Jiri Vidgren

# KYBERTURVALLISUUS YRITYSSTRATEGIASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

# TIIVISTELMÄ

Vidgren, Jiri
Kyberturvallisuus yritysstrategiassa
Jyväskylä: Jyväskylän yliopisto, 2019, 37 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Palonen, Teija

Kyberturvallisuuden integroiminen osaksi yrityksen kaikkia toimintoja, henkilöstön kouluttaminen ja tietoisuuden lisääminen vaativat yrityksen korkeimman johdon vastuunkantoa ja sitoutumista. Yritysjohdon tärkeimpänä työkaluna yrityksen ohjaamiseen on yritysstrategia, joka on yrityksen kattavin kokonaissuunnitelma siitä, miten yritys suorittaa kokonaistehtäväänsä, eli missiota. Tämän kirjallisuuskatsauksena toteutetun tutkielman tarkoituksena on selvittää, miten kyberturvallisuus ilmenee yritysstrategiassa ja millaisia hyötyjä kyberturvallisuuden integroinnilla yritysstrategiaan voidaan saavuttaa. Tutkielmassa tarkastellaan kyberturvallisuuden implementointia yritysstrategiaan, yrityksen johdon ja henkilöstön roolia tässä jatkuvaluonteisessa prosessissa sekä yritysjohdon sitoutumista ja vastuunkantoa. Tutkielmassa luodaan katsaus kyberturvallisuuden yritysstrategisen implementoinnin vaikuttavuuden arviointiin ja saavutettaviin hyötyihin. Kyberturvallisuuden implementointi yrityksen kokonaisstrategiaan viestii tehokkaalla tavalla koko yritysorganisaation henkilöstölle, että ylin johto on vastuullisesti sitoutunut yrityksen kyberturvallisuuden jatkuvaan ylläpitoon ja kehittämiseen. Kyberturvallisuuden yritysstrategisesta integroinnista saavutettavista hyödyistä keskeisimpiä ovat yrityksen parantunut suojaus kyberhyökkäyksiä vastaan, kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa, valmius kohdata häiriöitä ja kriisejä sekä koko organisaation tasoinen tietoisuus yrityksen kyberturvallisuudesta. Muita hyötyjä ovat muun muassa yritysimagon parantuminen ja sitä kautta vaikutukset yrityksen arvostukseen myös osakemarkkinoilla.

Asiasanat: kyberturvallisuus, tietoturvallisuus, yritysstrategia, strateginen suunnittelu

# ABSTRACT

Vidgren, Jiri
Cyber Security in Corporate Strategy
Jyväskylä: University of Jyväskylä, 2019, 37 pp.
Information Systems, Bachelor's thesis
Supervisor: Palonen, Teija

Integrating cyber security to all functions of the enterprise, educating the personnel and increase awareness demands accountability and commitment from the top management of the organization. The most important tool of top management to steer the enterprise direction is corporate strategy, which is the most comprehensive plan about the execution of the overall mission. The purpose of this research conducted by literature review, is to clarify how the cyber security occurs in the corporate strategy and which kind of benefits are achievable by integrating cyber security in to the corporate strategy. In this research, we examine the occurrence of cyber security in corporate strategy, the role of the top management and the personnel of the enterprise in this sustained process as well as review the commitment and accountability of the top management. In addition, we create an overview to impact assessment and achievable profits of strategic implementation of cyber security. Implementing cyber security to corporate strategy communicates effectively to the personnel of the enterprise, that the top management is responsibly committed to continuous maintenance and development of cyber security in the enterprise. The clearest profits from the implementation of cyber security into the corporate strategy are improved resilience and the enterprise-wide awareness of the cyber security. Other profits are improved company public image and the effects from that regarding the valuation of the company in the stock exchange.

Keywords: cyber security, information systems security, corporate strategy, strategic planning

## KUVIOT



## TAULUKOT

**SISÄLLYS**

# 1 JOHDANTO

Yhteiskuntaamme, talouttamme ja kriittistä infrastruktuuriamme ylläpitävät yritykset ovat laajalti riippuvaisia tietoverkoista ja informaatioteknologisista ratkaisuista (Jang-Jaccard & Nepal, 2014). Näihin yrityksiin kohdistuu jatkuvasti uusia turvallisuusuhkia niin ulkopuolelta kuin yritysten sisältäkin (Conti, Dargahi & Dehghantanha, 2018), eivätkä turvallisuusuhkat rajoitu pelkästään fyysiseen maailmaan, vaan yhä useampi uhka yritystoiminnalle ilmenee yrityksen digitalisoituneen ja verkottuneen toimintaympäristön kautta (Choo, 2011). Yritysten jatkuvasti teknologisoituvassa toimintaympäristössä tulee huomioida kyberturvallisuuden rooli sisäänrakennettuna ja integroituna osana yrityksen strategiaa eikä vain teknisenä toteutuksena (Islam & Stafford, 2017). Jang-Jaccardin ja Nepalin (2014) mukaan kyberhyökkäykset tulevat tulevaisuudessa rikollisille houkuttelevammaksi ja kohteilleen tuhoisimmiksi, kun yritysten riippuvuus informaatioteknologiasta kasvaa entisestään. Kim (2017) näkee kyberhyökkäysten yleistymisessä hyvääkin, sillä se kasvattaa tietoisuutta uhkista ja sitä kautta edistää rahoituksen sekä resurssien kohdentamista organisaation kokonaisvaltaisen kyberturvallisuuden rakentamiseen.

