasta löytyi runsaasti aikaisempia tutkimuksia. Yksittäisten kriteeristöjen totetustapoihin tai eroavaisuuksiin ei tutkimuksessa kiinnitetä huomiota, vaan pyritään poimimaan liiketoiminnan ja tietoturvallisuuden välisen yhteyden muodostamiseen tarvittavia tiedon palasia.

Työ toteutetaan kirjallisuustutkimuksena, jota sovelletaan tapojen ja ongelmien etsimisessä tietoturvallisuuden hallinnollisessa toteuttamisessa. Kandidaatin työn tutkimusmetodina on kirjallisuustutkimus.

# 2. Tietoturvallisuus organisaation tietojen turvaamisessa

Tietoturvallisuudessa huomioidaan kaikki liiketoimintojen hyödyntämät varannot. Nämä voidaan yleisellä tasolla jakaa ihmisiin, prosesseihin ja teknologiaan. Useilla sisäkkäisillä suojakerroksilla pyritään suojaamaan näitä organisaation toiminnalle tärkeitä asioita. Panostukset uloimpiin kerroksiin vähentävät painetta sisempien kerroksien suojaustasolle. Jakamalla suojauksen painotuksen tasaisesti, kullekin suojauskerrokselle, saavutetaan suojaustaso, missä yksittäisten asioiden käytettävyyttä ei liiaksi heikennetä. Tietoturva onkin usein mielletty käytettävyyden ja turvallisuuden väliseksi kamppailuksi. Tietoturvan jakaminen useampiin kerroksiin usein myös tukee toisiaan osittain päällekkäisillä suojauskeinoilla. Tällöin yhden suojauksen pettäminen ei heti vaaranna varannon tietoturvallisuutta.




***Kuva 1*** *Haavoittuvuus ja uhka suhteessa tietovarantoon*

Kuva 1 ilmentää tietovarantoa kohtaan suuntautuvat haavoittuvuuden ja uhkat. Vaikutussuhde haavoittuvuuksien osalta on suorempi uhkiin verrattuna. Uhkien on läpäistävä kaikki suojauskerrokset ennen kuin ne saavuttavat tietovarannon. Eri uhkilla on eri määrä suojauskeinoja läpäistävänä. Suojauskeinojen määrä riippuu suojausrakenteen toteutuksesta ja eri tasojen kyvystä suojata tietovarantoa uhkaa vastaan. Haavoittuvuuksien osalta tilanne on toinen, sillä haavoittuvuudet ovat osa tietovarannon toiminnallisuutta. Tietovarantoa uhkaavat haavoittuvuudet kuitenkin ovat usein suojauskeinojen vuoksi turvassa hyväksikäytöltä.

Tietoturvan fokus on ajan saatossa siirtynyt tekniikan soveltamisesta kohti ihmisiä ja heidän toimintaansa liittyvien riskien hallintaan. Ihmisiin liittyvää riskien hallintaa tuetaan organisaatiossa hallinnollisella ohjauksella. Ihmisiin ja heidän toimintaansa liittyvien riskien hallinnasta onkin tullut suurin tietoturvaongelmien pelikenttä. Organisaation hallinnan ja tietoturvan on yhdistänyt tietoturvakulttuurin johtaminen, mikä on tullut yrityskulttuurin rinnalle tärkeäksi tietoturvan edistäjäksi (Eloff & von Solms, 2000). (Da Veiga & Eloff, 2007)

Tietoturvallisuuden käsitteiden ymmärtäminen vaatii tietoturvallisuuden kehityksen pikaista tarkastelua. Historian kautta nähdään tietoturvallisuuden pelikentän laajentuminen, sekä ymmärretään paremmin kehityksen nopea vauhti ja sen synnyttämät

ongelmat. Tekniikka kehittyy ja uusien innovaatioiden mukana tietoturvan osa-alueet paisuvat entisestään. Näistä syistä kehityksen mukana pysyminen on vaikeaa. (Dlamini, Eloff, & Eloff, 2009)

Tietoturvan kehityksen ymmärtäminen selkeyttää tietoturvallisuuden perusteiden kokonaisuuden hahmottamista. Tiedon turvallisuusominaisuudet ovat osakokonaisuus, jolla tietoturvallisuuden pienimpiä osasia pystytään kuvaamaan. Yhdistämällä tiedon turvaominaisuuksia pääsemme tiedon turvaamiseen, mikä on jo lähempänä organisaation toiminnan turvaamista. Tiedon turvaamisessa itse tiedon oikeellisuuden käsite on tärkeä liiketoimintaprosesseissa, jossa tuotetaan arvoa käytettävissä olevasta tiedosta. Tiedon turvaominaisuuksien ja samalla tietoturvan merkitys kasvaa mitä tietointensiivisempi organisaatio on (Herath & Rao, 2009).

Ihmisen vaikutus organisaation tietoturvatasoon kasvaa edelleen. Vaikuttamalla ihmisten asenteisiin tietoturvaa kohtaan ja käyttäytymiseen vaikutetaan tehokkaimmin tietoturvallisuuden tasoon. Asenteilla saavutetaan hyväksyntää ja tuetaan tietoturvallisten toimintatapojen toteutumista organisaation toimijoissa. Tekniikan avulla ei saavuteta yhtä hyviä tuloksia, vaan sen käyttö tietoturvallisuudessa on lähinnä ohjaavaa ja rajoittavaa. Tietoturvan hallinnoinnista on tullut osa yrityskulttuurin rakentamista ja siten sen ohjaus on siirtänyt painopistettään tekniikasta kohti ihmisten johtamista. Tietoturva tulee ottaa osaksi jokapäiväistä organisaation johtamista ja se tulee mieltää asioiden mahdollistajaksi. Liiketoimintastrategian tulee myös huomioida tietoturvallisuus osana toimintamallia, millä organisaatio toimii. Seuraavaksi kuvataan lyhyesti ajan myötä tapahtunutta tietoturvan kehitystä.

## 2.1 Tietoturvallisuus muutoksessa

Tietoturvallisuus on yhä osana suurta muutosta, missä sen uhkat ovat kasvaneet vuosien saatossa pienistä rikkeistä yrityksen sisällä aina suuria konserneja ja jopa valtioita tuhoaviin voimiin. Ennen tietoturvarikkeet miellettiin lähinnä harmiksi, mikä oli vain liiketoiminnan kiusana. Liiketoiminnalle kiusaa syntyi haittaohjelmista, jotka eivät toiminnallaan vaikuttaneet liiketoiminnan jatkuvuuteen kovinkaan voimakkaasti. Muutos vakavampiin tietoturvaongelmiin on kuitenkin jälkikäteen selkeämmin havaittavissa. Liiketoiminnan suurimpiin uhkakuviin tietoturva on päässyt vasta viime vuosikymmeninä, kun suuretkin yritykset ja valtion laitokset ovat joutuneet tietoturvahyökkäyksien kohteiksi. (Dlamini et al., 2009)

Tietoturva kasvoi yrityksissä ongelmaksi samalla, kun tieto tuli käsiteltäväksi henkilökohtaisiin työasemiin. Aikaisemmin konesalissa sijaitsevan keskustietokoneen järjestelmällä suojattu tieto oli nyt hajautettuna ympäri yritystä useisiin eri työasemiin. Tiedon kontrollointiin ja sen suojaamiseen tuli etsiä ratkaisuja, joita voitaisiin käyttää hajautetussa tiedonkäsittelymallissa. Tieto myös liikkui yrityksen sisäverkossa ja pian myös yrityksen ulkopuolellakin. (Dlamini et al., 2009)

Verkottuvan maailman mukana tulivat disketeillä ja verkoissa leviävät madot. 1990-luvulla yrityksissä oli sisäverkot ja jonkinlaiset yhteydet puhelinverkon kautta yrityksen sisäisiin palveluihin. Myös internet-yhteydet alkoivat yleistymään, koska sähköpostin käyttö yritysten välisessä kommunikoinnissa kasvoi. Tietoturvallisuuden vaikutusalue laajeni jo yrityksen ulkopuolellekin. Ulkoiset uhkat oli nyt huomioitava laajemmin. Haittaohjelmauhkien kasvaessa yritykset alkoivat investoimaan virustorjuntaohjelmistoihin. (Dlamini et al., 2009)

Internet toi mukanaan myös uusia tietoturvahaasteita. Matojen lisäksi sähköpostia käytettiin myös haittaohjelmien levitykseen. Sähköpostijärjestelmän käyttöönotolla mahdollistettiin tuntemattomalle taholle suora pääsy yrityksen työasemalle asti. Sähköposti toi mukanaan siis kasvavan uhkan työaseman tietoturvallisuuteen ja näin työasemakohtaiset virustorjuntaohjelmistot näkivätkin päivänvalon. Myös verkon yhdyskäytävän turvaamiseen alettiin panostamaan, koska uhkat tulivat usein verkkojen välisestä liikenteestä. Omat palvelimet sisäverkon ja internetin välissä (DMZ) tuli suojata erillisillä palomuurilaitteilla, jotka toteuttivat liikenteen rajoitukset. (Dlamini et al., 2009)

Siirryttäessä 2000-luvulle haittaohjelmien tekijöiden motiivit muuttuivat. Oli saavutettu tietokoneiden levinneisyyden avustuksella taso, missä haittaohjelmien tekemisellä pystyi nyt tienaamaan. Enää haittaohjelmien tekijät eivät pyrkineet vain esittelemään taitojaan, vaan he pyrkivät tekemään rahaa tällä kyseenalaisella osaamisellaan. Tietotekniikka tuli tuottavuuden tehostamisen ohjaamana myös osaksi lähes kaikkien yritysten toimintaa. Valtion laitokset myös alkoivat siirtää palveluitaan verkkoon. IT-laitteiden yleistyminen toi laitteet ja internet -yhteydet myös useampiin koteihin. Yritysten tietotekninen suojavyöhyke laajeni näin myös osaltaan kattamaan kodissakin tapahtuvaa tietojen käsittelyä. (Dlamini et al., 2009)

Kotikäyttäjätkin oli huomioitava, koska kotona tietokonetta ja julkisia palveluita käytettiin kuten työpaikallakin. Lopulta kyberturvallisuuden käsitteen nosti esiin valtion laitoksien palveluiden siirtyminen internetiin. Kyberturvallisuus nähdään keskeisenä yhteiskunnallisena asiana, jolloin tietoturvallisuuden tärkeys tunnistetaan sekä henkilökohtaisella tasolla että, yritys-, kunta- ja valtiotason näkökulmista (Sharma & Sefchek, 2007). Yhteiskunnan tietojärjestelmien liitettävyys toisiinsa mahdollistaa kokonaisprosessien sujuvamman toiminnan ja tuo säästöjä yhteen liitettyjen toimintojen omistajille. Yksittäisten osien suojaamisesta siirryttiin yhteenliittymien ja yritysverkostojen suojaamiseen. (de Oliveira Albuquerque et al., 2014)

Valtion kriittinen infrastruktuuri nojaa verkkojen yhteenliittymiin, joiden kautta yhteiskunnan eri toimijat pääsevät käyttämään yhteiskunnalle tärkeitä palveluita. Kyberturvallisuuden parantamisella pyritään tukemaan valtion toimintaedellytyksiä verkottuneessa yhteiskunnassa siten, että ongelmatilanteita ei tulisi tai niistä pystyttäisiin selviytymään. Yhteyksien vaarantuminen vaarantaa samalla myös valtion toimintaa. Kaikki verkkoon liitettyjen kriittisten toimijoiden tulee huolehtia kaikkien prosessien ja ohjelmistojen turvaamisesta, jotta kyberturvallisuus pystytään kokonaisuudessaan varmistamaan. Kyberturvallisuus ei siis ole vain yhden osapuolen, kuten valtion toteutettavissa. (Rantapelkonen & Salminen, 2013)

Tietoturvallisuuden kenttä on siis ajan saatossa laajentunut yksittäisten keskustietokoneiden suojaamisesta internetin ja yhteiskunnan kautta kasvavien uhkien torjumiseksi. Laajentuminen on ollut mahdollista verkottumisen, sekä tietokoneiden ja yhteyksien käytön kasvun avustuksella. Kyberturvallisuus on laajuudessaan yhdistänyt kaikki verkkoihin liittyneet toimijat ja mahdollistanut näiden vaikutusmahdollisuudet toisiinsa. Ongelmakentän kasvaminen tuo haasteita tietoturvan näkökulmasta, mutta se avaa myös uusia mahdollisuuksia liiketoiminnalle. Ymmärtämällä kyberturvallisuuden mahdollisuudet voi valjastaa resursseja käyttöönsä ajasta ja paikasta riippumatta. Tähän on kuitenkin varauduttava rakentamalla suojarakenteet kaikkien varantojen suojaamiseksi tässä toimintaympäristössä. (de Oliveira Albuquerque et al., 2014)

Tietoturvallisuuden strategisessa johtamisessa on huomioitava historiasta johdettava tietoturvallisuuden yhä laajeneva pelikenttä. Tekniikan kehitys vie tietoturvallisuuden hallinnointia eteenpäin kiihtyvällä vauhdilla ja tämä on huomioitava

liiketoimintastrategiassa. Liiketoiminnan muutoksissa tulee hyödyntää hyvin toteutetun tietoturvallisuuden synnyttämiä mahdollisuuksia tehdä kannattavaa liiketoimintaa alueilla joissa huonosti hoidetulla tietoturvallisuudella toimiminen olisi katastrofaalista. Näin voidaan tukea liiketoimintaa käyttäen tietoturvalla saavutettua kilpailuetua. Seuraavaksi tarkastellaan tietoturvallisuuden pienimpiä perusyksiköitä: tiedon turvaominaisuuksia, joiden avulla pyritään hahmottamaan suojaustarpeet suojauskohteille.

## 2.2 Tiedon turvaominaisuudet

Tiedon ominaisuuksia käytetään määrittelemään tiedon laatua suhteessa sen turvallisuusominaisuuksiin. Tiedolla on myös erilaisia suojattavia tarpeita sen elinkaaren eri vaiheissa. Tiedon turvallisuusominaisuuksien suojaustarpeet säilyvät kuitenkin koko tiedon elinkaaren ajan muuttumattomina. Tiedon turvaominaisuuksien määrittelyssä on käytössä korkean tason lajittelu, missä sen on tuettava tiedon arvon säilymistä. Tiedon arvon säilyttämisellä on yleensä sen omistajalle jokin merkitys. Tätä arvoa tuetaan tietoturvallisuuden suojauskeinoilla. (Ezingeard et al., 2005)

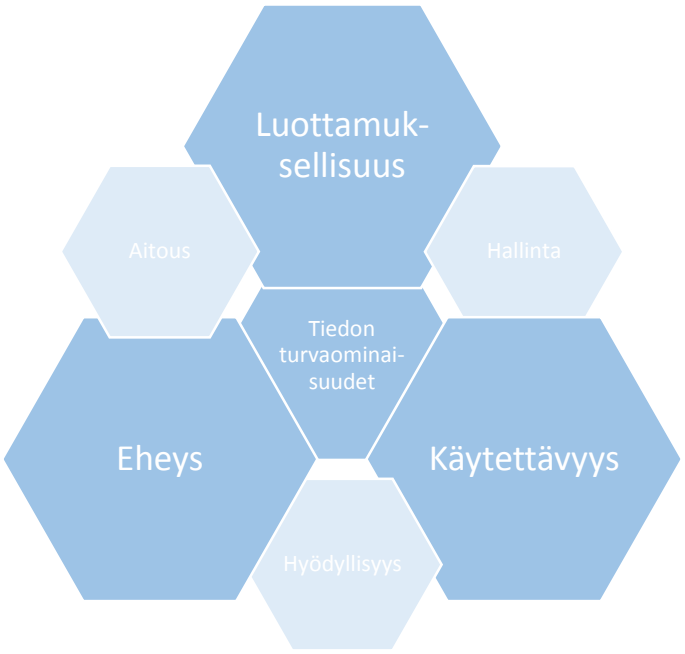
Merkitykselliseksi tiedon turvaominaisuuksien säilyminen tulee silloin, kun tietoa ollaan käyttämässä. Jos tietoon ei voida jostain syystä luottaa, sen arvo on vähäinen. Tällöin sitä ei voida käyttää hyödyksi ja investoinnit sen suojaamiseksi ovat olleet turhia. Liiketoiminnassa arvokasta tietoa käytetään päätöstentekoon. Päätösten tekemisessä käytettävän tiedon tulee olla luotettavaa, jotta päätöksistä tulisi hyviä. Hyvillä päätöksillä pyritään ohjaamaan yrityksen toimintaa arvoa tuottavaan suuntaan. Tieto menettää myös arvoansa, jos siihen ei voida luottaa. Tiedon turvaamiseen käytetään yrityksissä resursseja ja rahaa. Tämä on siis yritysmaailmassa sijoitus yrityksen tietopääoman turvaamiseksi, millä tuetaan yrityksen arvotuotantoa. (Ezingeard et al., 2005)

Tiedolla nähdään yleisesti olevan kolme ominaisuutta, jotka luovat tietoturvallisuuden kolminaisuuden. Tiedon *luottamuksellisuuden* merkitys pohjautuu rajoituksiin tietoon pääsyssä (Reid & Gilbert, 2010). Tiedon omistaja määrittelee tiedon käytön rajoitukset. Luottamuksellinen tieto on käytettävissä vain niillä, jotka tarvitsevat sitä sen omistajan määrityksen mukaan. Tarpeet tiedon käsittelylle voivat tulla työtehtävien tai henkilön roolin kautta. Luottamuksellisuuden käsitteen rikkoutuminen tarkoittaa tiedon joutumista sen omistajan määrittelemän tietoa käsittelevän käyttäjäryhmän ulkopuolelle. Luottamuksellisuuden tärkeys korostuu yritystoiminnassa liiketoimintaan liittyvän arkaluonteisen tiedon käsittelyssä. Käsittely-ympäristön tulee tarjota riittävät rajoitusmekanismit tietoon pääsylle, jotta luottamuksellisuuden käsite pystytään toteuttamaan, eikä suojattava tieto menetä silloin luottamuksellisuuden menetyksen kautta arvoaan.