Kyber- ja tietoturvallisuus nähdään usein yritysstrategisella tasolla vain teknisenä asiana, jonka toteuttaminen jää yrityksen tietohallinnon vastuulle (von Solms, 2011; Siponen & Oinas-Kukkonen, 2007; Siponen, Mahmood & Pahnila, 2014; Rothrock, Kaplan & van der Oord, 2018). Yritysten tietohallinto on perinteisesti ylläpitänyt ja vastannut vain yrityksen tietopääoman turvaamiseen keskittyvistä tietoturvallisuuskäytänteistä. Nämä eivät ole riittäviä toimia vastaamaan modernien, ubiikkien tietojärjestelmien turvaamiseen ja suojaamiseen liittyviin haasteisiin (Alreemy, Chang, Walters & Wills, 2016.) Kokonaisvaltaisempia uhkia varten yrityksissä on tarpeen implementoida kyberturvallisuusstrategia, joka ajantasaistaa yrityksen kybertoimintaympäristön, sekä mahdollistaa sen luotettavuuden ja toiminnan turvaamisen (Kayworth & Whitten, 2012).

Kyberturvallisuusstrategian implementointi osaksi yritysstrategiaa mahdollistaa selkeitä, mitattavissa olevia suoria hyötyjä, joita Khansan & Liginlalin (2009) mukaan ovat kyber- ja tietoturvallisuuden parantuminen yrityksen toiminnoissa, ja siitä seuraavia välillisiä hyötyjä esimerkiksi asiakas- ja henkilöstötyytyväisyys sekä yritysimagon paraneminen, joka omalta osaltaan tukee jopa yrityksen arvonnousua.

Tutustuessa kyberturvallisuutta ja yritysstrategiaa käsittelevään kirjallisuuteen havaittiin, että tutkimustietoa kyber- ja tietoturvallisuudesta sekä yritysstrategiasta on erikseen saatavilla paljon, muttei juurikaan monitieteellisesti konvergoituna tutkimuksena. Monitieteellinen lähestymistapa on Lehdon ja Kähkösen (2015a) mukaan hyvin tyypillistä nimenomaisesti kyberturvallisuuden tutkimuksessa, sillä kyberympäristöt koskettavat modernia yritystoimintaa yrityksen koosta ja toimialasta riippumatta.

Tämän kirjallisuuskatsauksena toteutettavan tutkielman tarkoituksena on tutkia, miten kyber- ja tietoturvallisuus näkyy yritysten strategisessa suunnittelussa ja millaisia tutkittuja hyötyjä yritysten on mahdollista kyberturvallisuuden strategisella suunnittelulla saavuttaa. Tutkielman tutkimuskysymykset ovat:

- Miten kyberturvallisuus ilmenee yritysstrategiassa?
- Millaisia hyötyjä yritys voi saavuttaa integroimalla kyberturvallisuuden osaksi yritysstrategiaa?

Tämän tutkielman terminologisen sisällön kannalta on hyvä huomata, että 2000-luvun alussa kyberturvallisuuden (engl. cybersecurity) käsite ei ollut vielä juurikaan käytössä sen enempää yleisessä kuin tieteellisessäkään sanastossa. Sen sijaan yleisemmin käytetty termi oli tietoturvallisuus (engl. information security). Kyberturvallisuuden käsitteiden määrittelyn yhteydessä kappaleessa 3.1.4 käydään läpi tieto-, ICT- ja kyberturvallisuuden eroja ja samankaltaisuuksia. Kuten kuvio 3 havainnollistaa, voidaan näitä käsitteitä pitää varauksella synonyymeina, ja tässä tutkielmassa näin myös tehdään. Koska teknologiat on rajattu tämän tutkielman ulkopuolelle, voidaan viittaukset kyberturvallisuuteen, tietoturvallisuuteen sekä kyber- ja tietoturvallisuuteen tulkita selkeyden vuoksi tarkoittavan samaa asiaa.

Aineistona tutkielmassa on käytetty tieteellistä tutkimusaineistoa, kuten vertaisarvioituja tieteellisiä artikkeleita, -kirjallisuutta sekä -raportteja. Lähdeaineiston evaluoinnissa on huomioitu Julkaisufoorumin tieteellisen julkaisutoiminnan laadunarviointia tukevan luokitusjärjestelmän luokitukset eri julkaisukanaville. Lähteissä on painotettu erityisesti luokitusjärjestelmän mukaisten arviointien perusteella tasojen 1-3 julkaisukanavia.

Taulukossa 1 on havainnollistettu tutkielman tieteellisten lähteiden määrä tasoluokituksen mukaisesti. Taulukossa on mainittu myös ei-tieteelliset, vertaisarvioimattomat lähteet, joita tässä tutkielmassa ovat julkishallinnon, kuten ministeriöiden tuottamat raportit ja strategiset muistiot, sanastokeskuksen julkaisut, standardit sekä viittaukset lakeihin. Ei-tieteelliset lähteet ovat osana tutkielmaa lähinnä taustoittavina ja käsitteistöä tukevina elementteinä.