Yleisesti tiedon liikkumisen aikana järjestelmästä tai verkosta toiseen pyritään suojaamaan se siten, että sitä ei voida muuttaa ilman muutoksen havaitsemista. *Eheydellä* tarkoitetaan tiedon pysymistä muuttumattomana, eli luotettavana (Reid & Gilbert, 2010). Muuttumisen havainnointi tai estäminen on suojauskeino esimerkiksi tietoverkoissa liikkuvalle tiedolle. Tiedosta lasketaan tarkistussumma, mikä tallennetaan salatun liikenteen sisälle. Näin mahdollinen tiedon muuttuminen havaitaan sitä vastaanotettaessa.

Tiedon *saatavuuden* näkökulmalla tarkastellaan tiedon käytettävyyden ominaisuutta. Tieto on käytettävissä niillä, jotka sitä tarvitsevat ja silloin kun sitä tarvitaan (Reid & Gilbert, 2010). Tietoon käsiksi pääseminen on näkökulma ominaisuudesta missä tieto on sitä tarvitsevien käytettävissä oikeaan aikaan.

Yhdessä nämä kolme tiedon ominaisuutta luovat tietotuvallisuuden kolminaisuuden. Tiedon kolmen pääominaisuuden lisäksi niiden rinnalle on otettu täydentäviä aliominaisuuksia. Esimerkiksi Parkerin (Parker, 1998) kuusikulmio kuvassa Kuva 2 on yksi yleisimmin käytetyistä turvaominaisuuksia täydentävistä malleista. Siinä tiedon turvaominaisuuksia on täydennetty lisäominaisuuksilla, joiden kautta saavutetaan kriittisten turvallisuusalueiden entistä kattavampi kuvaus. (Reid & Gilbert, 2010).




***Kuva 2*** *Tiedon turvaominaisuudet, Parkerin kuusikulmio (Parker, 1998; Reid & Gilbert, 2010)*

Tiedon hallintaominaisuudella pyritään kuvaamaan tiedon turvaominaisuutta, missä tiedon omistajuus määritellään. Tätä ominaisuutta käytetään mm. digitaalisen tiedon aineettomien oikeuksien määrityksessä, missä omistaja määrittelee tiedon käytölle tai kopioimiselle säännöt. Hyödyllisyyden näkökulmassa tietoa pystytään käyttämään, eli se on käytettävässä muodossa. Ominaisuus on siis käytettävyyden aliominaisuus, missä tieto on saatavilla ja samaan aikaan myös hyödynnettävissä. Hyödynnettävyys korostuu esimerkiksi salausavaimen tallessa pitämisessä. Ilman avainta tieto on saatavilla, mutta ei hyödynnettävissä. Aitouden osalta tiedolle tuodaan jäljitettävyyden ominaisuus. Ominaisuuden avulla pystytään määrittämään oikea tiedon omistaja. (Reid & Gilbert, 2010)

Parkerin (Parker, 1998) kuusikolmion lisäksi tiedon turvaominaisuuksia ovat myös kiistämättömyys ja yksityisyys. Kiistämättömyydellä vahvistetaan tapahtuma siten, että kumpikaan osapuoli ei voi kieltää tehneensä tapahtumaa. Tapahtumasta on kiistämätön todistus, jonka yleensä tapahtuman omistaja tallentaa. Yksityisyydellä estetään tiedolle sen tekijän henkilöllisyyden paljastuminen. (Reid & Gilbert, 2010)

Tiedon turvaominaisuuksia suojataan käyttötarpeeseen suunnitelluilla turvakontrolleilla. Turvakontrollien käytöllä pyritään säilyttämään tiedon turvaominaisuudet koko tiedon elinkaaren ajan. Tiedon omistajataho määrittelee suojattavan tiedon, käytettävissä olevat resurssit, sekä käytännöt tiedon suojaamiselle. Tätä toimintaa kutsutaan tietoturvallisuuden hallinnaksi.

Tiedon turvaominaisuudet tulee säilyttää yrityksen liiketoiminnalle tärkeiden tietojen osalta. Turvaominaisuuksien tärkeys korostuu, jos tiedot ovat liiketoimintastrategialle tärkeitä. Tällöin tiedon arvon säilyttäminen on toteutettava erityisellä huolellisuudella, jottei liiketoiminta kärsisi huonoarvoisen tiedon käytön synnyttämistä ongelmista. Tiedon turvaominaisuuksien varmistamisella pyritään luomaan luotettava ympäristö tietojenkäsittelylle. Turvallinen ja tiedon arvon säilyttävä tietojenkäsittely-ympäristö on strategisen tietoturvallisuuden ydintoimintoja, mihin koko yrityksen liiketoiminnan on nojauduttava. Seuraavassa kappaleessa kuvataan, miten tiedon arvo pyritään säilyttämään organisaatiossa tiedon turvaamisen keinoin.

## 2.3 Tiedon turvaaminen organisaatiossa

Tiedon turvaaminen on englanninkielestä sanoista *"information assurance"* johdettu sanapari. Termi käsittää tiedon eli yksittäisen merkityksellisen asian varmistamista, tai oikeastaan sen turvaominaisuuksien varmistamisen, sekä sen varmistamiseen käytetyt tietoturvallisuudesta tutut menettelyt. Parhaimmillaan tämä tiedon turvaamistoiminto mahdollistaa luotettavan päätöksenteon, asiakkaan luottamuksen, liiketoiminnan jatkuvuuden ja hyvän hallintatavan (Ezingeard et al., 2005). Liiketoiminta pohjautuu päätösten tekemiseen, ja hyvän päätöksen tekeminen tarvitsee luotettavaa tietoa. Tiedon turvaamisella pyritään toteuttamaan sellainen liiketoimintaa tukeva järjestelmä, missä tiedon turvaominaisuuksista huolehditaan ja luodaan näin luotettava pohja liiketoiminnalle. (Ezingeard et al., 2005)

Tiedon turvaaminen on luottamuksen luontia organisaation tiedon luotettavuudesta, turvallisuudesta, yksityisyydestä ja virheettömyydestä. Tiedon turvaaminen pitää sisällään laajan toimintojen kokonaisuuden turvallisuuden hallinnoinnista aina riskien ja liiketoimintojen jatkuvuuden hallintaan (Ezingeard et al., 2005). Tiedon turvaaminen on siis helpommin ymmärrettävissä ja selvitettävissä yrityksen johdolle, kuin pelkästään tietoturvallisuus ja sen käsitteet. Tiedon turvaamisessa siis ollaan lähempänä johdon ymmärtämää termistöä ja käsitteitä. Tiedon turvaamisessa tietoturva on käsitettävä käytettävänä keinona taustalla ja tiedon turvaaminen on arvonäkökulmalla täydennetty tiedon turvaominaisuuksien puolustusjärjestelmä. Logiikkaa on helpompi havainnollistaa ääriesimerkeillä, missä tuotetaan haluttu täydellinen seurannan tulos mutta ilman bisneksen tuomaa arvoajattelua. Kun suojaukset toteutetaan ilman arvoon liittyvää analysointia, menetetään yhteys siihen liittyvään liiketoimintaan. Tiedon turvaamisen linkittyminen liiketoiminnan johtamiseen helpottuu yksinkertaistamisen ja äärimmäisyyksien kautta. Näin tietoturvallisuuden asiantuntijat pääsevät keskustelemaan samalle kielelliselle tasolle yrityksen johtajien kanssa. (Ezingeard et al., 2005)

Tiedolle voidaan määrittää sen tarvitsemat turvallisuusominaisuudet, kun tiedetään sen käyttötarve. Tiedon turvallisuusominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys. Näiden näkökulmien kautta tarkasteltuna tiedolle syntyy suojattavia tarpeita sen eri konteksteissa. Aikaisemmin kuvattu tiedon turvaaminen voidaan ottaa kuvaamaan tätä suojaustoimintaa kokonaisuudessaan. (Ezingeard et al., 2005)

Tietoturvallisuuden pyrkimyksenä tulee olla mahdollistaminen estämisen sijaan. Mahdollistavan lähestymistavan kautta saadaan positiivista vastetta muutoksille ja mahdollistetaan suurtenkin muutosten toteuttaminen. Samalla vähennetään muutosvastarintaa ja nostetaan työtehokkuutta. Mahdollistava lähestymistapa myös luo ilmapiirin hyväksynnälle, millä saadaan tietoturvallisuuden kattavuus organisaation eri tasoilla paremmaksi. (Ezingeard et al., 2005)

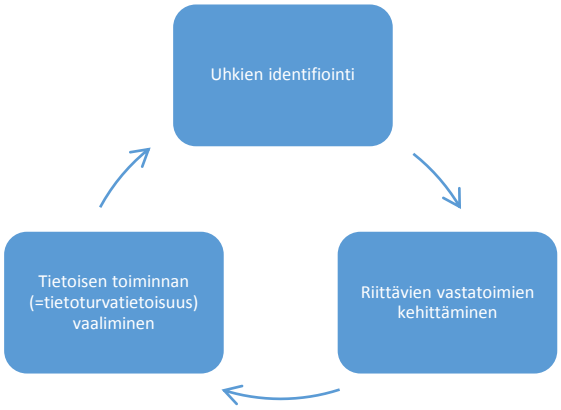
Tietotekniikkaan sijoitetut panostukset täytyy tuottaa liiketoiminnalle hyötyä. Tietoturva koetaan liiketoiminnassa laajemmaksi kuin vain turvallisuudeksi. Näin hyötyjen laajuus myös kasvaa ja liiketoiminnan on helpompi nähdä sijoitetun pääoman hyödyt. Tiedon luotettavuus nousee uuteen arvoon, kun sen käytettävyyttä liiketoiminnassa tarkastellaan. Liiketoiminnan kannalta tämä on tärkeää, jotta hyöty pystytään huomaamaan tai jopa mittaamaan. Liiketoiminnassa myös on havahduttu, että huonoon tietoon pohjautuvat päätökset voivat tulla kalliiksi. Tiedon turvaamisen arvostus myös liiketoiminnan johdossa on kasvussa. Valtiotason ohjaus lakien ja normien muodossa tiedon turvaamisessa on myös lisääntynyt. (Ezingeard et al., 2005)

Tiedon turvaaminen organisaatiossa on panostusta luotettavaan päätöksentekoon, asiakkaan luottamuksen lisäämiseen, liiketoiminnan jatkuvuuteen ja hyvään hallintatapaan. Nämä ovat myös osatekijät strategisessa tietoturvallisuuden johtamisessa. Tiedon turvaaminen tulee nähdä osana liiketoiminnan arvotuotantoketjua, jotta sen strateginen merkitys erottuu. Käytetyn tiedon tulee olla oikeaa, jotta siihen perustuvat päätökset olisivat hyviä. Ilman tiedon turvaamisen keinoin saavutettua tiedon arvon säilymistä tietoon pohjautuvat liiketoiminnan arvoketjut eivät pysty kasvattamaan liiketoiminnan arvoa. Tiedon turvaamisella on strateginen merkitys ja se tulee tietointensiivisissä arvoketjuissa huomioida osana liiketoiminnan strategiaa.

Tässä luvussa tarkasteltiin tietoturvallisuuden vaikutusalan muutosta organisaatioissa historian kautta, sekä tietoturvallisuuteen liittyviä peruskäsitteitä. Tarkastelun kohteena oli erityisesti tiedon turvaamisen näkökulma, koska sen kautta on mahdollista konkretisoida tietoturvallisuuden yhteys organisaation strategisiin tavoitteisiin. Organisaation tietoturvatoiminnalla pyritään strategisesta lähestymistavasta johdettuna joko ylläpitämään tai kasvattamaan sen omistaman tiedon arvoa. Liiketoiminta ei voi tehdä hyviä päätöksiä ilman tietoturvallisuuden keinoin suojattua strategista tietoa. Seuraavassa luvussa keskitytään hallinnolliseen tietoturvallisuuteen ja riskien hallintaan.

# 3. Tietoturvallisuuden hallinta tietoturvallisuuden ylläpitämisessä

Tietoturvallisuuden hallinnalla tarkoitetaan niitä jatkuvia toimenpiteitä, prosesseja ja toimintoja millä ylläpidetään haluttua tietoturvallisuuden tasoa organisaation tiedossa, tietovarannoissa ja prosesseissa (Alavi, Islam, & Mouratidis, 2014). Tietoturvallisuuden hallinnoinnilla pyritään edistämään luottamusta organisaation tietojärjestelmiin (R. von Solms, 1996). Sen ydin on riskienhallintatyössä, missä työkaluina ovat tietoturvapolitiikat ja tietoturvakontrollit, sekä mekanismit, millä minimoidaan ja poistetaan haavoittuvuuksia (Loser, Nolte, Herrmann, & te Neues, 2011). Tietovarannot käsittävät ne liiketoiminnan toimintojen kannalta kriittiset palaset, joilla on vaikutusta liiketoiminnan prosessien suoritukseen. Pitämällä nämä tietovarannot suojattuna uhkia vastaan tietoturvallisuuden keinoin, pystytään varmistamaan liiketoiminnan prosessien haluttu toiminta. (Alavi et al., 2014)



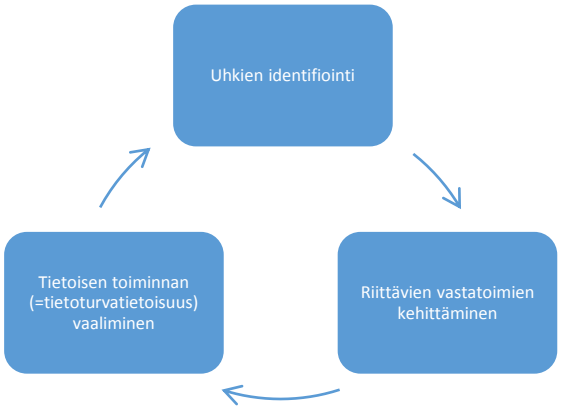

***Kuva 3*** *Sosiotekninen lähestymistapa tietoturvan hallintaan (Loser et al., 2011)*

Tietoturvallisuutta hallinnoidaan tietoturvallisuuden hallintajärjestelmällä, mikä muodostaa järjestelmällisen viitekehyksen ja rajaukset tietojärjestelmien turvalliselle resurssien käytölle. Järjestelmän päätavoitteena on luoda sellaiset järjestelyt, millä poistetaan tai vähennetään tietoturvallisuuteen liittyviä riskejä ja niiden kautta vähennetään haavoittuvuuksien hyväksikäyttö-mahdollisuuksia, joilla voisi olla vaikutusta organisaation toimintaan. Tämä järjestelmä sisältää myös inhimillisten tekijöiden huomioimisen, kuten yleensäkin johtamisessa. (Alavi et al., 2014)

Tietoturvallisuuden hallinta jaetaan tekniikkaa ja hallinnollista näkökantaa kuvaaviin osiin. Osien tarkoitus on tukea toisiaan ja muodostaa yhdessä kokonaisuus hallinnointia varten. Tietoturvallisuutta hallinnoidaan tietoturvadokumentaation avulla. Tietoturvallisuuden hallinnan dokumentaatiota kutsutaan tietoturvapolitiikaksi. Tietoturvapolitiikka kirjoitetaan eri organisaation tasojen käyttöön, jotta sitä olisi helppo soveltaa kullakin tasolla.