TAULUKKO 1 Lähteiden määrä julkaisukanavan tasoluokituksen mukaan

| **Tasoluokka** | **Lähteiden määrä** |
|---|---|
| Taso 0 tai luokittelematon | 5 |
| Taso 1, perustaso | 17 |
| Taso 2, johtava taso | 19 |
| Taso 3, korkein taso | 11 |
| **Tieteelliset lähteet yhteensä** | **52** |
| Ei-tieteelliset lähteet | 7 |
| **Kaikki lähteet yhteensä** | **59** |

Lähdeaineiston etsimiseen on käytetty Jyväskylän yliopiston kirjaston JYKDOK-palvelua, Elsevierin Scopusta sekä Googlen Scholar -palvelua. Aineiston valinnassa ja laadun arvioinnissa on huomioitu julkaisukanavien tasoluokitusten lisäksi myös lähdeviittausten määrät, jotka on tarkistettu Googlen Scholar -palvelusta. Aineiston hakemiseen on käytetty muun muassa hakusanoja ja -lauseita ”cybersecurity”, ”corporate strategy”, ”strategic planning”, ”information security management”, “(implementation OR investment) AND information security”, “corporate security policy”.

Tutkielma rakentuu seuraavasti: Toisessa luvussa tarkastellaan strategiaa yritysstrategian näkökulmasta sekä käydään läpi strategista suunnittelua. Luvun loppupuolella perehdytään strategisen suunnittelun tutkimukseen. Kolmannessa luvussa määritellään kyberturvallisuuden käsitteet, jonka jälkeen tarkastellaan erityisenä mielenkiinnon kohteena olevaa kyberturvallisuuden asemaa ja merkittävyyttä yrityksissä. Neljännessä luvussa yhdistetään aiempien sisältölukujen tuloksia ja havaintoja sekä tarkastellaan kyberturvallisuutta osana yritysstrategiaa. Lisäksi neljännessä luvussa vastataan tutkimuskysymyksiin tieteelliseen kirjallisuuteen perustuen.

Tutkielman erityisiä kiinnostusalueita ovat yrityksen strateginen johtaminen, kyberturvallisuuden strateginen asema osana yritysstrategiaa sekä yritysstrategian implementointi. Kyberturvallisuuteen liittyvät teknologiat, trendit ja ilmiöt jäävät tämän tutkielman tarkastelun ulkopuolelle.

# 2 STRATEGIA

Tässä sisältöluvussa tarkastellaan strategiaa käsitteenä yrityskontekstissa sekä määritellään yritysstrategian alakäsitteen lisäksi, mitä strategisella suunnittelulla tarkoitetaan ja miten se eroaa strategisesta ajattelusta. Lopuksi luodaan katsaus strategisen suunnittelun tutkimukseen.

Strategia-sanan sekä toisaalta myös itse käsitteen juuret ulottuvat yleisen tietämyksen mukaan antiikin kreikkaan. Ensimmäiseksi konseptointiin liittyväksi viittaukseksi on esitetty Sun Tzu:n klassikkoa ”The Art of War” (Grant & Jordan, 2015, s. 8.) Vaikka kyseinen teos on ennen kaikkea sotastrateginen, tulee kuitenkin huomioida, että sodan ja liiketoiminnan strategiat jakavat keskenään lukuisia konsepteja sekä periaatteita (Henderson, 1989; Grant & Jordan, 2015, s. 8). Grantin ja Jordanin (2015, s. 8) mukaan yksi keskeisimmistä, sodalle ja liiketoiminnalle yhteisistä tekijöistä on strategian ja taktiikan erottaminen selkeästi toisistaan. Strategia on kokonaissuunnitelma, kun taas taktiikka on suunnitelma jonkin yksittäisen toiminnon toteuttamiseksi. Molemmilla on merkityksensä ja tarkoituksensa, mutta ne tulee pitää erillään (Henderson, 1989.) Sekä sota- että liiketoimintastrategioita yhdistää Grantin ja Jordanin (2015, s. 8) mukaan, että:

- Ne ovat tärkeitä;
- Niihin liittyy huomattavaa resurssien sitouttamista;
- Ne eivät ole helposti peruutettavia.

Organisaatioiden, yritysten ja erilaisten liikelaitosten strategisen suunnittelun eli strategiatyön saavuttaessa jalansijaa 1960-luvun puolivälissä alkoivat yritysjohtajat tulkita asiantuntijoiden avulla strategista suunnittelua ’parhaana käytäntönä’ toteuttaa uudella tavalla strukturoituja suunnitelmia kilpailukyvyn parantamiseksi (Mintzberg, 1994). Hieman jalostuneemmassa ja modernimmassa strategia-ajattelussa Johnson, Scholes ja Whittington (2008, s. 2) kuvaavat strategian keskeisimmän olemuksen organisaation pitkäaikaisena suuntana. Johnson ym. (2008, s. 3) antavat tukea tälle määritelmälle, ja täydentääkseen sekä syventääkseen kuvausta, määrittelevät strategian myös organisaation toiminnan alana, kilpailuetuna, sopivuutena liiketoimintaympäristöön sekä resursseina että kompetensseina.

Strategia esiintyy organisaatioissa lukuisilla eri tasoilla. Johnson ym. (2008, s. 7) esittelevät kolme päätasoa, jotka ovat yritysstrategia, liiketoimintastrategia ja operatiivinen strategia. Johnsonin ym. (2008, s. 7) tavoin Porter (1996, s. 285) viittaa eritasoisiin strategioihin, ja jakaa monipuolisen yrityksen strategiat kilpailu- ja yritysstrategioihin. Tämän tutkielman kannalta näistä keskeisin on yritysstrategia (engl. corporate strategy).