Tietoturvallisuuden sosioteknisessä lähestymistavassa, mitä Kuva 3 esittää, otetaan huomioon ihmisten sosiaalinen vaikutus tietoturvan hallinnassa. Tämä tarkoittaa sitä, että kaikissa tietoturvallisuuden alueissa käydään läpi kunkin varannon arvoon liittyvät asiat sen omistajan määrittelemänä. Omistajan kanssa varannosta saadaan yhteisen käsittelyn kautta paremmin esille tietovarannon sosiotekniset näkökulmat. Tämä varanto ja siihen liittyvä tietoyhdistelmä luokitellaan, sekä liitetään niitä koskeviin liiketoiminnan

prosesseihin. Käymällä läpi kaikki liiketoimintaprosesseihin liittyvät varannot saadaan tuotettua kattava lista niihin osallistuvista tahoista sisältäen organisaatiot, ihmiset, tekniset järjestelmät, ympäristöt ja tietovirrat (Loser et al., 2011). Näistä yhdessä koostuvat liiketoimintaprosessien varannot, joita tietoturvallisuuden keinoin pyritään suojaamaan. Tämän varantojen ja liiketoimintaprosessien kautta kerätyn tiedon perusteella voidaan selkeämmin nähdä prosessien omistajat, vastuut ja tietojen luokitukset, sekä pystytään määrittelemään organisaation varantojen merkitys liiketoiminnalle. (Loser et al., 2011)




***Kuva 3*** *Sosiotekninen lähestymistapa tietoturvan hallintaan (Loser et al., 2011)*

Tietoturvallisuutta hallinnoidaan organisaatiossa tietoturvallisuuden hallintajärjestelmällä. Se luo rungon toiminnalle, jonka pyrkimyksenä on ylläpitää haluttua tietoturvallisuuden tasoa organisaatiossa riskienhallinnan keinoin. Seuraavaksi käsitellään tarkemmin sosiaalisten tekijöiden vaikutusta tietoturvallisuuden hallinnassa, jotta voidaan ymmärtää riskien hallinnan merkittävintä tekijää paremmin.

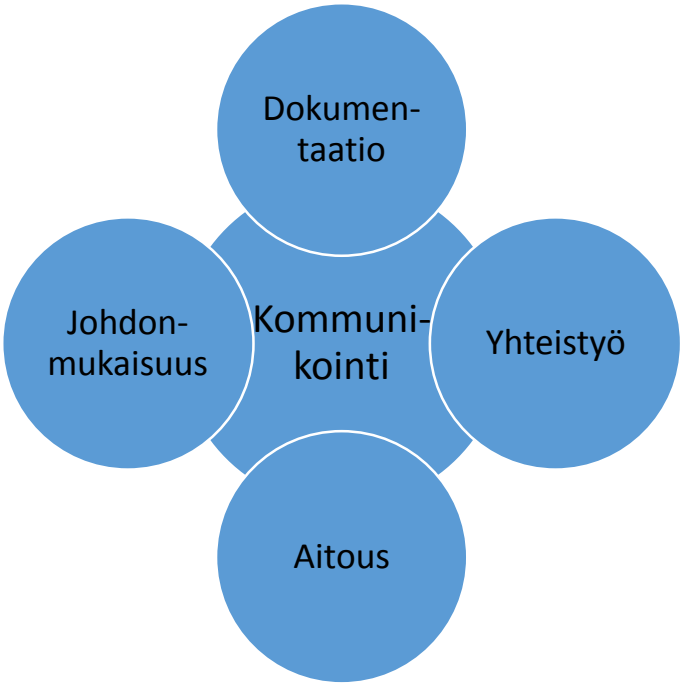
## 3.1 Sosiaalisten tekijöiden vaikutus tietoturvallisuuden hallintaan

Tietoturvallisuuden hallinnassa on huomioitava myös sosiaaliset tekijät työprosessien osana. Tietoturvallisuuden hallinta on jatkuva prosessi, mitä pitää johtaa kuten liiketoiminnan muitakin osia. Tietoturvallisuuden johtamisessa on huomioitava tekniset ja sosiaaliset näkökulmat, koska kyseessä ovat ihmisten ja tekniikan avulla yhdessä saavutettavat tavoitteet. Johtamisen keinoilla vaikutetaan tavoitteellisesti ihmisten käyttäytymiseen ja teknisillä muutoksilla ihmisten käyttämiin järjestelmiin. Tietoturvallisuuden johtamisen tarkoituksena on sekä hallintaprosessien järjestyksen varmistaminen että niiden kontrolli tekniikan avulla. (Loser et al., 2011)

Tietoturvallisuuden hallintajärjestelmässä huomioidaan inhimilliset tekijät, jotta yksilön tehokkuus voidaan optimoida. Hankalaksi koetut asiat pyritään korvaamaan helpommiksi koetuilla järjestelyillä. Kukin ihminen kuitenkin ohjaa eniten omaa käyttäytymistään ja pyrkii tehostamaan omaa toimintaansa kykyjensä mukaan. Tämä voi johtaa yksilöiden toiminnassa tietoturvaa heikentäviin menettelyihin. Sen vuoksi on tärkeää, että sosiotekninen näkemys huomioidaan tietojärjestelmien ja tietoturvallisuuden hallintajärjestelmän kehityksessä. (Alavi et al., 2014)

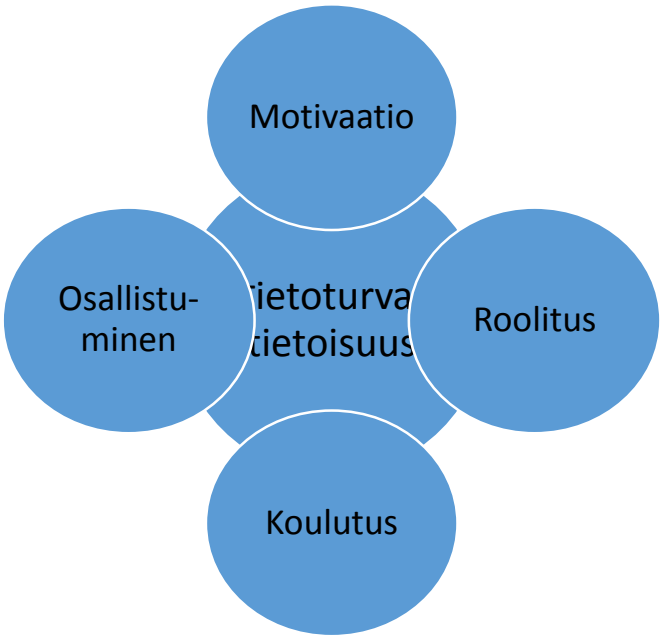
Inhimillisiin tekijöihin organisaation tietoturvallisuudessa vaikutetaan erityisesti kommunikoinnin, tietoturvatietoisuuden sekä johdon tuen avulla. Kuten Kuva 4 havainnollistaa, kommunikoinnin täytyy olla kohdeyleisöä houkuttelevaa, jotta sillä

pystytään vaikuttamaan ihmisten ajatteluun ja tekemiseen. Hyvässä kommunikoinnissa täytetään aitouden määritelmä, mikä sisältää luottamuksellisuuden, luotettavuuden sekä välttämättömyyden käsitteet. Viestinnällä tuodaan esille vain asioita, joiden oletetaan kiinnostavan vastaanottajia. Kommunikoinnin tulee myös perustua jo sovittuihin asioihin. Virallisen tiedon vastaisesti viestittäessä aiheutetaan sekaannusta. Kommunikaation määrittelyssä on otettava huomioon johdonmukaisuus ja jatkuvuus. Viestintää tulee ylläpitää, jotta siitä tulee osa jokapäiväistä toimintaa. Viestintä ei saa olla vain yhdellä medialla tiedon siirtämistä, vaan useilla eri tasoilla toimivaa tiedon kokoaikaista siirtoa. Näin tiedottamisen vaikuttavuus korostuu ja siitä tulee oletettu osa toimintaa. Yhteistyön tarkoituksena on saavuttaa sekä luotettava yhteys että yhteisymmärrys eri toimijoiden välillä. Kommunikoinnilla pyritään myös ylläpitämään samanlaista ajattelutapaa ja tuomaan esille eri osapuolien eroavia näkemyksiä. Näin kommunikoinnilla saavutetaan kaksisuuntainen tiedon siirto ja lopputuloksena on suuremman joukon yhteinen ymmärrys kokonaisuuteen, mitä myös kulttuuriksi kutsutaan. (Alavi et al., 2014)




***Kuva 4*** *Inhimilliset tekijät kommunikoinnissa (Alavi et al., 2014)*

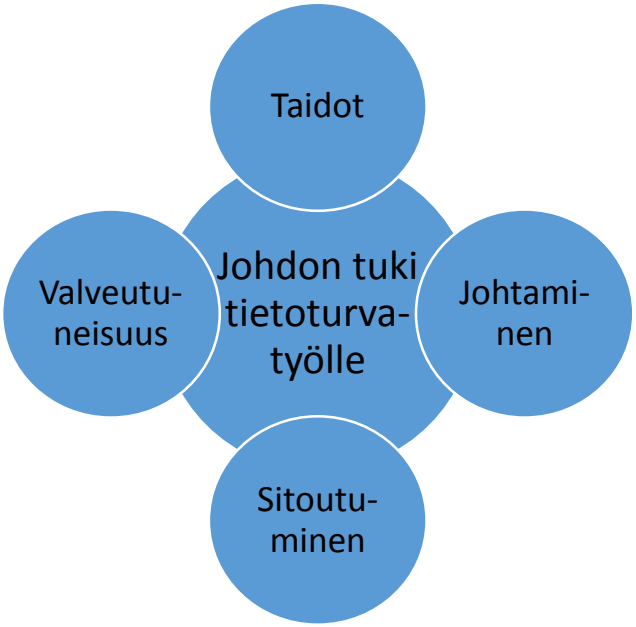
Tietoturvatietoisuus ohjaa organisaation toimijoita oikeanlaiseen tietoturvapolitiikan soveltamiseen ja järjestelmien käyttöön. Kuva 5 avaa tietoturvatietoisuuden inhimilliset tekijä. Tietoturvatietoisuus tehdään osaksi työkulttuuria pitämällä tietoturvallisuuden aiheita yllä jokapäiväisessä toiminnassa ja tuomalla uusia uhkia organisaation jäsenten tietoon. Tietoturvatietoisuuteen kasvattamisen tarkoituksena on motivoida henkilöstöä tietoturvaohjeistuksen noudattamiseen, sekä sen pyrkimyksenä on myös saada kaikki osallistumaan tietoturvatietoiseen toimintaan. Tarkoituksena on tehdä osallistumisen ulkopuolelle jäämisestä vaikeampaa kuin itse osallistuminen, määrittää eri toimijoiden vastuut, roolit ja vaikutusmahdollisuudet sekä kasvattaa tietämystasoa tietoturvallisesta toiminnasta jokapäiväisissä tilanteissa. *(Alavi et al., 2014)*




***Kuva 5*** *Inhimilliset tekijät tietoturvatietoisuudessa (Alavi et al., 2014)*

Yrityksen johdon tuella Kuva 6 tietoturvasta tehdään jokapäiväinen toimintamalli ja luodaan siitä osa yrityskulttuuria. Yrityksen johdon tulee näyttävästi antaa tukensa tietoturvatyölle, jotta viesti sen tärkeydestä tulee kaikille selväksi. Jotta yrityksen johto pystyisi näyttämään esimerkillään tietoturvan tärkeyden, sen tulee ensin omaksua tietoturvan valveutuneisuuden osaksi omaa johtamistaan. Sen jälkeen vasta voi vakuuttavasti johtamisen keinoin viedä tietoturvan tärkeyttä eteenpäin organisaatiossa. Ymmärryksen ja arvostuksen tulee olla aistittavissa, jotta viesti kuulijalle menee läpi. Tietoturva tulee mieltää tärkeäksi välttämättömyydeksi ja sen johtamisjärjestelmää tulee avoimesti tukea. Yrityksen johdon asenne tietoturvaa kohtaan ohjaa koko yrityksen suhtautumista siihen. Tämän vuoksi johdolla on suurin merkitys tietoturvan soveltamisessa ja heidän esimerkkinsä ohjaa myös eniten tietoturvakulttuurin kehitystä organisaatiossa. (Alavi et al., 2014)

Tietoturvallisuuden hallintajärjestelmään tulee sitoutua. Sitä tulee ylläpitää ja kehittää koko organisaation elinkaaren ajan. Järjestelmän käyttäminen organisaatiossa on jatkuva prosessi, mihin tulee koko organisaation panostaa. Ilman sitoutumista ja motivaatiota sitä ei saada toimimaan yrityksen liiketoiminnan tavoitteiden mukaisesti. Ylimmässä johdossa tulee myös olla riittävä määrä osaamista, jotta tietoturvallisuuden hallintajärjestelmä saadaan toimimaan. Yrityksen johdossa tulee vähintäänkin olla ymmärrys strategisesta tietoturvallisuudesta, sekä siitä miten se toteutetaan organisaatiossa. Jotta organisaatio saadaan etenemään kohti yhteisiä tavoitteita, sillä pitää olla runsaasti osaamista myös johtamisesta. Yrityksen johdon tulee määritellä vastuut ja omistajuudet tietoturvalle, sekä strategisen turvallisuuden johtamiselle. Koska itse johtamisella on suuri vaikutus organisaation käyttäytymiseen, on se silloin myös yksi tärkeimmistä inhimilliseen tietoturvallisuuteen vaikuttavista tekijöistä. (Alavi et al., 2014)




***Kuva 6*** *Inhimilliset tekijät johdon tuessa tietoturvatyölle (Alavi et al., 2014)*

Inhimilliset tekijät on huomioitava tietoturvallisuuden hallinnoinnissa. Ihmisten toimintaan vaikuttaminen parantaa tietoturvallisuuden tasoa parhaiten. Kommunikointi, tietoturvatietoisuus ja johdon tuki tietoturvatyölle luovat perustan inhimilliseen suhtautumiseen tietoturvallisuuteen organisaatiossa. Seuraavassa kappaleessa käsitellään riskienhallintaa, joka hyvin toteutettuna antaa oikeanlaisen syötteen tietoturvatyölle ja huonosti toteutettuna huonontaa liiketoiminnan toimintaedellytyksiä.

## 3.2 Riskien hallinta

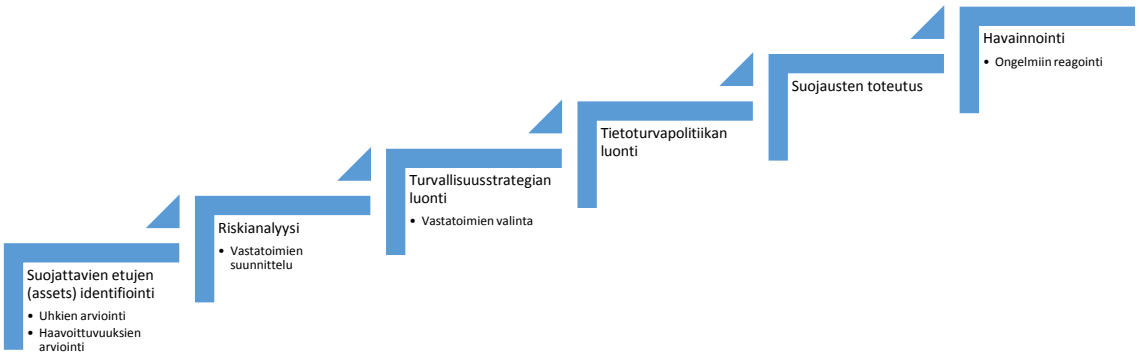
Riskien hallinta on tietoturvallisuuden kehityksen lähtökohta. Riskien hallinnalla pyritään minimoimaan liiketoiminnan esteeksi nousevia ongelmia etukäteen, sekä tuntemaan toimintakenttää missä yritys toimii. Riskien hallinnan tavoitteena on tietovarantojen suojeleminen uhkia vastaan liiketoiminnan jatkuvuuden mahdollistamiseksi, tappioiden vaikutusten alentamiseksi ja tuottavuuden turvaamiseksi *(Asosheh, Hajinazari, & Khodkari, 2013).* Parhaimmillaan riskien hallinta on yrityksen strategisen suuntautumisen ohjaamista syöttävä toiminto, millä mahdollistetaan liiketoiminnan selviytyminen. Turvallisuusriskien lähtökohtana on tuntea liiketoimintaprosessit, suojauskohteet ja niiden suojaustarpeen. Usein jo tämän ensimmäisen riskien hallinnan vaiheen toteuttaminen yrityksissä on haasteellista. Ilman suojattavien liiketoimintaprosessien ja suojauskohteiden tuntemista ei riskien hallinnalla saavuteta hyviä tuloksia. Tämä pohjatyö on tehtävä oikein, jotta siihen nojautuvat kerrokset toteuttavat suojauksen parhaalla mahdollisella tavalla. Riskien hallinnan keinoin myös mahdollistetaan resurssien oikea ja riittävä ohjaus. (Sadok & Spagnoletti, 2011)


***Kuva 7*** *Tietovaranto tietoturvadokumentaatiossa (Sadok & Spagnoletti, 2011)*

Kuva 7 esittää tietovarantojen koostumisen luokituksesta, tiedon liiketoiminta-arvosta, sekä arkaluonteisuudesta. Nämä ominaisuudet huomioidaan tietovarantojen luokittelussa, jotta varannoille pystytään varmistamaan mahdollisimman tehokas suojaus liiketoiminnan kannalta. (Sadok & Spagnoletti, 2011) Tietovarannon merkitys liiketoiminnalla tulee olla suojauksen perusteena, jotta sen hyötynäkökulma nähtäisiin selkeämmin liiketoiminnassa. Sama toimintamalli on käytössä kuten missä tahansa muussakin liiketoiminnan investoinnissa. Samalla varantojen havainnointikykyä kasvatetaan yrityksen johdossakin ja luodaan ymmärrystä liiketoimintavetoisesta tietoturvallisuuden hallinnasta. Yhteisen varannon arvostuksen jälkeen resurssien kohdentaminen on helpompaa ja riskienhallinnan tehokkuutta saadaan parannettua.

Tietoturvariskien hallinnan haasteet tuovat omat ongelmansa prosessiin, koska kustannusten, riskien ja uhkien arviointi ei ole yksiselitteistä ja objektiivista. Vaikka suoraan riskeistä tai uhkista ei voida tehdä kustannusarvioita, yrityksen käyttämistä resursseista ja yrityksen suojaamista varannoista nämä voidaan tehdä. Yrityksen näkemät kustannukset voidaan laskea kuluseurannan kautta, jolloin tiedetään investointimäärät kullekin varannolle. Useinkaan lukuja ei saada suoraan taloushallinnon järjestelmästä, vaan lukujen saamiseksi pitää tehdä runsaasti töitä. Yksistään varantojen arvo on vain osa riskienhallinnan kustannuksista, mutta antaa riskienhallinnalle enemmän uskottavuutta. Myös hyökkäysten ennustettavuutta on vaikeaa arvioida luotettavasti, koska hyökkäystapoja syntyy koko ajan lisää. Ei ole mitään ennalta määritettyä tekniikkaa ennustaa näitä etukäteen, vaan ne tulee todeta vasta havainnoinnin jälkeen. (Sadok & Spagnoletti, 2011)

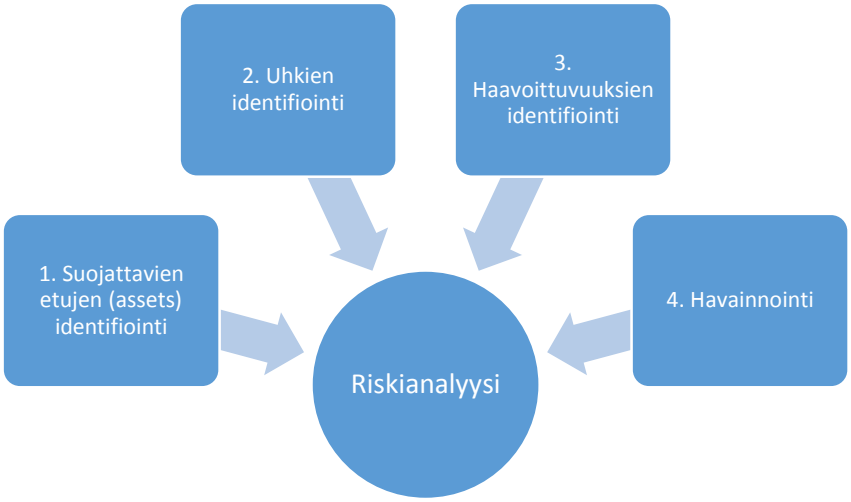
Liiketoimintakohtaisien kriteeristöjen puuttuessa suojauksien toteuttamiseksi jokainen liiketoimintaprosessi on ainutlaatuinen. Juuri omalle liiketoimintamallille ei ole valmiina kontrollikirjastoa. Tähän ongelmaan liiketoiminnan prosessien standardointi tai liiketoimintojen suunnittelu sopimaan valittuun standardiin (Gutiérrez-Martínez, Núñez-Gaona, & Aguirre-Meneses, 2015; Hussein, Ghoneim, & Dumke, 2011) toisi merkittävän edun. Koska riskien hallinnan prosessit eivät määrittele yhteyttä liiketoiminnan, valvonnan ja tietoturvarikkeisiin vastaamisen välillä, liiketoimintaa pidetään liian kaukana tietoturvatyöstä. Riskien hallinnan tulisi syöttää liiketoimintaan liittyvien päätöksien tekijöitä, ja yrityksen johdon tulisi antaa tietoa liiketoiminnan liikkeistä riskien hallintaan. Tällä toimintojen erillään pitämisen syiden ratkaisemisella päästäisiin turvallisempaan liiketoimintamalliin, missä suojauksella tuotaisiin liiketoiminnalle liikkumavaraa ja pidettäisiin liiketoiminta vaarantumattomana. (Sadok & Spagnoletti, 2011)




***Kuva 8*** *NetRAM© kehys riskien hallintaan (Sadok & Spagnoletti, 2011)*

Riskien hallinnan toteuttaminen kokonaisvaltaisella itseään iteroivalla oppimisprosessilla päästään kohti toimivampaa kokonaisuutta. Kuva 8 esittää NetRAM© riskien hallintametodin askeleet. Lähes samoja askeleita käyttävät useat muutkin riskienhallintamenetelmät. Tässä metodissa *suojattavien etujen identifioinnissa* etsitään tietojärjestelmän kaikki osat. Suojauskohteet selvitetään ihmisten, proseduurien ja tietovarantojen (data, ohjelmistot, laitteistot) luokista. Liiketoiminnan edustajien on avattava prosessinsa niin selkeiksi osakokonaisuuksiksi, että siitä pystytään listaamaan kaikki asiat, mitä kukin liiketoimintaprosessi tarvitsee toimiakseen. Koostettu listaus kaikista liiketoiminnan suojauskohteista on pohja, mille koko riskien hallinta rakennetaan. Tämä on siis syytä tehdä huolella, jotta riskienhallinta tulisi kattamaan kaikki liiketoiminnan osat. Näihin kohdistuvien riskien hallinnan työlle arvioidaan seuraavaksi kustannukset suunnitteluun perustuen. Uhkien ja haavoittuvuuksien arvioinnin tavoitteena on varantojen heikkouksien luokittelu tietoturvallisuuden rikkoutumista ja hyökkäyksiä mahdollistavia toimia vastaan. (Sadok & Spagnoletti, 2011)

Varannot, niiden haavoittuvuudet ja uhkat kerätään listoiksi. Listoja täydennetään uusilla eri identifioinnin iteraatiokierroksilla, sekä havainnoinnista saadusta syötteestä. Kuva 9 esittää nämä syötteet *riskianalyysille*. Ensimmäisen riskien hallinnan vaiheen onnistuminen luo pohjan seuraavien vaiheiden onnistumiselle. Onnistuminen tarkoittaa löydösten kattavuutta suhteessa liiketoiminnan varantoihin. Riskienhallinnalla on kussakin toiminnossa oltava käytettävissä syötteenä suojattavat kohteet. Näiden kohteiden kattavalla identifioimisella mahdollistetaan riittävä suojaus kaikille liiketoimintaprosessien suojattaville kohteille. Jos jotain suojattavaa kohdetta ei löydetä analyysin tuloksena, niin se jää täysin suojaamatta tietoturvallisuuden hallintajärjestelmässä. Tämän vuoksi suojattavien kohteiden löytämiseen on kiinnitettävä erityistä huomiota. Suojattaville kohteille määritellään myös omistajat, sekä kriittisyysluokitus suhteessa sen merkitykselle kyseiseen liiketoimintaprosessiin. Jotta kaikki riskit olisivat kontrolloituja, niiden analysointi tulee suorittaa perusteellisesti (Sadok & Spagnoletti, 2011).




***Kuva 9*** *Riskianalyysin osat (Sadok & Spagnoletti, 2011)*

Riskien analyysin tuloksena määritellyt varantoja uhkaavat riskit määritellään ja järjestetään suojaustarpeen mukaisesti. Riskilistojen tarkoitus analyysivaiheessa on pitää yllä riskeihin liittyviä tietoja ja suojaukseen liittyviä päätöksiä. Käsittelyn ohessa tehdään linjaukset suojauksien toteutuksesta kuhunkin riskiin, minkä vaikutusta halutaan vähentää. Liiketoiminnan johdolle esitetään riskienhallinnan tarvitsemat resurssit perustuen suojaustarpeeseen. Liiketoiminnan johdon kanssa yhdessä toteutetaan *turvallisuusstrategia*, minkä pohjana käytetään riskien hallinnasta saatua syötettä. (Sadok & Spagnoletti, 2011)

Suojaus suunnitellaan *tietoturvapolitiikkana* organisaatioon. Tietoturvapolitiikka kuvaa yrityksen eri tasojen tietoturvatarpeet. Varantojen suojaukset toteutetaan liiketoiminnan johdolta saatua budjettia käyttäen. Annettu rahasumma jaetaan suojauksen toteutuskustannuksiin varannon ja riskin tärkeyden määrittelemällä järjestyksellä. Tätä samaa menettelyä käytetään aina budjetointikierrosten yhteydessä perusteluna tietoturvallisuuden investointeihin. Lopulta *suojauksen toteutus* suunnitellaan ja toteutetaan, minkä jälkeen varantojen suojaamisen toimivuutta *havainnoidaan* organisaatiossa. Suojausten havainnoinnissa käytetään metriikoita, joilla pyritään saamaan mahdollisimman hyvä kuva suojauksen toimivuudesta sen oikeassa ympäristössä. Metriikoiden toimivuutta on myös ajoittain tarkasteltava, jottei sokeuduta muutosten synnyttämille havainnointiongelmille. (Sadok & Spagnoletti, 2011)

Riskienhallinnan resursoinnin on pohjauduttava varantojen liiketoiminta-arvoihin. Suojaukseen käytettävien resurssien painotuksen on oltava suhteutettuna varannon liiketoiminta-arvoon, jotta suojauksella saadaan eniten hyötyä liiketoiminnalle. Kattava varantojen määritys on pohja onnistuneelle riskienhallinnalle. Viemällä riskienhallintatoiminta yrityksen johtotasolle tuodaan johdolle lisää työkaluja strategiseen suunnitteluun ja ohjaukseen, sekä vaihdetaan tehokkaammin tietoa liiketoimintariskeistä. Kun strategisessa johtamisessa huomioidaan liiketoimintariskejä laajemmin, niin yrityksen toimintaa pystytään ohjaamaan strategiassa kuvattua tavoitetilaa kohti varmemmin askelin. Seuraavassa kappaleessa käsitellään tarkemmin miten liiketoiminnan tekijät tulisi huomioida riskianalyysissä.

### 3.2.1 Liiketoimintaan liittyvät tekijät riskianalyysissä

Riskienhallinnan on tärkeää olla sidoksissa organisaation liiketoimintaan ja sen on huomioitava mahdollisimman kattavasti organisaation toteuttamat tavat käsitellä, säilyttää ja hävittää tietoa. Lähtökohtana riskien hallinnalla on oltava liiketoiminnan suojaaminen. Liiketoimintaa suojataan analysoimalla sitä ja löytämällä sen tärkeät osatekijät eli varannot. Jokaiseen liiketoimintaprosessiin liitetyt varannot ja niihin liittyvät riskit käsitellään liiketoiminnan omistajan ja yrityksen tietoturvallisuuden omistajan kesken. Liiketoimintaprosessi tulee ymmärtää, jotta siihen liittyviin riskeihin osaa määritellä kriittisyyden. Liiketoiminnan on myös osattava kertoa pystyykö liiketoimintaprosessi etenemään mahdollisesti toteutuvan riskin kanssa. (Sadok & Spagnoletti, 2011)

Riskienhallinnan on myös oltava dynaamista ja proaktiivista, sillä riskit muuttuvat jatkuvasti teknologisen ja taloudellisen kehityksen vaikutuksesta. Riskienhallinta-prosessissa on huomioitava erityisesti yrityksen operationaalinen toiminta, resurssien hallinta, yrityksen strategia, asiakassuhteet ja arvoketju. *Strategisella* tasolla kilpailun voimakkuus, sekä lakiperustaiset vaatimukset vaikuttavat riskien painotuksiin. Kilpailun voimakkuuden kautta painetta tulee suojata omaa kilpailuetua suhteessa kilpailijoihin ja lakisääteisten painotusten kautta syntyy painetta yritysjohdon vastuullisuuden kasvun vuoksi. Organisaatiotasolla on yhdistettävä käytäntöjä ohjeistuksien ja sääntöjen avulla riskienhallintaprosessien yksinkertaistamiseksi. Lisäksi on otettava huomioon turvallisuuden kontrollien vaikutus suoritukseen ja käyttää kontrollien seurantajärjestelmää, jonka avulla voidaan vähentää päätöksentekoon tai toimintaan liittyviä virheitä. *Asiakassuhteiden* tasolla vaikuttavat asiakkuuksien ja asiakaskanavan monimuotoisuus. Erilaiset asiakassuhteet synnyttävät enemmän erilaisia uhkia, kuin täysin samanlaiset. Asiakaskanavien erilaisuus synnyttää vaihtelua samanlaisesti, kuin itse asiakkuudetkin. Kanavien erilaisuus on huomioitava riskienhallintatyössä, jotta niihin liittyvät riskit voidaan minimoida. *Arvoketjun* osalta riskeihin vaikuttavat tietojärjestelmien integrointitaso toimitusketjussa, sekä yrityksen riippuvuus kyberturvallisuudesta. Verkottuneiden toimitusketjujen ongelmat piilevät kaikkien liitettyjen arvoketjujen yhteenlasketuista riskeistä. Toimittajien tietoturvallisuuden taso tulee vähintäänkin tietää ja liitäntöjen kautta syntyviin ongelmiin on varauduttava riskien analysoinnissa. Toimitusketjuissa jaettavan tiedon turvallisuudesta on huolehdittava kaikkien osapuolien järjestelmissä ja ongelmat ketjun muissa jäsenissä voi vaikutuksiltaan olla vakavampaa muille arvoketjuun osallistuville yrityksille. (Sadok & Spagnoletti, 2011)

Liiketoimintalähtöisessä riskianalyysissä on huomioitava liiketoiminnan prosessit, toteuttavat tekijät, sekä kaikki liiketoiminnan liityntäpinnat. Toimitusketjut on myös tunnettava, jotta omaan organisaatioon kohdistuvat ulkoiset riskit voidaan huomioida liiketoiminnassa. Riskianalyysissä on analysoitava liiketoimintaprosessit ja niiden toimintaedellytykset riskin toteutuessa, sekä myös määriteltävä toiminnan mahdollistavat vähimmäistekijät. Näiden tekijöiden kautta pystytään kohottamaan liiketoimintaprosessin suoritukseen vaadittavien kriittisten tekijöiden suojauksen arvoa suhteessa liiketoimintaan ja resurssit kohdentuvat liiketoimintajohtoisesti tarkemmin. Riskianalyysin tuloksena saadaan kattava kuva liiketoimintaan kohdistuvista riskeistä yrityksen toimintaympäristössä. Tätä listaa on täydennettävä liiketoiminnan strategian suunnittelussa, jottei liian suurta riskinottoa syntyisi. Seuraavassa kappaleessa tarkastellaan strategista tietoturvallisuusjohtamista. Siinä liiketoiminta hyödyntää syötteenä strategiassaan tietoturvallisuuden tuottamaa tietoa.