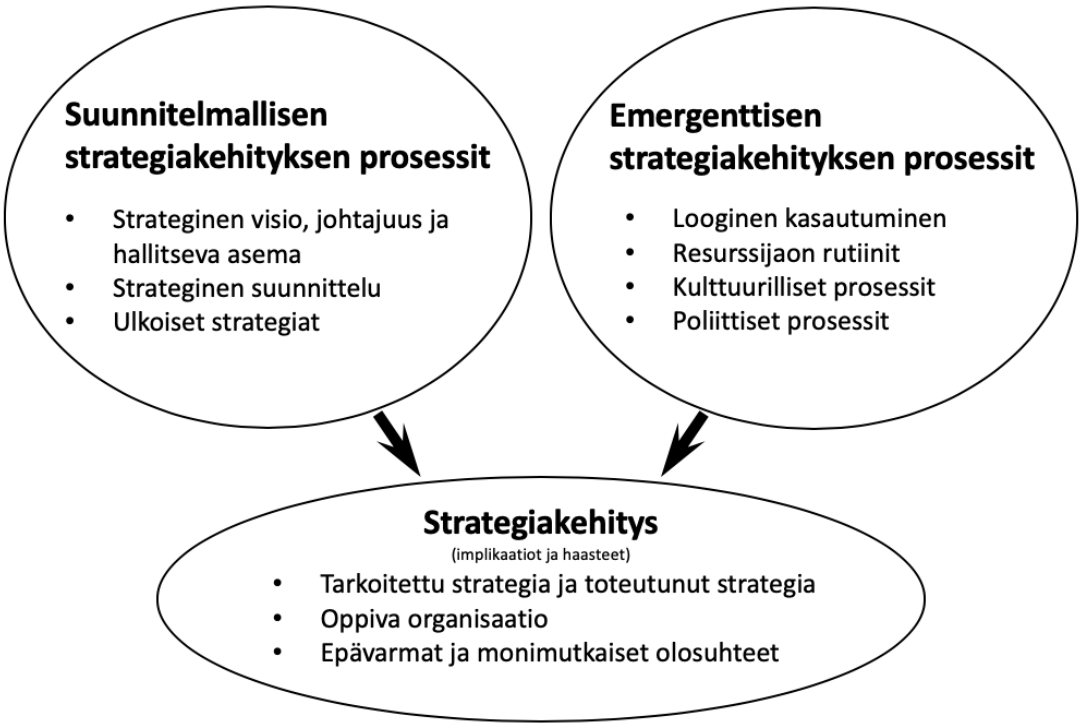
## 2.1 Yritysstrategia

Andrews (1997, s. 52) kuvaa strategiaprosessin ylintä päätasoa, eli yritysstrategiaa, yrityksen päätöksentekomallina, joka määrittää ja paljastaa yrityksen päämäärät sekä tarkoituksen. Andrewsin (1997, s. 52) mukaan yritysstrategia tuottaa periaatteelliset käytännöt ja suunnitelmat näiden päämäärien saavuttamiseen sekä lopulta määrittää ne toimialat ja markkinat, jossa yritys haluaa toimia omistajiensa eduksi. Johnsonin ym. (2008, s. 7) mukaan yritysstrategia määrittelee yrityksen koko toiminnan alan, ja sen miten arvoa lisätään yritysorganisaation eri liiketoimintayksiköissä.

Yritystason strategia kiinnostaa ennen kaikkea yrityksen omistajia ja osakemarkkinoita odotusten suhteen. Yritysstrategia voi hyvinkin olla muotoiltu eksplisiittisesti tai implisiittisesti yrityksen suuremman kokonaistehtävän, eli 'mission' muotoon, joka peilaa näitä odotuksia edellä mainituille yrityksen sidosryhmille. (Johnson ym., 2008, s. 7; Andrews, 1997, s. 52.) Yritysstrategiaa kehitetään strategisen suunnittelun avulla (Johnson ym., 2008, s. 400) ja muut lähikäsitteet, kuten strategiaprosessi ovat Andrewsin (1997, s. 53) mukaan synonyymeja yritysstrategian kehittämiselle.

## 2.2 Strateginen suunnittelu

Strategisen suunnittelun perimmäisenä tarkoituksena on yrityksen nykyistä strategiaa evaluoimalla ja jalostamalla muokata se vastaamaan paremmin jatkuvasti muuttuvia olosuhteita, kuten markkinoiden tarpeita ja kilpailutilannetta (Johnson ym., 2008, s. 400). Strateginen suunnittelu mielletään yleisesti geneeriseksi, varsin loogiseksi ja järjestelmälliseksi prosessiksi (Porter, 1985). Minzberg (1994) tuo kuitenkin esille Porterin (1985) ajatusten kanssa ristiriitaisen näkemyksen, jonka mukaan strategian tekeminen on äärimmäisen monimutkainen prosessi, johon liittyy kaikkein kehittyneintä, hienovaraisinta ja toisinaan jopa ihmisen alitajuntaista ajattelua. Johnson ym. (2008, s. 400) selittää strategisen suunnittelun kahden, varsin laajan näkemyksen kautta, jotka eivät kuitenkaan ole toisiaan poissulkevia. Kuviossa 1 on visualisoitu Johnsonin ym. (2008, s. 400) näkemys strategian kehitysprosessista.




KUVIO 1 Strategian kehitysprosessi (Johnson ym., 2008, s. 400 mukaan)

Näistä ensimmäinen näkemys rakentuu suunnitelmallisen strategiakehityksen prosessina siten, että strateginen suunnittelu on tarkoituksenmukaista, huolellista ja harkittua toimintaa, joka tyypillisesti perustuu ylimmän johdon päätöksiin. Toinen näkemys on emergenttinen, uudistuvan strategiaprosessin mukainen, jossa strategiat kehittyvät organisaatiossa ajan myötä keskustelun, kokemusten ja ideoiden siivittämänä sekä luovat täysin uutta ajattelua. (Johnson ym., 2008, s. 400.) Jälkimmäinen näkemys saa tukea myös Minzbergin (1994) havainnoista, sillä hänen mukaansa tutkimus toisensa jälkeen on näyttänyt toteen, että kaikkein tehokkaimmat johtajat luottavat joihinkin kaikkein pehmeimpiin tiedon ilmenemismuotoihin, kuten juoruihin, kuulopuheisiin ja muihin aineettomiin tiedonjyväsiin.

### 2.2.1 Strateginen suunnittelu vs. strateginen ajattelu

Minzbergin (1994) ajatukset strategista suunnittelua kohtaan ovat kriittisiä ja hänen mukaansa strateginen suunnittelu pilaa strategisen ajattelun, sillä menestyksekkäimmät strategiat ovat ennemminkin visioita kuin suunnitelmia. Heracleous (1998) yhtyy Minzbergin kritiikkiin strategista suunnittelua kohtaan ja argumentoi strategisen suunnittelun todellisena tarkoituksena olevan strategisen ajattelun kehittämisen. Heracleous (1998) lisää, että strateginen suunnittelu onkin ajan saatossa muuttunut enemmän strategisen ajattelun suuntaan.

Minzbergin (1994) mukaan ”Strategiaa suunnittelevien henkilöiden tulisi tehdä kontribuutionsa pikemminkin strategiaprosessin ympärillä, kuin sen sisällä.” Tällä Minzberg tarkoittaa, että strategista suunnittelua tekevien henkilöiden tulisi toimittaa muodollisia analyyseja tai faktoja strategisen ajattelun polttoaineeksi silloin, kun he tekevät sen laajentaakseen asioiden tarkastelua ja pohdintaa sen sijaan, että pyrkisivät löytämään yhden oikean vastauksen. Lisäksi heidän tulisi toimia katalyytteina, jotka tukevat strategian tekemistä ohjaamalla ja rohkaisemalla johtajia ajattelemaan strategisesti. Lopulta strategiaa suunnittelevien henkilöiden tehtävänä on strategiaa ohjelmoimalla auttaa määrittelemään ne konkreettiset toimet, jotka tarvitaan vision toteuttamiseksi. (Minzberg 1994.)

Bouhali, Mekdada, Lebsir ja Ferkha (2015) näkevät sekä strategisen ajattelun että strategisen suunnittelun kuuluvan osaksi modernia strategiatyötä. Johtajien tulee olla luovia niin strategisina ajattelijoina kuin suunnittelijoina, johtuen jo pelkästään siitä, että suunnitelmat muuttuvat usein. Strategisen ajattelun tavoitteena on ylläpitää tarkoituksen, suunnan ja pysyvyyden tunnetta strategiaprosessin aikana. Strateginen suunnittelu taas tukee strategista ajattelua, kuvaamalla reitin nykyisestä positiosta tulevaan, suunniteltuun ja toivottuun positioon. (Bouhali ym., 2015.)

### 2.2.2 Tutkimus ja haasteet

Szulanski, Porac ja Doz (2005, s. xiii) toteavat, että strategiaprosessien tutkimuksen asema kiinnostavana ja hyväksyttynä aiheena on vakiintunut akateemisessa kirjallisuudessa. Szulanski ym. (2005, s. xiii) arvioivat, että kestävä tieteellinen kiinnostus strategiaprosessiin johtuu siitä jatkuvasta oletuksesta, että erilaiset strategiaprosessit ja strategisen suunnittelun menetelmät olisivat toisia tehokkaampia esimerkiksi yrityksen pitkäaikaisen suorituskyvyn kautta mitattuna kuin pelkästään onneen perustuen. Hutzschenreuterin ja Kleindienstin (2006) mukaan strategiaprosessin tutkimus on kehittynyt merkittävästi viime vuosikymmeninä ja sillä on lukuisia jatkotutkimusmahdollisuuksia eri näkökulmiin perustuen. Van de Ven (1992) toteaa strategiaprosessin tutkimuksesta, ettei tutkijoiden tulisi vain olettaa tai kuvata strategista muutosta, vaan pyrkiä myös selittämään kuinka ja miksi strateginen muutos tapahtuu. Strategiaprosessin tutkimusta tehdään van de Venin (1992) mukaan kolmella tavalla: (1) Logiikkana, jota käytetään selittämään syy-seuraussuhdetta varianssiteoriassa, (2) käsitteiden ja konseptien ryhmänä viitaten yksittäisten henkilöiden tai organisaation toimintaan ja, (3) ajan myötä muuttuvien tapahtumien sekvenssinä. Pettigrew (1992) esittää kritiikkiä siitä, että näistä vain viimeksi mainittu lähestymistapa käsittelee strategiaprosessia toiminnassa ja pystyy siten ottamaan huomioon, miten strategiaprosessissa mainitut asiat kehittyvät ja muuttuvat ajan myötä. Strategia on Whittingtonin (2007) mukaan sosiaalinen käytäntö, jossa on monia näkökohtia ja monia seurauksia. Strategiaprosessia ei tulisi siis tutkia pelkästään sen suorituskyvyn ja saavutusten kautta, vaan sen tutkimuksessa tulisi huomioida myös sosiologinen aspekti. (Whittington, 2007.)