## 3.3 Tietoturvallisuuden hallinnan formalisointi

Tietoturvallisuuden hallinta voidaan formalisoida esimerkiksi käyttämällä tutkimukseen valittua tietotuvallisuuden standardia ISO27002. Formalisoinnilla pyritään yhtenäistämään tietoturvallisuuden hallinnan prosessit ja toimintatavat, jolloin saavutetaan ylemmällä tasolla esimerkiksi liiketaloudellisia vertailuarvoja tai pyritään yhtenäistämään yritysostoilla hankitun uuden osan tietoturvallisuuden toimintamallit. Formalisoinnin etuja ovat myös hallinnan selkeytyminen ulkopuolisen tarkistuksien osalta, sekä toimintamallien yhtenäisyys esimerkiksi alihankkijoiden kanssa. Formalisoinnilla pyritään myös takaamaan riittävä tietoturvataso ja voittamaan uusia liiketoimintasopimuksia (R. von Solms, 1996). Yhtenä formalisoinnin etuna voidaan pitää myös tietoa siitä, että formalisoinnin tuloksena kaikki tietoturvallisuuden osa-alueet on varmimmin otettu huomioon tietoturvallisuuden hallintajärjestelmän eri osissa.

| **Nimi:** | **Selite englanniksi:** |
|---|---|
| ISO 13335: ISO/IEC 13335 | Consists of two parts, under the general title *Information technology —Security techniques — Management of information and communications technology security.* Several sections of the original ISO 13335 are replaced with ISO 27005. |
| ISO 17799: ISO17799 (BS7799) | Is comprehensive in its coverage of security issues. It contains significant control requirements, extremely complex. |
| ISO 27001 | Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System. This standard adopts a process approach. |
| ISO 27002 | Provides control objectives and best practice controls to be selected and implemented in order to mitigate risks and achieving information security. This standard contains 11 security control clauses including 39 main security categories and 133 controls. |
| ISO 27003 | Provides practical implementation guidance for ISMS in accordance with ISO/IEC 27001. |
| ISO 27004 | Provides guidance on the development and use of measures in order to assess the effectiveness of ISMS, control objectives, and controls as specified in ISO/IEC 27001. |
| ISO 27005 | Provides guidelines for information security risk management. |
| ISO 27006 | Specifies requirements and provides guidance for bodies providing audit. |
| ISO 27007 | Provides guidance on conducting ISMS audits, as well as guidance on the competence of ISMS auditors. |
| ISO 27008 | Provides guidance on reviewing the implementation and operation of controls. |

***Taulukko 1*** *ISO/IEC 27000-sarjan yleisimmät standardit (Asosheh et al., 2013)*

ISO/IEC 27000 –sarja on valikoima tietoturvallisuuden hallinnan standardeja, millä eri tietoturvallisuuden osa-alueita voidaan kehittää formaaliin suuntaan. Standardit

pohjautuvat ISO 27001 standardiin ja tukevat sen osa-alueiden toteutusta. Taulukko 1 listaa näistä tärkeimmät standardit kuvauksineen. (Asosheh et al., 2013)

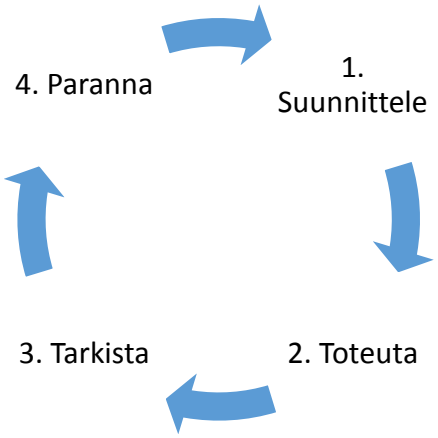
Yleisesti käytössä oleva tietoturvallisuuden hallintajärjestelmä on kuvattu ISO 27002–standardissa. Hallintajärjestelmä on jaettu yhteentoista eri osa-alueeseen. Taulukossa Taulukko 2 on lueteltuna nämä osa-alueet, sekä niiden suomenkieliset vastineet. Eri osa-alueet pyrkivät kattamaan tietoturvallisuuden hallinnan kannalta tärkeät näkökulmat kohdeorganisaatiossa ja näin varmistamaan monipuolisen tietoturvallisuuden hallintajärjestelmän. Tietoturvallisuuden hallinnassa olennaisinta on oikein mitoitettu organisaation suojaaminen uhkilta ja haavoittuvuuksilta *(Loser et al., 2011)*. Tällä pyritään mitoittamaan resurssit oikein, jotta liiketoiminnan muut toiminnot eivät kärsisi liiallisista tietoturvainvestoinneista tai toteutuneista tietoturvapoikkeamista. ISO 27002 Tietoturvallisuuden hallintajärjestelmässä ei keskitytä löytämään varantoja pelkästään liiketoiminnan prosesseista, vaan myös muista prosesseista liiketoiminnan ulkopuolelta. Näitä prosesseja ovat liiketoiminnan tukitoimintojen prosessit, mitkä eivät suoranaisesti ole liiketoimintaa. (Loser et al., 2011)

| **Osa-alueen englanninkielinen nimi** | **Osa-alueen suomenkielinen nimi** |
|---|---|
| 1. Security policy | Tietoturvallisuuspolitiikka |
| 2. Organization of information security | Tietoturvallisuuden organisoiminen |
| 3. Asset management | Suojattavien kohteiden luokitus ja valvonta |
| 4. Human resources security | Henkilöstöturvallisuus |
| 5. Physical and environmental security | Fyysinen turvallisuus ja ympäristön turvallisuus |
| 6. Communications and operations | Tietoliikenteen ja käyttötoimintojen hallinta |
| 7. Access control | Pääsyoikeuksien valvonta |
| 8. Information systems acquisition | Ohjelmistoturvallisuus |
| 9. Information security incident | Tietoturvapoikkeamien käsittely |
| 10. Business continuity | Liiketoiminnan jatkuvuuden hallinta |
| 11. Compliance | Vaatimustenmukaisuus |

***Taulukko 2*** *ISO/IEC 27002:2008 tietoturvallisuuden hallintajärjestelmän osa-alueet (Loser et al., 2011)*

Standardin hallinnollisen osan toteutus aloittaa tietoturvallisuuden hallintajärjestelmän koostamisen dokumentaatiosta. Tietoturvallisuuspolitiikan luomisella pyritään hahmottamaan yrityksen toimintaa ja sen kautta avaamaan suojausrakenteet dokumentaation muotoon. Taulukko 2 ei nosta riskien hallintaa erikseen otsikkotasolle. Sen sijaan riskienhallinta on sisällytettynä kuhunkin toimintoon osaksi sen aliosan hallintajärjestelmän ydintä. Riskienhallinta toimii syötteenä tietoturvallisuuspolitiikalle organisaatiossa. Riskienhallinta on siis toteutettava ennen kuin pystytään koostamaan tietoturvallisuuspolitiikka.

ISO 27001 määrittelee tietoturvan hallintajärjestelmän toteutuksen 4 eri vaiheeseen. Nämä vaiheet on esitetty alla Kuva 10 .




***Kuva 10*** *ISO/IEC 27001 – standardin määrittelemä tietoturvallisuuden hallintajärjestelmän kehityksen vaiheet (Asosheh et al., 2013)*

Suunnitteluvaiheessa luodaan tietoturvapolitiikka, määritellään tavoitteet, prosessit ja menettelytavat. Kaikki yritykselle merkitykselliset toiminnot, millä hallinnoidaan riskejä liiketoiminnassa ja sen ulkopuolella on kuvattava. Näiden toimintamallien pitää tukea liiketoiminnan muuta ohjeistusta ja tavoitteita. Toteutusvaiheessa luodaan tietoturvallisuuden hallintajärjestelmän politiikka, eli dokumentaatio, toteutetaan tietoturvakontrollit, sekä niihin liittyvät prosessit ja menettelyt. Itse toteutusvaihe on kuvattuna ISO27003 standardissa tarkemmin, mistä on löydettävissä 5 erillistä toimintavaihetta. Nämä vaiheet on kuvattu alla Taulukko 3. Standardin ohjeistusta seuraamalla pystytään vaiheittain luomaan toimiva tietoturvallisuuden hallintajärjestelmä. (Asosheh et al., 2013)

| | |
|---|---|
| 1. | Hankitaan organisaation johdon tuki tietoturvallisuuden hallintajärjestelmän kehittämisprojektille |
| 2. | Määritellään tietoturvallisuuden hallintajärjestelmän laajuus, rajat ja johdon tietoturvapolitiikka |
| 3. | Suoritetaan tietoturvavaatimuksien analyysi |
| 4. | Tehdään riskien arviointi ja suunnitellaan riskienkäsittelytoiminnot |
| 5. | Suunnitellaan tietoturvallisuuden hallintajärjestelmä |

***Taulukko 3*** *Tietoturvallisuuden hallintajärjestelmän toteutusprojektin vaiheet ISO/IEC 27003-standardin mukaisesti*

Tietoturvapolitiikka voidaan jakaa kolmeen alueeseen Kuva 11, millä pyritään selkeyttämään sen hallintamallia. Korkeimmassa tasossa kuvataan yleiset tavoitteet. Tämän osuuden määrittelee yrityksen johto yleensä tietoturvasta, sekä tietohallinnosta vastaavien henkilöiden kanssa yhdessä. Keskimmäisessä kerroksessa kuvataan tietoturvallisuuteen liittyvien päätösten tekoon tarvittavat tiedot. Alimmaisessa kerroksessa kuvataan yksityiskohtaisemmin toteutus ja vaatimukset valikoiduissa käyttötarpeissa. (Baskerville & Siponen, 2002)


*Kuva 11 Tietoturvapolitiikan tasot (Baskerville & Siponen, 2002)*

Näin kuvattuna synnytetään dokumentaatio, jonka sisältö antaa ohjeistusta kaikilla yrityksen tasoilla toimiville henkilöille. Osana tietoturvallisuuden johtamista kuvataan myös tietoturvallisuustyöhön varattu henkilöstö. Tietoturvallisuuden organisoinnin tavoitteena on kuvata käytettävissä oleva henkilöstö, sekä heidän roolinsa tietoturvallisuustyössä. Roolien kautta tietoturvallisuuden hallinnan prosessit saavat tekijät ja koko organisaatio ymmärtää paremmin tietoturvallisuustyöhön liittyvät vastuut. Yleisiä standardeja käytettäessä tulee myös pyrkiä huomioimaan niiden ongelmat, sekä soveltuvuus suojattavaan ympäristöön. Muita huomioitavia asioita ovat sosiaaliset näkökulmat, sekä liiketoiminnan vaatimuksien huomioiminen (Baskerville & Siponen, 2002).

Tietoturva koetaan usein hyvin tekniseksi ja hankalaksi asiaksi. Tämä hankaloittaa tietoturva-asiantuntijoiden ja yrityksen ylimmän johdon kommunikointia. Tekninen lähestymistapa johtamisen kautta tulisi sivuuttaa ja käyttää yleisempiä termejä keskustelussa. Yrityksen johdon tulee ymmärtää asia mistä puhutaan, jotta siihen saadaan selkeä linjaus. Tämä ongelma on otettava huomioon toimittaessa ylimmän johdon kanssa. Johtamisen kautta ongelmana on siis tietämys ja erityisesti tekninen tietämys. Tällöin yhtenä ratkaisuna olisikin tietoturvallisuudesta ymmärtävän henkilön nostaminen johtoryhmään. Johtoryhmässä toimiminen vaatisi tietoturvallisuuden asiantuntijalta myös johtamisen osaamista, jotta työ onnistuisi. Näin johtoryhmällä olisi tietämys käytettävissään ja tämä henkilö pystyisi keskustelemaan muiden johtajien kielellä tietoturvallisuuden asioista. (Ezingeard et al., 2005)

Formalisoinnissa tulee huomioida liiketoimintalähtöisyys, jotta standardin toteuttamisesta olisi liiketaloudellista hyötyä. Yhtenäistämällä tietoturvallisuuden toimintatapoja saavutetaan etuja, joita tulee käyttää hyväksi liiketoiminnassa. Formalisoinnin tavoitteet tulee määritellä liiketoiminnan etuina, eikä saavutetulla standardilla, jotta sen liiketoimintahyöty jää yrityksen toiminnan tukemiseen. Seuraavassa kappaleessa käsitellään strategisen tietoturvallisuuden hyötynäkökulmaa liiketoiminnassa.

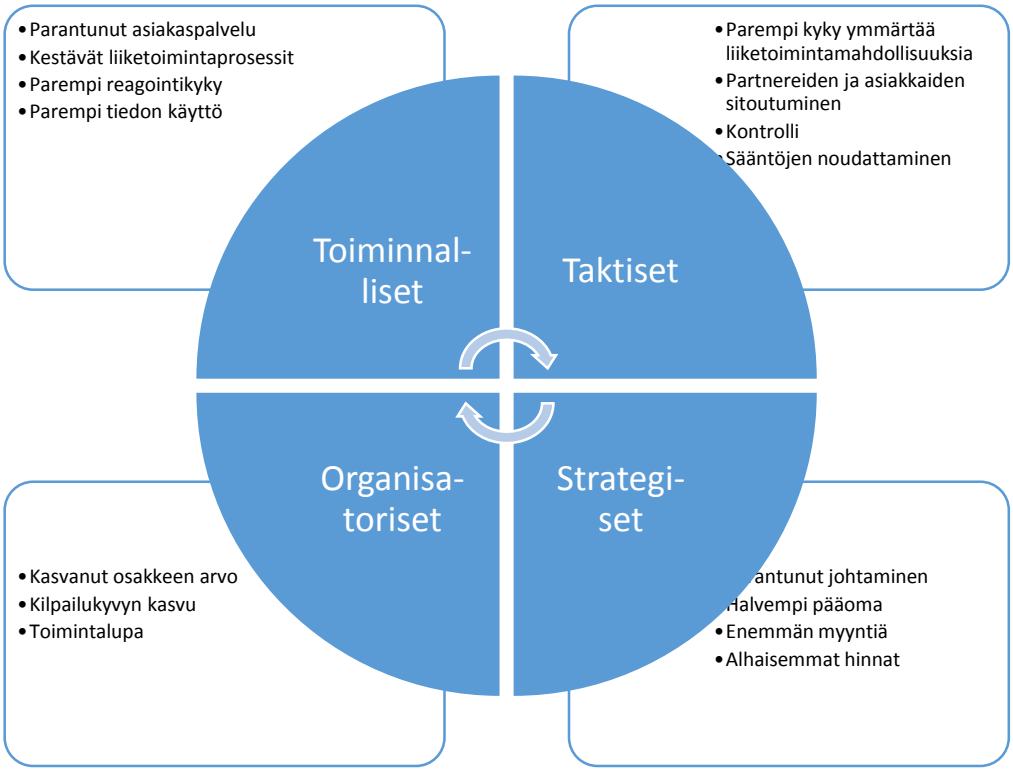
# 4. Strategisen tietoturvallisuusjohtamisen hyötynäkökulma

Tiedon turvaamisen strategia määritellään seuraavasti *”Määritellään kuinka luotettavuutta, tarkkuutta, turvallisuutta ja käytettävyyttä yrityksen tietovarannoissa pitäisi johtaa jotta organisaatio saisi toiminnasta maksimaalisen hyödyn suhteessa yrityksen tavoitteisiin ja strategiaan.”* (Ezingeard et al., 2005, s.23)

Tiedon turvaamisen strategian on oltava linjassa yrityksen strategian kanssa ja sen tulee tukea yrityksen toimintaa. Huonosti laadittu tiedon turvaamisen strategia haittaa pahimmillaan yrityksen toimintaa ja realisoi uhkien synnyttämien kustannuksien vaikutukset liiketoiminnan kannettavaksi. Näin toteutuisi strategisiksi nostetut riskit ja liiketoiminta olisi suurissa ongelmissa. (Ezingeard et al., 2005)

Yrityksen liiketoiminnan suunnan määrityksessä voidaan käyttää tiedon turvaamisen strategiasta saatua syötettä. Siinä organisaation strategiatyön pohjaksi otetaan tiedon turvaamisen merkitys organisaation toiminnalle. Tämän merkityksen kautta voidaan johtaa lähtökohdat liiketoiminnalle, jossa huomioidaan paremmin liiketoimintariskit. Tiedon turvaamisessa pyritään saamaan organisaation käytössä olevasta tiedosta maksimaalinen hyöty sen tietoturvaominaisuuksien säilymisen kautta, mikä sekä parantaa liiketoiminnan mahdollisuuksia tehdä hyviä päätöksiä, että selviytymismahdollisuuksia liiketoimintariskien toteutuessa.