# 3 KYBERTURVALLISUUS

Kyberturvallisuuden tuottaminen ja ylläpito on jatkuvaluonteista työtä, joka vaatii jatkuvaa yritystä ja erehdystä kehittyäkseen ja jalostuakseen kunkin yrityksen tarpeisiin ja haasteisiin. Yritysorganisaation ei tulisi koskaan lakata kehittämästä kyberturvallisuusstrategiaansa, työkalujaan, taktiikoitaan ja teknologioitaan. (Kim, 2007.) Kyberhyökkäykset yleistyvät jatkuvasti, sillä ne ovat hyökkääjälle edullisempia, kätevämpiä ja vähemmän riskialttiita kuin fyysiset hyökkäykset (Jang-Jaccard & Nepal, 2014). Choo (2011) pitää elintärkeänä sitä, että yhteiskuntamme, yrityksemme, hallituksemme ja tutkimusinstituutiomme innovoivat nopeammin kuin rikolliset ja muut haitalliset toimijat. Kyberhyökkäysten toteuttamiseen ei tarvita juurikaan muita resursseja kuin verkkoyhteys ja tietokone. Maantieteelliset etäisyydet eivät rajoita kyberhyökkäyksiä, ja lisäksi niitä on vaikeaa tunnistaa ja saattaa tekijöitä vastuuseen internetin anonymiteetin vuoksi (Jang-Jaccard & Nepal, 2014.) Kyberturvallisuus tuleekin rakentaa ja ylläpitää täysin eri lähtökohdista kuin esimerkiksi fyysinen turvallisuus (von Solms & van Niekerk, 2013).

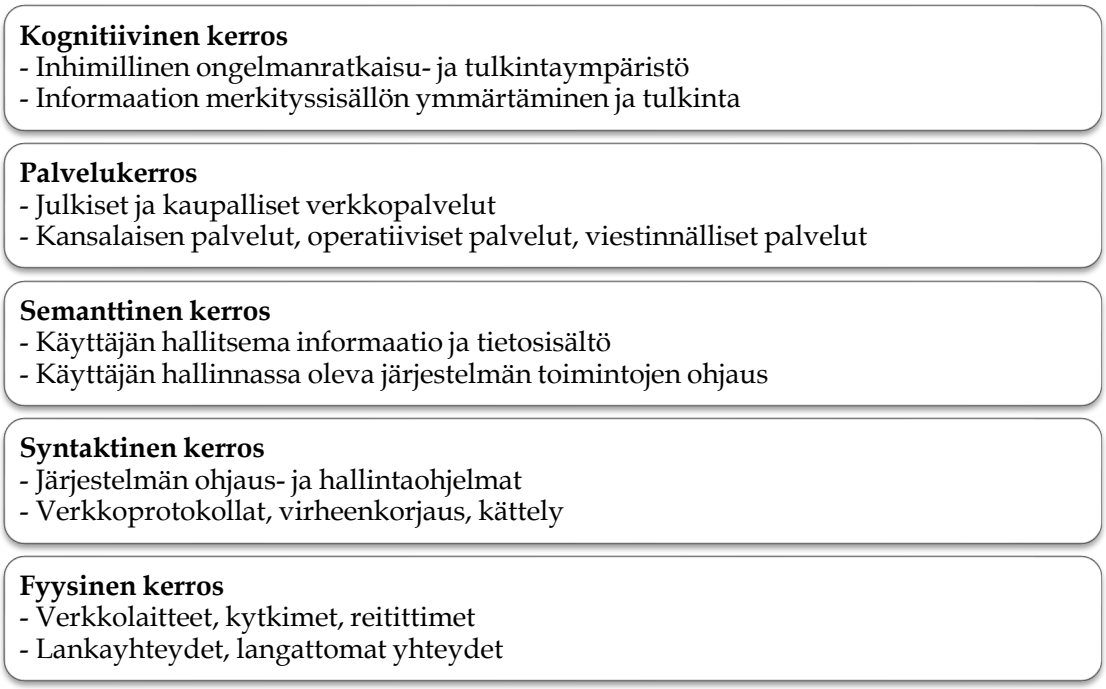
Tässä sisältöluvussa määritellään kyberturvallisuuden keskeisimmät käsitteet, kuten kybermaailma, kyberturvallisuus ja kybertoimintaympäristö. Lisäksi tarkastelemme tieto-, ICT- ja kyberturvallisuuden eroja sekä yhtäläisyyksiä. Lopuksi käymme läpi kyberturvallisuutta yritysten näkökulmasta.

## 3.1 Käsitteiden määrittely

Kyberturvallisuuden käsitteellinen määrittely yksiselitteisesti on vaikeaa (von Solms & van Niekerk, 2013), johtuen jo pelkästään siitä, että kyberturvallisuus itsessään on varsin laaja käsite ja vaatii määrittelyssään (Sanastokeskus TSK, 2018) myös muiden lähikäsitteiden, kuten kybermaailman ja kybertoimintaympäristön määrittelemisen.

### 3.1.1 Kybermaailma

Libicki (2007, s. 236-240) on luonut OSI-malliin (Open Systems Interconnection model) perustuvan kybermaailman rakenteen, joka perustuu viisikerroksiseen rakenteeseen. OSI-mallin tapaan Libickin kybermaailman rakenteen eri kerrokset käyttävät alemman kerroksen palveluita ja tarjoavat omia palveluitaan ylemmälle kerrokselle. Kybermaailman tasomalli on visualisoitu kuviossa 2.




KUVIO 2 Kybermaailman tasomalli (Lehto & Kähkönen, 2015a mukaan)

Kerroksiin kuuluu fyysinen kerros, joka pitää sisällään fyysiset verkkoyhteydet kuten valokuitu-, kaapeli- ja langattomat yhteydet sekä laitteet kuten esimerkiksi kytkimet, reitittimet ja keskittimet. Seuraava kerros on syntaktinen kerros, jonka piirissä ovat järjestelmän ohjaukseen ja hallintaan tarvittavat ohjelmistot sekä laitteiden vuorovaikutuksen mahdollistavista protokollista ja niiden vaatimista alitoiminnoista vastaavat toiminnot. Tämän jälkeen tuleva semanttinen kerros on koko kybermaailman ydin (Lehto & Kähkönen, 2015a), johon kuuluu käyttäjän hallitsema tietosisältö ja käyttäjän hallinnassa olevat järjestelmätoiminnot, kuten esimerkiksi tehdasprosessin valvonta ja operointi. Rakenteessa seuraavana olevan palvelukerroksen sisältö perustuu julkisiin, kaupallisiin sekä yksityisiin digitaalisiin verkkopalveluihin. Ylin kerros on kognitiivinen kerros, joka kuvaa yksittäisen käyttäjän informaation ymmärrysmaailmaa, jossa muodostetaan henkilökohtainen ymmärrys ja käsitys. (Lehto & Kähkönen, 2015a; Libicki, 2007, s. 236-240.)

### 3.1.2 Kyberturvallisuus

Von Solms & van Niekerk (2013) toteavat, että kyberturvallisuutta on käytetty tieteellisissä julkaisuissa usein kattavana yleisterminä, ja jatkavat, että lisäksi kyberturvallisuuden määritelmät ovat usein hyvin samankaltaisia tietoturvallisuuden määritelmien kanssa. Jyväskylän yliopiston kyberturvallisuuden professorina toimiva Martti Lehto (2015a) määrittelee kyberturvallisuuden lyhyesti ”toimenpiteiksi, joilla suojaudutaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteutetaan tarvittavia vastatoimenpiteitä”.

Suomen kyberturvallisuusstrategia (2013) ja Sanastokeskus TSK:n (2018) kyberturvallisuuden sanasto määrittelevät kyberturvallisuuden abstraktisti tavoitetilana, ”jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Kybertoimintaympäristöön viitataan myös Lehdon (2015a; 2015b) määritelmien tarkennuksissa. On siis tarpeen tarkastella, mitä kybertoimintaympäristöllä tarkoitetaan.

### 3.1.3 Kybertoimintaympäristö

Suomen kyberturvallisuusstrategia (2013) määrittelee kybertoimintaympäristön seuraavasti: ”sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö”. Kybertoimintaympäristön määritelmä on perusmuotoisena melko tiivis ja sisältää lisäksi erillisen käsitteen ”tietojärjestelmä”, jolle sopiva määritelmä löytyy Sanastokeskus TSK:n (2013) Tietohuollon sanastosta: ”järjestelmä jonkin yhtenäisen, pysyväisluonteisen tietojenkäsittelykokonaisuuden suorittamiseen”. Tietojärjestelmän määritelmää on vielä laajennettu Sanastokeskus TSK:n (2013) tietueessa seuraavasti: ”Tietojärjestelmän muodostavat tiedot ja niiden käsittelysäännöt, käsittelyn henkilö- ja laiteresurssit sekä tiedonsiirtolaitteet ja toimintaohjeet”. Käytännön esimerkkeinä kybertoimintaympäristön tietojärjestelmistä Sanastokeskus TSK (2018) käyttää ydinvoimalan ohjausjärjestelmiä, elintarvikkeiden kuljetus- ja logistiikkajärjestelmiä, liikenteen ohjausjärjestelmiä sekä pankki- ja maksujärjestelmiä.

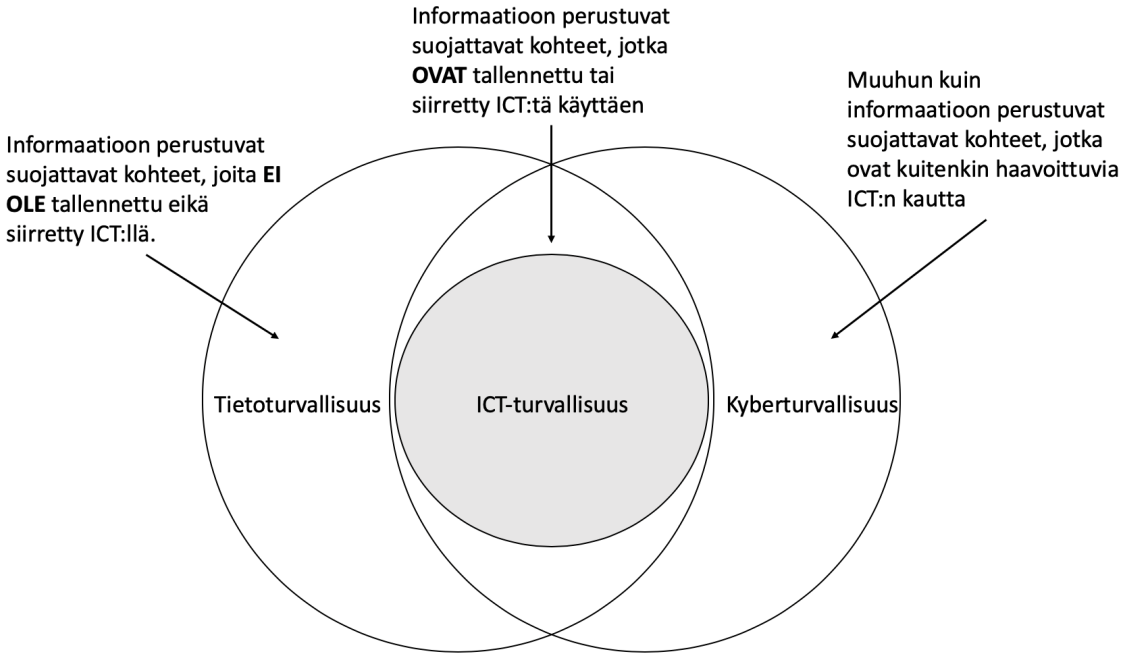
### 3.1.4 Tieto-, ICT- ja kyberturvallisuuden erot