Hyvällä tiedon turvaamisella tuetaan yrityksen liiketoiminnan ydintä. Tietointensiivisten yritysten tapauksessa puhutaan ydinliiketoiminnasta ja sen onnistumisesta. Hyödyt ovat nähtävissä useilla eri tasoilla yrityksessä toiminnallisina, taktisina, strategisina ja organisatorisina hyötyinä, mitkä tiivistää Kuva 12. (Ezingeard et al., 2005)




***Kuva 12*** *Tiedon turvaamisen hyödyt (Ezingeard et al., 2005)*

Kuva 12 kuvaa hyötynäkökulmia, mitä tietoturvallisuuden onnistuneessa tiedon turvaamisessa voidaan liiketoiminnassa saavuttaa. Koska nämä osatekijät ovat konkreettisempia kuin tietoturvan turvaominaisuudet ne ovat helpommin siirrettävissä osaksi liiketoimintastrategiaa. Konkreettiset hyödyt ovat helpommin nähtävissä tietoturvallisuuden ulkopuolelta liiketoimintaa tarkkailevien johtajienkin toimesta.

Tiedon turvaamisen *toiminnalliset hyödyt* (Kuva 12) vaikuttavat välittömästi liiketoiminnan kykyyn tuottaa palveluita ja tuotteita. Tiedon laadun parantuminen parantaa myös asiakaspalvelua, kun tieto on oikeassa paikassa, oikeassa muodossa sekä käytettävissä. Liiketoimintaetujen tavoittelu tuotantoketjujen avulla vaatii luottamuksellisen tiedon turvallista siirtoa ketjuun osallistuville tahoille. Hyvällä tiedon suojaamisella tietoa voidaan jakaa turvallisesti, jopa samaan tuotantoketjuun osallistuvalle kilpailijalle. Tämä ei olisi mahdollista ilman hyvin toteutettuja tiedon turvaamisen käytäntöjä ja korkeaa tietoturvallisuustasoa. Liiketoimintojen kestävyyttä pystytään parantamaan tiedon turvaamisen toteuttamisella laajasti koko organisaation toiminnassa. Tieto on myös paremmin käytettävissä ja samalla käytössä arvokkaampaa, kun se on riittävällä tasolla suojattuna. Riskisietoisuuden kasvaessa liiketoiminnalle jää enemmän pelivaraa toteuttaa rohkeampia strategisia linjauksia ja samalla se tuo nopeamman reagointikyvyn liiketoiminnan ongelmiin mm. varautumisen kautta. (Ezingeard et al., 2005)

Kuva 12 kuvaa tiedon turvaamisen *taktiset hyödyt*, joiden kautta liiketoimintaan saadaan keskipitkän aikavälin parannuksia kumppanisuhteisiin. Liiketoimintamahdollisuuksia voidaan löytää tahoilta, joilla ei ole aikaisemmin uskallettu toimia ympäristön suurten riskien vuoksi. Liiketoiminta- ja markkinatiedon oikeellisuudella parannetaan menestymisen mahdollisuuksia. Parantamalla liiketoiminnan riskiensieto- ja samalla reagointikykyä voidaan saavuttaa paremmat asetelmat riskien ja hyötyjen suhteen uudessa toimintaympäristössä. Sitouttamisella pyritään saamaan liiketoimintaan liittyvien toimijoiden, sekä asiakkaiden yhteistyö pitkäjänteiseksi toiminnaksi. Paremmalla kontrollilla voidaan hallita organisaation käytössä olevaa tietoa ja varmistua sen oikeellisuudesta. Se myös parantaa kokonaisturvallisuutta pitäen riskit organisaation tiedossa ja näin vähentää yllätyksellisiä löydöksiä ulkoisista auditoinneista. (Ezingeard et al., 2005)

*Strategisten hyötyjen* osalta (Kuva 12) pyritään saamaan pitkän aikavälin etuja ja erottumaan muista kilpailijoista saavutettavan kilpailuedun kautta. Tiedon turvaamisen seurannalla ja raportoinnilla yrityksen johdolle pidetään huolta siitä, että myös johdolla on käsitys ongelmista ja riskeistä. Samalla kun johtoa pidetään tiedon turvaamisesta ajan tasalla, niin he voivat tehdä tarkempaa resurssien ohjausta, sekä näin he pystyvät myös vakuuttamaan muut osakkaat yrityksen liiketoimintojen hyvästä turvallisuustasosta. Omistajat sekä sijoittajat myös pitävät yrityksen hyvää tietoturvatasoa osakkeen arvoa nostavana asiana, koska hyvin varautuneen liiketoiminnan katsotaan olevan paremmin turvassa muutoksilta ja ongelmilta. Toimitusketjujen osana toimittaessa muut ketjun kumppanit arvostavat myös hyvää tietoturvallisuuden tasoa samoista syistä kuin omistajatkin. Havaittavimpana tekijänä strategisista hyödyistä kuitenkin nähdään alhaisemman kustannustason saavuttaminen. Toimintojen pysähtyminen, tietoturvaloukkaus tai vakava häiriintyminen on liiketoiminnalle hyvin kallista. Toimiva tiedon turvaamisen strategia vähentää kustannuksia ja parantaa liiketoiminnan jatkuvuutta, sekä laskee organisaation kokonaiskustannuksia. (Ezingeard et al., 2005)

*Organisatoriset hyödyt* (Kuva 12) ovat osittain päällekkäin strategisten hyötyjen kanssa. Tietoturvaan investoiminen järkevästi nostaa omistajien arvostusta yrityksen toimintaa kohtaan. Tämä voidaan toteuttaa jakamalla käytettävissä olevia resursseja perustuen

tiedon turvaamiseen sijoitettuun tuottoon. Näin toimitaan yleisesti kaikkien muidenkin investointien kanssa liiketoiminnassa, joten tiedon turvaamisesta saadaan samanlainen liiketoiminta-arvon tuotannon väline kuin muistakin investoinneista. Yrityksen johtoryhmä on vastuussa osakkeen arvosta sen omistajille. Hyvällä tiedon turvaamisella arvo pystytään säilyttämään ja jopa kasvattamaan. Tiedon turvaaminen muuttuu liiketoiminnan kilpailueduksi, kun sen avulla erotutaan kilpailijoista. Vaarallinen tai kansalliseen etuun liittyvä liiketoiminta voi myös olla luvanvaraista. Ilman toimintalupaa liiketoimintaa ei voi tehdä. Näissä tapauksissa toimintalupa on ansaittava ja sen epääminen pysäyttää, tai jopa lopettaa liiketoiminnan kokonaan. (Ezingeard et al., 2005)

Kun tietoturva mielletään yrityksen työntekijöiden keskuudessa hyväksi asiaksi, on siinä vaiheessa onnistuttu luomaan organisaatioon tietoturvakulttuuri, joka tukee turvallisuuden toteutumista laajemminkin. Laajasti toteutettuna tietoturva kattaa koko yrityksen toiminnan ja sen hyötynäkökulmat tiedostetaan yrityksen johdossa kilpailutekijänä. Asiakkuuksissa toimintaa aletaan pitämään hyvänä toimittajan ominaisuutena. Näin toteutettuna tietoturvalla tuetaan oman liiketoiminnan menestystä sen hedelmistä nauttivien asiakkaiden keskuudessa ja samalla huononnetaan tietoturvasta heikommin suoriutuvien kilpailijoiden mahdollisuuksia menestyä samassa liiketoimintaympäristössä. (Ezingeard et al., 2005)

Strategisessa tietoturvallisuusjohtamisessa tulee nähdä kokonaiskuva suojauksista ja toimenpiteistä, joita on myös kehitettävä kokoajan paremmiksi. Lakisääteiset vaatimukset, sekä valitut liiketoimintaa sitovat standardit on täytettävä asiallisesti. Tiedon turvaamisstrategian on myös oltava linjassa liiketoimintastrategian kanssa, sekä henkilöstön tulee olla koulutettu soveltamaan luotua strategiaa jokapäiväisessä työssään. (Ezingeard et al., 2005)

# 5. Pohdinta

Tässä luvussa yhteen vedetään kirjallisuuskatsauksen pääteemat liiketoiminnan hyötyjen huomioinnista tietoturvallisuuden hallinnollisessa toteuttamisessa ja pohdiskellaan kunkin teeman merkitystä käytännön näkökulmasta. Samalla nostetaan esiin kuhunkin pääteemaan liittyviä tutkimustarpeita.

## 5.1 Tietoturvallisuus organisaatiossa

Tietoturvaan vaikutetaan tehokkaimmin ihmisten toimintaan vaikuttamalla. Ihmisten toimintaa ohjataan johtamisen keinoilla, millä pyritään luomaan organisaatioon haluttu tietoturvallisuuskulttuuri. Tietoturvallisuuden huomiointi johtamisessa on suuri haaste teknologisen tietoturvallisuuden lähestymistavan omaaville yritysjohtajille. Tietoturvallisuuden mukaan ottaminen organisaation strategiseen suunnitteluun on suuri askel johtajalle, jolla ei ole syvällistä osaamista tietoturvallisuudesta.

Organisaation tietoturvallisuuskulttuuria tulisi kehittää aina yrityskulttuurin rinnalla. Yrityskulttuuria kehitetään jokapäiväisellä toiminnalla ja ohjaavien toimien esillä pitämisellä. Tässä organisaation johdon rooli on hyvin suuri, jotta kaikki mieltävät asian tärkeyden oikein. Tietoturvallisuudesta on luotava organisaatiossa mahdollistaja liiketoiminnan, sekä organisaatiossa toimivien kannalta. Näin luodaan positiivista kuvaa tietoturvallisuuden estävän toimien korostamisen sijasta. Toimintaa estävien ongelmien ratkaisujen tehokkaalla toteuttamisella parannetaan tietoturvallisen toimintatavan hyväksyntää. Tämä vaatii organisaatiolta avointa keskusteluyhteyttä jokaisen organisaatiotason välillä ja on luotavissa yrityskulttuurin kehityksen keinoin.

Yrityksen ylin johto on vastuussa tietoturvallisuudesta. Jos ylin johto ei ole sitoutunut tietoturvallisuuden toteuttamiseen, niin se haittaa ja jopa estää toimivan tietoturvallisuustoiminnan yrityksessä. Ylimmän johdon tehtävänä ei enää ole vain liiketoiminnan kasvattaminen ja siitä huolehtiminen, vaan myös organisaation tietoturvallisuudesta huolehtiminen. *”Ylimmän johdon kiinnostus herää vasta silloin, kun he ymmärtävät jonkun toisen yrityksen saaneen tietoturvasta kilpailuedun tai voittaneen sen avulla asiakkuuksia.”* (R. von Solms, 1996, s.283) Tällöin tietoturvallisuus on siirtynyt johdon ymmärtämälle alueelle ja sitä voidaan alkaa hyödyntämään kuin mitä tahansa muutakin kilpailuetua. *”Johdon kiinnostuessa tietoturvallisuudesta liiketoiminnassa he alkavat vaatimaan vakuuksia, että kontrollit pitävät ja kallis investointi tuottaa oikeata tulosta.”* (R. von Solms, 1996, s.283) Aktivoitunut yritysjohto tukee näin tietoturvallisuuden toteutusta ja tietoturvan ammattilaisten tulee pystyä perustelemaan heille turvaamiseen tarvittavat investoinnit. (R. von Solms, 1996)

Tekniikan kehitys laajentaa tietoturvallisuuden vaikutusaluetta. Yrityksen on huomioitava tämä aina laajentaessaan toimintaansa, tai ottaessaan käyttöön uutta teknologiaa. Sovellettavien tietoturvallisuuden ajatusmallien on toimittava myös uusien tekniikoiden käytön yhteydessä. Tämä vaatii usein lisäkoulutusta ja teknologioiden analysointia tietoturvamielessä ennen niiden käyttöönottoa. Jotta tietoturvallisuuden riskit eivät realisoituisi, on niiden hallintaan varattava riittävästi resursseja. Riskienhallinnan olisi siis tapahduttava jo ennen teknologian käyttöönoton päätöksiä. Päätösten vaikutus on hyvä huomioida strategiassa asti, jos uudella tekniikalla on kauaskantoisia vaikutuksia organisaation toiminnassa.

Henkilöstöhallinnon tulisi olla mukana tietoturvallisuuden kehityksessä, sekä sen ylläpitämisessä hyvin suurella panostuksella. Kuitenkaan tietoturvaa ei mielletä ihmisten

luomaksi ongelmaksi, vaan enemmän tekniseksi ongelmaksi. Tämä vie resursointia yhä enemmän tekniikalla luotavien rajoitteiden suuntaan ja inhimillinen näkökulma jää toisarvoiseksi. Henkilöstön kouluttaminen, kehitystyöhön mukaan ottaminen ja sitouttaminen ovat henkilöstöjohtamisessa olennaisia osa-alueita, joilla pyritään vaikuttamaan organisaation käyttäytymiseen. Luomalla toimiva tietoturvakulttuuri organisaatioon saavutettaisiinkin useimmiten parhaimmat tulokset tietoturvallisuuden kehityksessä. Painotus tulisikin olla enemmän ihmisessä kuin tekniikassa.

Yhtymäkohdat tiedon suojauksen ja yrityksen johdon välillä on pystyttävä näkemään, jotta tiedon suojauksen hyödyt pystytään ottamaan osaksi yrityksen menestymistä. Luomalla tietoturvallisuudesta menestystekijä voidaan parantaa oman yrityksen toimintaedellytyksiä kilpailluilla markkinoilla. Tämän luulisi olevan yritysjohtoa kiinnostava hyötynäkökulma. Yrityksen markkinointi voisi tukea yrityksen liiketoimintaa luomalla omalle markkina-alueelle uuden tarpeen, mikä täytettäisiin oman organisaation hyvin tuotetun tietoturvallisuuden avulla toteutetuilla palveluilla. Näin eriytettäisiin oma toiminta muista huonommin tietoturvaa hoitavien kilpailijoiden toiminnasta ja luotaisiin omasta hyväntasoisesta tietoturvatoiminnasta kilpailuetu. Kun tietoturvallisuudesta olisi luotu haluttava toimittajan ominaisuus, niin kilpailevien yritysten olisi hyvin vaikea haastaa ilman vähintäänkin samalle tasolle yltävää tietoturvatoimintaa. Samalla tietoturvan taso olisi myös lupaus toimittajille, sekä asiakkaille toiminnan laadusta ja liiketoiminnan paremmasta häiriökestävyydestä. Useinkaan tietoturvallisuuden tasoa ei pystytä nopeasti nostamaan. Näin ensimmäisenä tähän markkinatilanteeseen päässeelle jäisi runsaasti aikaa kerätä tulosta asiakkuuksista ja vahvistaa omaa asemaansa markkinoilla.

Koska erityisesti henkilöstöhallinnon ja yritysjohtajien tietoturvaan liittyvän kehitystyön ja tietoturvainvestointeihin liittyvän päätöksenteon merkitys on keskeinen strategista toimintaa tukevan tietoturvakulttuuri kehittämisessä, yhdeksi keskeiseksi tutkimusteemaksi nousee näiden keskeisten tahojen asenteisiin ja päätöksentekoon liittyvien vaikutuskeinojen tarkasteleminen. Tuleva tutkimus voisi edistää tietoturvakulttuurin kehittymiseen vaikuttavien tekijöiden ymmärtämistä esimerkiksi tarkastelemalla onnistuneiden ja epäonnistuneiden tietoturvahankkeiden ominaisuuksia yllä mainittujen sidosryhmien näkökulmasta. Näitä tekijöitä voisi hyödyntää tehokkaiden koulutus- ja yhteistoiminnallisten tietoturvahankkeiden suunnittelussa.

## 5.2 Tiedon turvaominaisuudet ja tiedon arvo

Tiedon turvaominaisuuksien avulla pyritään tiedon arvon säilyttämiseen tai jopa kasvattamiseen. Liiketoiminnassa arvon kasvattamisella pyritään parantamaan tulosta. Tiedon turvaominaisuuksien kautta tiedon arvoa ei yleensä aktiivisesti pyritä kasvattamaan, vaan näkemyksenä on enemmänkin tiedon arvon säilyttäminen ja pyrkimys siihen että arvo ei laskisi. Usein liiketoiminnassa myös haetaan perusteluita tietoturvallisuuden kautta tiedolle ja sen arvolle. Näin tiedon arvon määrittelyssä voidaan nojautua samoihin käsitteisiin, mitä käytetään myös liiketoiminnan johtamisessa. Yhteinen ymmärrys tiedon arvolle luo hyvän perustan suojaustarpeelle ja resursoinnille.

Selkeää arvoa tiedolle ei voida aina määrittää, eikä sille ole aina edes tarvettakaan. Tiedon arvon määritykseen on kuitenkin käytössä useita erilaisia kaavoja joihin sisällytetyt osat koostuvat usein epämääräisistä arvioista. Tiedon arvon ymmärtämiselle kuitenkin voidaan luoda suhteellinen järjestys, minkä avulla saavutetaan suuruusluokaltaan ymmärrettävät suhteet eri tiedolle. Tämä suhteellinen arvo on hyvä ohjaava työkalu määriteltäessä suojaustarpeita, sekä niiden toteutuksen prioriteetteja. Tiedon arvon

analyysin tuloksena syntyvä lista myös toimii kattavana suojauskohteiden listana ja on hyvä apuväline suojaustyötä tekevälle.

Tiedon arvo myös nähdään liiketoiminnan prosesseissa, joiden syvälliseen ymmärtämiseen tarvitaan yrityksen ylimmän johdon osaamista ja ohjausta. Suojauksen resursoinnin ohjauksena tulisi olla riippuvuudet arvon ja sen menetyksen synnyttämässä erotuksessa. Mitä isompi rahamäärä tarvitaan tiedon arvon palauttamiseksi, sitä suuremmat pitäisivät olla myös resurssit tiedon suojaamiselle.

Tiedon turvaominaisuuksien varmistamisella pyritään luomaan luotettava ympäristö tietojenkäsittelylle. Tällaisen ympäristön luomiseksi toteutetaan sipulinkuoren omaisesti suojarakenteita, millä pyritään suojaamaan sipulin ytimessä oleva tietovaranto, eli itse suojattava tieto. Mitä useampi ohut suojakerros on käytössä, sitä vähemmän suojaus näkyy käyttäjälle. Mitä vähemmän tietoturvallisuus näkyy käyttäjälle, sitä paremmin se käytännössä vaikuttaa ja toteuttaa tehtäväänsä.

Tiedon olomuodot tuovat omat haasteensa tietoturvallisuuden pelikenttään. Suojeltava tieto voi olla paperilla, tietokoneen kovalevyllä, tietoliikenteenä verkossa, ihmisen päässä, esineessä muotoiluna, tai vaikkapa ilmassa radiosäteilynä. Tiedon olomuoto määrittelee sen suojausmahdollisuuksien rajoitukset. Vähän käytetty tiedon olomuoto heittää ison haasteen suojauksen suunnittelijalle. Joskus suojauksen suunnittelussa joutuu perehtymään täysin itselle uuteen aihealueeseen, jotta voi suunnitella sille sopivimman suojaustavan.

Tiedon suojaamisen on perustuttava sen olomuodon tukemiseen ja tiedon käytön helpottumiseen, tai ainakin yhtä helppona pitämiseen. Suojaamiskeinon vaikeuttaessa tiedon käsittelyä, ihminen pyrkii suojauksen jotenkin kiertämään ja näin suojauksella aiheutetaan tietoturvatasoon huononnus tavoitellun parannuksen sijasta. Yksittäisten toimijoiden tietoturvallisuusohjeistuksen väärä soveltaminen on myös hyvin vaikeata havaita, koska valittu toimintamalli on usein suojattu paljastumiselta. Kierto toteutetaan usein oman toiminnan tehostamisen vuoksi. Jos käyttäjä vielä tietää, että hän toimii vastoin ohjeistusta, niin ongelmakohtaa ei haluta kiinni joutumisen pelosta edes nostaa esille. Tämän vuoksi on äärimmäisen tärkeää, että kommunikointiyhteys on toimiva jopa arkaluonteisissakin asioissa. Yleensähän suurimmat ongelmat syntyvät tahattomien tai tahallisten virheiden kautta. Jotta ongelmat voidaan mahdollisimman nopeasti korjata, tulee kommunikaation toimia monella tasolla sujuvasti. Tähän ongelmaan voidaan vaikuttaa tiedon jakamista tukevalla yrityskulttuurilla.

Tietoturvallisuuden tärkeys korostuu tietointensiivisissä yrityksissä. Mitä vahvemmin tieto on yrityksen liiketoimintaprosessissa syötteenä, liiketoimintaprosessien käsittelyssä mukana ja lopputuotteena, sitä tietointensiivisempi yritys on. Tiedon arvon säilymisellä on näinollen suurempi merkitys ja tiedon turvaominaisuuksien suojaamiseen voidaan enemmän panostaa.

Tiedon turvaominaisuuksien varmistaminen koko tiedon elinkaaren ajan on toiminto, mihin pyritään tietoturvajohtamisen keinoin. Kaikki tietoturvallisuuden toteuttamisessa perustuu tähän oletukseen. Tiedon turvaominaisuuksien suojaamisen avulla tieto pysyy sen omistajalle arvokkaana. Tiedon arvo myös tukee suojaustoimenpiteiden kustannuksia, eli siis ruokkii näin itseään. Mitä arvokkaammasta tiedosta on kyse, sitä enemmän sen turvaominaisuuksien suojaamiseen kannattaa sijoittaa yrityksen resursseja. Toiminnalla varmistetaan näin yrityksen arvon tuotantoa, mikä on jokaisen yrityksen olemassaolon perusta.

Tietoturvallisuuden suojauskeinojen käytettävyys tulee huomioida. Inhimillisten ominaisuuksien huomioiminen parantaa suojauksen käyttöastetta, ellei sitä ole toteutettu toimintoja täysin estäväksi. Ihmisten toiminnan kautta syntyvien uhkien osuus on merkittävä suhteessa muihin tietoturvallisuuden osa-alueisiin. Tämän tulisi ohjata myös tietoturvallisuuden resurssien painotusta organisaatiossa enemmän ihmisten toiminnan aiheuttamien uhkien hallinnointiin. (Schultz, Proctor, Lien, & Salvendy, 2001)

Tiedon arvon ja siihen liittyvien turvaominaisuuksien määrittely on haasteellinen tehtävä erityisesti isoissa ja toiminnoiltaan hajautuneissa organisaatiossa, koska se edellyttää syvällistä substanssitietoutta useilta eri liiketoiminnan osa-alueilta. Tästä syystä tiedon arvon ymmärtämisessä ja priorisoinneissa voi olla merkittäviä eroja liiketoiminnan kannalta kriittisten toimijoiden kesken. Tätä kautta nousee esiin mielenkiintoinen näkökulma tutkimukselle tarkastella eri käyttäjien välisten arvojen ja priorisointien eroja ja tiedon suojaamiseen liittyviä arvoristiriitoja. Näiden usein substanssisidonnaisten arvokäsitysten ymmärtäminen tarjoaa tärkeää tietoa tietoturvan kehittämiseen liiketoiminnan näkökulmasta.

## 5.3 Inhimilliset tekijät tietoturvallisuudessa

Inhimilliset tekijät on huomioitava tietoturvallisuuden hallinnassa. Koska tietoturvallisuuden suurimmat ongelmat pohjautuvat ihmisten toimintaan on siihen pyrittävä vaikuttamaan mahdollisimman paljon. Yksittäisten ihmisten tekeminen on ymmärrettävä koko organisaation ongelmaksi. Tietoturvakulttuurin kehittämisellä pyritään vaikuttamaan kollektiiviseen toimintaan koko organisaation sisällä. Toimintaan vaikutetaan johtamisesta tutuilla keinoilla, joten organisaatioista usein löytyy tähän runsaasti tekijöitä, eikä tietoturvallisuudesta vastaavan henkilön tulekaan tehdä kaikkea yksin. Tietoturvallisuudesta on myös jaettava vastuuta kaikille, koska sen toteuttaminen on kaikkien vastuulla. Yksilö saadaan toimimaan tietoturvallisesti hyvän johtamistyön keinoilla.

Kommunikoinnilla, tietoturvatietoisuudella ja johdon tuella tietoturvatyölle saavutetaan parhaimmat tulokset organisaation tietoturvakäyttäytymisessä. Koska kyseessä ovat johtamisen keinot, niin niiden soveltaminen on motivoitava koko organisaatioon. Ei voi olla niin, että yhdellä tasolla tietoturvallisuudelle naureskellaan, toisella haukutaan ja kolmannella pidellään kiukkua toimimattomien tietoturvarajoituksien vuoksi. Tällöin tietoturvallisuus on toiminut, mutta johtaminen ei. Johdon ei tarvitse tukea liiketoimintaa hankaloittavaa tietoturvatyötä, vaan heidän tulee haastaa tietoturvan ammattilaiset toteuttamaan riskien hallintatyö liiketoimintaa tukevalla tavalla.

Myöskään mattoa ei voi vetää tietoturvallisuudesta vastaavan alta tekemällä tietoturvaa selkeästi loukkaavia päätöksiä. Tällöin johto ei osoita tukea tietoturvallisuustyölle, vaan vähentää sen merkitystä ja aiheuttaa näkyvän kolhun motivaatioon, sitoutumiseen, kommunikointiin, yhteistyöhön, sekä johdonmukaisuuteen. Kaikki tietoturvallisuuden inhimillisten tekijöiden osa-alueet on pidettävä kunnossa, jotta tietoturvakulttuuria pystytään parantamaan organisaatiossa.

Inhimillisten tekijöiden ollessa suurimpia vaikuttajia tietoturvallisuudessa, niiden vaikutusta suojauskeinojen tehokkuuden parantamiseen tulisi edelleen tutkia. Inhimillisten tekijöiden ollessa suurena osana käyttäjien kokemaa käytettävyyttä, tulisi tätä pyrkiä tutkimaan myös osana hallinnollista tietoturvatoimintaa. Inhimillisten tekijöiden vaikutus tietoturvallisuuden johtamiseen on tärkeä osata, jotta tietoturvallisuuden vaikutusta pystyy jatkuvan kehittämisen keinoin parantamaan organisaatiossa.

## 5.4 Riskien hallinta

Tietoturvallisuuden resurssien ohjaamisessa tulisi olla käytössä järjestelmälliset keinot, minkä avulla uhkien kustannukset huomioiden voidaan keskittää panostukset oikeisiin suojauskeinoihin (Sawik, 2013). Varantojen liiketoiminta-arvot tulisivatkin olla riskienhallinnan resursoinnin pohjana. Panostamalla oikeisiin asioihin tuetaan liiketoiminnan etua ja parannetaan kannattavuutta. Tällöin resursseja ei hukata ja asiakkaille näkyvät kustannukset pystytään pitämään alhaisina. Alhaisten kustannusten avulla voidaan taas saavuttaa strateginen etu kilpailijoihin verrattuna, missä joko parannetaan liiketoiminnan katetta tai kilpaillaan hinnalla omassa markkinassa. Hyvin hoidetulla ja strategiselle tasolle viedyllä tietoturvatyöllä siis voidaan hyvinkin edistää liiketoiminnan edellytyksiä menestyä.

Tietoturvallisuuden hallinnassa olennaisinta on oikein mitoitettu organisaation suojaaminen uhkilta ja haavoittuvuuksilta *(Loser et al., 2011)*. Tällä pyritään mitoittamaan resurssit oikein, jotta liiketoiminnan muut toiminnot eivät kärsisi liiallisista tietoturvainvestoinneista tai toteutuneista tietoturvapoikkeamista. Mitä kriittisempi varanto on liiketoiminnalle, sitä paremmin se tulisi suojata. Varantojen määritys siis tulee tehdä huolellisesti, jotta niiden arvo nähdään suhteessa muihin varantoihin. Kattava lista varannoista onkin tärkeämpää kuin kattava riskilista, sillä ilman identifioituja varantoja ei voi nähdä kaikkia riskejä, eikä ymmärretä mitä pitäisi suojata. Tällöin ollaan helposti tilanteessa, missä ei tiedetä mitä suojataan ja toteutetaan vain valitun standardin vaatimuksia sokkona. Näin saadaan auditoijat kyllä vakuuttuneeksi suojauksista, mutta itse liiketoiminta tai sen osa voi jäädä kokonaan suojaamatta.

Resurssien ohjaaminen liiketoiminnan uhkien painotuksien mukaan säästää selvää rahaa. Ohjaus liiketoiminnan johdolta on myös helpommin saatavissa perustelemalla tietoturvainvestoinnin kulua suhteessa sen tuotto-odotuksiin. Tämän näkökulman toivoisi siirtyvän myös auditointikriteeristöjen sisältöihin suuremmalla painotuksella. Liiketoiminnan tietoturvasuunnittelun lähtökohdat tulisi olla ensiarvoisen tärkeitä myös ulkoisten tarkistuksien kannalta. Tietoturvallisuuden toteutuksessa on tärkeämpää identifioida ja suojata varannot, kuin robottimaisesti toteuttaa pitkä lista vaatimuksia. Tähän sudenkuoppaan on astuttu useissa standardeissa, eikä KaTaKri ole tässä mielessä poikkeus. Tietoturvainvestointien tuotto-odotukset ja riskien hallinnan standardien vastaavuus käytännön tarpeisiin muodostaa mielenkiintoisen jatkotutkimusaiheen.

## 5.5 Tietoturvallisuuden hallinnan formalisointi

Tietoturvallisuuden standardien tulisi ohjata soveltajiaan liiketoimintalähtöiseen tietoturvallisuuden rakentamiseen, eikä pyrkiä vain kehittämään listaa tarvittavista suojauksista. Kustakin tämän tyylisestä standardista on helposti löydettävissä ohjauksia, jotka toimivat liiketoiminnan hyötyjen vastaisesti. Tämän tyylisiä toteutuksia ei tulisi toteuttaa, vaan ne tulisi määritellä uudelleen siten, että ne soveltuvat liiketoimintaan täydellisesti. Auditoijan tehtäväksi jää näin purkaa liiketoiminta ja sen suojausmenettelyt, sekä varmistaa että ympäristössä sovelletaan vaatimusten henkeä. Usein kuitenkin auditoijalta puuttuu ymmärrys itse suojattavasta liiketoiminnasta, joten tehtävä jää auditoitavan organisaation kontolle saada auditoija ymmärtämään vaatimuksen ongelma ja siihen sovellettu vaatimuksesta poikkeava toteutus.

Tietotuvallisuuden standardeissa eri suojattavien varantojen yhtymäkohtien kautta on koottava lista uhkista ja niihin on toteutettava liiketoimintaa tukevat suojauskeinot. Kriteeristöjen merkitys voisikin olla irrallisten vaatimusten sijasta enemmän varantojen

määrittelyssä, sekä suojauskeinojen vaikuttavuuden määrittelyssä, jotta itse soveltaminen jäisi organisaation vastuulle koska siellä on paras kokonaisuuden ymmärrys.

Riskien hallinnan lähtökohtana toimiva liiketoimintaprosessien kautta varantojen määrittely on haasteellista, koska sovellettavat standardit eivät huomio erilaisia liiketoiminnan muotoja riittävällä tavalla. Onnistunut tietoturvallisuuden riskienhallinnan pohjatyö vaatii vahvaa osaamista sekä liiketoimintaprosesseista, riskien hallinnasta, sekä tietoturvallisuudesta. (Sadok & Spagnoletti, 2011) Liiketoiminnan tuntemisen ja sen hyväksikäyttäminen tietoturvallisuuden huolellisessa toteuttamisessa on sen kriittinen onnistumistekijä. Huolehtimalla tietoturvatietämystä johdon tasolle, sekä tietoturvallisuuden omistajalle liiketoimintatietämystä, saavutetaan parhain yhdistelmä laadukkaalle tietoturvallisuudelle organisaatiossa.

Tietoturvallisuuden hallintajärjestelmää määriteltäessä standardeja tulisi pitää vain välillisesti ohjaavina työkaluina. Itse toteutuksen ei tulisi koskaan noudattaa kirjaimellisesti standardia, vaan sen tulisi tukea täysin liiketoimintaa. Standardissa kuvattu vaatimus ei saa koskaan vaikuttaa negatiivisesti liiketoimintaan. Miten tällaista voisi edes perustella liiketoiminnan johdolle? Standardin soveltamisella pyritään määrittelemään tavoitetila prosessille minkä lopputuloksena on liiketoiminnan kannalta toimiva kokonaisuus. Usein liiketoiminnan johdon asettama lähtökohta on kuitenkin vain standardin toteuttaminen, eikä liiketoiminnan suojaaminen. Tämä voi helposti johtaa sellaisen tietoturvallisuuden hallintajärjestelmän toteutukseen, mikä ei sovellukaan kyseiseen liiketoimintaan. Tällöin panostukset on tehty standardin saamiseksi, eikä liiketoiminnan suojaamiseksi. Tavoiteasetanta voidaan todeta organisaation kannalta tällöin vääräksi.

Paluu liiketoiminnan perusteisiin on syytä tehdä tässä vaiheessa. Liiketoiminnan kantava ajatus on aina luoda voittoa omistajille. Jos formalisoinnilla haetaan liiketoiminnalle haittoja, niin liiketoiminnan tie tulee olemaan kivikkoinen. Formalisoinnilla tulee hakea etuja liiketoimintaan, jotta se yleensäkään kannattaa tehdä. Yhtenäistämällä tietoturvallisuuden toimintoja voidaan saavuttaa synergiaetuja yhteistyökumppaneitten, alihankkijoiden, sekä organisaation sisäisten yksiköiden välillä. Etuja voidaan saavuttaa myös yrityskauppojen yhteydessä, missä formalisointi toimii liiketoimintojen yhdistämisessä vauhdittajana.

Sijoitus formalisointiin on myös nähtävänä sijoituksena liiketoiminnan kehitykseen. Pelkkä standardin saavuttaminen ei palvele liiketoimintaa, kuin myyntimielessä vähäisessä määrin. Tavoitteiden asettaminen tulee toteuttaa niin, että investointi tuottaa liiketoiminnalle tuloa ja sitä pitää pystyä seuraamaan. Näin suurikin investointi voidaan nähdä panostuksena liiketoimintaan ja sitä voidaan tarkkailla yrityksen johdossa samoin eväin kuin muitakin investointeja.

Liiketoimintahyöty formalisoinnista on jäätävä yrityksen käytettäväksi mm. parantaen liiketoiminnan häiriönsietoa, tukemalla yhteistyökumppanien arvostamaa toimitusvarmuutta, parantaa yhteistyökykyä liiketoimintaverkostoissa, mahdollistaa liiketoimintaa suuren riskin liiketoiminta-alueilla, sekä varmistaa tuotantoketjujen osien toimintavarmuutta. Liiketoimintahyöty on näin mitattavissa ja se konkretisoituu viimeistään silloin, kun liiketoiminta kohtaa häiriöitä. Panostukset tietoturvallisuuteen on nähtävä investointina, joilta odotetaan liiketoiminnalle hyötyä. Hyöty on häiriötilanteissa mitattavissa esimerkiksi häiriön vaikutuksen laajuuden ja keston mittareilla. Mitä isompi häiriö kyseessä on ja mitä kauemmin se kestää, sitä enemmän siihen on syytä etukäteen panostaa. Investointi tietoturvallisuuteen palauttaa rahaa häiriötilanteen ennakoimisena, häiriön sietämiskyvyn kasvamisena, tai häiriön keston sekä sen vaikutuksien

vähäisyytenä. Yksinkertaista kaavaa kustannussäästöjen laskemiselle ei ole, mutta yleisimmin käytettyjä ovat miestyötuntien, sopimussakkojen, materiaalituhojen, maineen, sekä asiakkuuksien menettämisen kautta arvioitavat tulojen menetykset.

Standardien toteutuksien tarkistuksissa ei koskaan oteta kantaa siihen miten liiketoimintaa on jouduttu muuttamaan standardin soveltamiseksi, eikä sitä ovatko muutokset olleet hyviä. Usein muokattu liiketoimintaprosessi käytännössä oikoo siihen huonosti sopivaa suojausta ja aiheuttaa enemmän tietoturvaloukkauksia, kuin parannuksia. Standardin toteutuksen yhteydessä tehtyjen liiketoiminnan prosessien muutosten tarkistamisella saataisiin parempi kuva siitä onko standardia sovellettu liiketoimintaan oikein, vai onko standardia vain sovellettu sokeasti. Hyvä suojaus saavutetaan ymmärtämällä sekä liiketoimintaprosessit, niiden toteutustaso, sekä tietoturvallisuus samalla kertaa. Tämä ei onnistu vain keskustelemalla joko johdon tai toteutusportaan kanssa, vaan siihen tarvitaan kaikkien osapuolten tietämyksen yhdistämistä.

Koska kaikki toiminta suojattavissa ympäristöissä on aina inhimillisen käyttäytymisen aikaansaannosta, ongelmaa ei ole riittävästi huomioitu tietoturvatutkimuksessa. Olisi loogista tehdä tutkimusta enemmän niistä asioista, joilla voidaan parhaiten vaikuttaa tietoturvallisuuteen, eli henkilöstöturvallisuuden osa-alueeseen. Henkilöstön toimintaan vaikuttamisesta tietoturvakulttuurin rakentamisella tulisi olla paljon tutkimusta, jotta sen soveltaminen olisi helpompaa organisaatioissa. Tietämys tältä alueelta puuttuu usein kokonaan, tai on hyvin puutteellista. Henkilöstöjohtajien osaamisalueeseen kun eivät niinkään kuulu tietoturvallisuuden osa-alueet, vaan henkilöstöjohtajaksi kasvetaan organisaation johdon kautta. Yleisesti henkilöstöjohtajan koulutustausta onkin kaupallisten aineiden suunnalla. Osoittaako tämä, että johtamisen koulutusohjelmissa ei ole ymmärretty tietoturvallisuuden olevan myös tärkeä osa henkilöstöjohtamista?

Tutkimukseen valitut tietoturvallisuuden kriteeristöt vaativat tietoturvallisuuden hallinnan toteutusta liiketoiminnan tueksi, mutta eivät vaadi sitä toteutettavaksi osaksi strategista liiketoimintaa. Vaatimus on tältä osin löyhä ja sen tulkinta riippuu tarkastelijan kyvystä ymmärtää tietoturvan strategisia ja liiketoiminnallisia puolia. Vaatimukset ovatkin lähinnä tarkistuslistoja eivätkä siten vaadi auditoijaa käymään läpi riskienhallinnan kautta tehtyä varantojen suojaamista, kuten tietoturvallisuuden periaatteissa olisi tavoitteena. Tämä vaarantaa tietoturvan hyötynäkökulman ja kasvattaa johdon ja tietoturvallisuuden välistä ymmärtämisen kuilua, sekä heikentää suojauksien toteutuksien osuvuutta kohdeorganisaation varantoihin.

Tuleva tietoturvan hallinnan tutkimus voisi selvittää, miksi kriteeristöjen suojauskeinot eivät ole varantoihin perustuvia. Liiketoimintalähtöisessä riskianalyysissä huomioidaan liiketoiminnan prosessit, toteuttavat tekijät, sekä kaikki liiketoiminnan liityntäpinnat toimitusketjuineen. Riskianalyysissä analysoidaan liiketoimintaprosessit ja niiden toimintaedellytykset riskin toteutuessa sekä määritellään toiminnan mahdollistavat vähimmäistekijät. Kun tiedetään, mitä resursseja ja varantoja prosessissa minimissään tarvitaan, niin voidaan merkitä ne kriittisiksi. Liiketoiminnalle kriittisille varannoille suunnitellaan suojauskeinot. Kriteeristön tulisi olla siis sellainen, missä lähtökohtana olisivat organisaation riskienhallinnan prosessit ja ohjattaisiin suojauskeinojen valinnassa antamalla uhkakuvat käyttöön suojauksia suunnitteleville asiantuntijoille. Näin kriteeristöt eivät rajoittaisi suojauskeinojen toteutusta, tai liiketoiminnan toimintamahdollisuuksia ja pohjautuisivat tietoturvallisuuden perusteisiin yksittäisten ongelmakohtien ratkaisun sijasta. Kriteeristöjä luovilla organisaatioilla on yleensä kattava käsitys uhkakuvista, joten niitä päivittämällä päivittyisivät myös toteuttavien organisaatioiden suojaukset oikeilta osiltaan. Näin toteutusten kustannukset myös

pysyisivät kurissa, kun organisaatio voisi luoda omaan liiketoimintaansa sopivat keinot varantojen suojaukselle.

Yksi suurimpia tietoturvallisuuden toteutuksen kompastuskiviä on käytettävyyden ja tietoturvallisuuden välinen suhde. Aina on mahdollista kieltää jotain tietoturvan nimissä, mutta miten se mahdollistettaisiin tietoturvallisesti ja siten, että se jopa tukisi tehtävää toimintaa? Ongelmana onkin totuttujen toimintojen estäminen, vaikka todellisuudessa tietoturva tulisi nähdä enemmänkin mahdollistajana. Tietoturvallisuuden käytettävyyteen tulee panostaa, jotta siitä ei tulisi tietoturvallisten toimintatapojen tai järjestelmien käytön estäjä (Schultz et al., 2001). Myös tämä tietoturvallisuuden erityispiirre tarjoaa mielenkiintoiseen jatkotutkimuskohteen.

## 5.6 Strateginen tietoturvallisuusjohtaminen

Strategisessa tietoturvallisuuden johtamisessa on nähtävä kokonaiskuva suojauksista ja toimenpiteistä. Näitä on seurattava ja kehitettävä kokoajan paremmiksi. Tietoturvallisuuden hallintatyö ei lopu organisaation toiminnan osana koskaan. Parhaiten tietoturvallisuuden strategista ohjaamista toteutetaan organisaation johtoryhmän tasolla, jolloin se tulee osaksi yrityksen johtamisen käytäntöjä ja siitä saadaan paras hyöty yrityksen liiketoiminnan käyttöön.

Tietoturvallisuusstrategia tulee toteuttaa liiketoiminnan strategian yhtenä osana. Liiketoiminnan tulee ottaa huomioon tietoturvan tarjoamat mahdollisuudet ja käyttää tietoturvallisuuden strategisessa ohjaamisessa hyväksi liiketoiminnan strategian suuntaa. Liiketoiminta ei voi ummistaa silmiään tietoturvallisuudelta, vaan sen on käytettävä sitä tietoa hyväksi mitä tietoturvallisuus yrityksessä luo. Liiketoiminnan strategisessa ohjauksessa voidaan hyödyntää tietoturvallisuuden avulla luotuja mahdollisuuksia toimia uusissa toimintaympäristöissä, tai kontrolloida paremmin toimintaympäristön riskejä. Liiketoiminnassa tietoturvallisuuden hyväksikäyttö tulisi olla istutettuna päätöstenteon ytimeen, missä käytettävään liiketoiminnalle kriittiseen tietoon ja riskianalyyseihin perustuen kyetään tekemään parempia päätöksiä liiketoiminnan suunnasta. Tuleva tutkimus voisi tähän liittyen tarkastella onnistuneita ja epäonnistuneita tietoturvallisuuteen liittyviä päätöksentekoprosesseja ja niiden yhtymäkohtia yrityksen liiketoiminnan tarpeiden huomioimiseen.

Tietoturvallisuuden avulla yritys voi hakea sellaisia toimintamalleja liiketoiminnalle, mitkä eivät olisi mahdollisia toteuttaa ilman toimivaa ja kokonaisvaltaista tietoturvallisuuden tarjoamaa suojaa (Ezingeard et al., 2005). Näkemykseen tietoturvallisuuden estävästä voimasta voidaan vaikuttaa inhimilliset tekijät huomioivilla tietoturvaprojektien toteutustavoilla. Suojauksien toteutuksessa on huomioitava niiden käytettävyys ja käyttäjiä on hyvä motivoida tietoturvatietoisuuden keinoilla, sekä rakentamalla yrityksen sisälle toimiva tietoturvallisuuskulttuuri.

Organisaation johdon ja tietoturvallisuuden välille on rakennettava toimintamalli, missä kommunikointi toimii ja tietoturvaan sijoitetut resurssit käsitellään kuten mitä tahansa muutakin liiketoiminnan investointia. Investointien, investointiodotusten ja riskien välillä ei kuitenkaan ole käytettävissä selkeää kaavaa mitä soveltamalla tietoturvallisuuden investoinnit olisi selkeästi perusteltuja. Yleisesti käytössä olevissa kaavoissa on aina arviotekijöitä, joiden kautta luvut muuttuvat haluttuun suuntaan. Investointilähtöinen tietoturvallisuuden resursointi tarjoaisi siis mielenkiintoisen jatkotutkimuskohteen.

# 6. Johtopäätökset

Tässä kirjallisuuskatsauksessa tarkasteltiin eri näkökulmia tietoturvallisuuden hallinnollisessa toteuttamisessa liiketoiminnan hyötyjen näkökulmasta. Aikaisemmasta kirjallisuudesta löydettiin kuusi laajaa aihepiiriä, jotka osoittavat keskeisiä periaatteita ja toimintatapoja, jotka tulisi huomioida liiketoimintalähtöisen tietoturvallisuuden toteuttamisessa: tietoturvallisuus organisaatioissa, tiedon turvaominaisuudet ja tiedon arvo, inhimilliset tekijät tietoturvallisuudessa, riskien hallinta, tietoturvallisuuden hallinnan formalisointi ja strateginen tietoturvallisuusjohtaminen.

Käsiteltyjen aihepiirien pohjalta esitettiin yleisiä toimintasuosituksia ja jatkotutkimusaiheita havaittujen tietoturvan hallinnan haasteiden ymmärtämiseksi ja organisaatioiden toiminnan kehittämiseksi. Kirjallisuuskatsaus osoitti, kuinka tietoturvallisuus nähdään usein vievän organisaatioiden ja käyttäjien voimavaroja ja estävän tekemistä. Tämä on viite siitä, että tietoturvallisuuskulttuurissa ja johtamisessa olisi paljon parantamisen varaa. Tutkimuksessa tuotiin esille, kuinka tietoturvallisuuden, liiketoiminnallisten hyötyjen ja käytettävyyden välisen taistelun pitäisi kirvoittaa tutkimusta käsittelemään niiden suhdetta syvemmin. Erityisesti tutkimuksen tulisi entistä enemmän keskittyä niihin asioihin, jotka vaikuttavat ihmisen toimintapäätöksien tekemiseen, koska sieltä syntyvät suurimmat tietoturvaongelmat. Yksilön käyttäytymiseen vaikuttamalla voidaan parantaa tehokkaimmin organisaation tietoturvallisuuden tasoa. Tähän isoissa organisaatiossa on käytössä henkilöstöhallinnon organisaatio, minkä yhdeksi keskeiseksi tehtäväksi tulisikin nostaa tietoturvallisuuden parantaminen yhteistyössä organisaation eri sidosryhmien kanssa.

# 7. Lähteet

Alavi, R., Islam, S., & Mouratidis, H. (2014). *A conceptual framework to analyze human factors of information security management system (ISMS) in organizations*

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. *International Journal of Information Science and Management, 11*(SPL.ISS.), 111-126.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati, F., & Kim, T. -. (2014). A layered trust information security architecture. *Sensors (Switzerland), 14*(12), 22754-22772.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3–4), 189-198. doi:http://dx.doi.org/10.1016/j.cose.2008.11.007

Eloff, M. M., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers & Security, 19*(3), 243-256. doi:http://dx.doi.org/10.1016/S0167-4048(00)88613-7

Ezingeard, J. -., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. *Information Systems Management, 22*(2), 20-29.

Gutiérrez-Martínez, J., Núñez-Gaona, M. A., & Aguirre-Meneses, H. (2015). Business model for the security of a large-scale PACS, compliance with ISO/27002:2013 standard. *Journal of Digital Imaging,*

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hussein, A. A., Ghoneim, A., & Dumke, R. R. (2011). *An approach for securing and validating business processes based on a defined enterprise security ontology criteria*

Loser, K., Nolte, A., Herrmann, T., & te Neues, H. (2011). Information security management systems and socio-technical walkthroughs. *Socio-Technical Aspects in Security and Trust (STAST), 2011 1st Workshop On,* 45-51.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information* Wiley New York, NY.

Rantapelkonen, J., & Salminen, M. (2013). The fog of cyber defence. *Julkaisusarja 2.Artikkelikokoelma N: O 10,*

Reid, R. C., & Gilbert, A. H. (2010). Using the parkerian hexad to introduce security in an information literacy class. *Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10,* 45-47.

Sadok, M., & Spagnoletti, P. (2011). A business aware information security risk analysis method. *Information Technology and Innovation Trends in Organizations - ItAIS: The Italian Association for Information Systems,* 453-460.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems, 55*(1), 156-164. doi:http://dx.doi.org/10.1016/j.dss.2013.01.001

Schultz, E. E., Proctor, R. W., Lien, M., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security, 20*(7), 620-634. doi:http://dx.doi.org/10.1016/S0167-4048(01)00712-X

Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security, 26*(4), 290-299. doi:http://dx.doi.org/10.1016/j.cose.2006.11.005

Sipior, J. C., & Ward, B. T. (2008). A framework for information security management based on guiding standards: A united states perspective. *Issues in Informing Science & Information Technology, 5*, 51-60.

*Valtionhallinnon tietoturvasanasto* (2008). . Helsinki: Edita Prima Oy. Retrieved from https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10128&groupId=10229

von Solms, R. (1996). Information security management: The second generation. *Computers & Security, 15*(4), 281-288. doi:http://dx.doi.org/10.1016/0167-4048(96)88939-5

Von Solms, S. H. (2005). Information security governance - compliance management vs operational management. *Computers and Security, 24*(6), 443-447.