Siinä missä tietoturvallisuudella tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin (Sanastokeskus TSK, 2018). ICT[1]:n turvallisuus koskee sellaisia teknologisten järjestelmien suojaamista, jota käytetään tiedon ja muiden informaation perustuvien resurssien tallentamiseen tai siirtämiseen (von Solms & van Niekerk, 2013).

[1] ICT = Tieto- ja viestintäteknologia (engl. information and communication technology)

Kansainvälinen ISO/IEC standardi 13335-1 (2004) määrittelee ICT-turvallisuuden hallinnan kaikilla niillä osa-alueilla, jotka liittyvät tiedon luottamuksellisuuden, eheyden, kiistämättömyyden, vastuullisuuden, autenttisuuden ja luotettavuuden määrittelyyn, saavuttamiseen ja ylläpitämiseen (ISO/IEC 13335-1, 2004, s. 3).

Kyberturvallisuuden määritteleminen tieto- ja ICT-turvallisuuden kautta auttaa asemoimaan kyberturvallisuuden laajuutta ja vaikutusaluetta. Kuten von Solms & van Niekerk (2013) kuviossa 3 esittävät, tieto- ja kyberturvallisuuden yhtymäkohdat ovat siellä, missä ICT-turvallisuus vaikuttaa molempiin. Määritelmän kannalta olennaista on myös se, perustuuko suojattava kohde informaatioon vai ei, sekä miten ICT:tä on käytetty. (von Solms & van Niekerk, 2013.)




KUVIO 3 Tieto-, ICT- ja kyberturvallisuuden väliset suhteet (von Solms & van Niekerk, 2013 mukaan).

## 3.2 Yritysten kyberturvallisuus

Kybertoimintaympäristöjen infrastruktuuri on suurilta osin pikemminkin yksityisten yritysten, kuin julkisen sektorin hallussa. Verkottuneiden palveluketjujen luonne tarkoittaa sitä, että hyökkäys yhdelle liike-elämän sektorille voi aiheuttaa ongelmia toisilla sektoreilla (Choo, 2011; Hiller & Russell, 2013.) Boonen (2017) mukaan yksikin hakkeroitu yritys voi vaarantaa jokaisen tuotantoketjuun kuuluvan yrityksen turvallisuuden.

Kansakuntien turvallisuus, talouden hyvinvointi ja kansalaisten suojelu ovat kaikki yhteydessä toisiinsa (Hiller & Russell, 2013.) Hallitukset eivät voi Choon (2011) mukaan kuitenkaan täysin delegoida kybertoimintaympäristöjen

turvaamista yksityisille yrityksille, sillä hallitukset eivät voi työskennellä eristyksissä kriittistä infrastruktuuria ylläpitävistä yrityksistä, jotka ovat usein yksityisessä omistuksessa. Poikkeuksena tähän toimintamalliin Choo (2011) mainitsee kommunistiset valtiot, kuten Kiinan, joissa kriittinen infrastruktuurikin on valtion omistuksessa. Tämä tiettyjen yritysten huoltovarmuuskriittinen asema on huomioitu myös Suomen kyberturvallisuusstrategiassa (2013) ihan omana lukunaan. Elinkeinoelämän toimintaedellytyksiä varten on perustettu yritysmaailman toimijoista sekä valtionhallinnon toimijoista oma huoltovarmuusorganisaatio, jonka varautumistoimenpiteillä turvataan yhteiskunnan toimivuuden kannalta välttämätön infrastruktuuri ja kriittisen tuotannon jatkuminen kaikissa tilanteissa sekä poikkeusoloissa (Suomen kyberturvallisuusstrategia, 2013).

Yritykset ovat itse vastuussa omasta kokonaisturvallisuudestaan, tieto-, ICT- ja kyberturvallisuus mukaan lukien. Yrityksen tulee tunnistaa suojattavat kohteet, prosessit ja tieto. Olennaista on yrityksen kyvykkyys ennakoida, havainnoida, torjua ja rajoittaa sen toimintaa uhkaavia riskejä niiden ilmenemismuodoista riippumatta (Merete Hagen, Albrechtsen & Hovden, 2008.) Huang, Rau ja & Salvendy (2010) argumentoivat lisäksi, etteivät pelkästään tekniset keinot riitä tiedon suojaamiseen ja uhkilta varautumiseen, vaan jokaisen yksittäisen työntekijän, johtajan tai henkilöstön jäsenen – ihmisen – toiminnalla on merkittävä rooli tietoturvallisuuden ylläpitämisessä.

### 3.2.1 Johdon rooli

Kyberturvallisuuden tulisi olla ylimmän johdon prioriteetti, sillä ylin johto on kuitenkin lopulta vastuussa kaikesta, mitä yrityksessä tapahtuu. Kyberturvallisuutta tulisi myös johtaa koko organisaation laajuisesti, keskitetysti ja johdonmukaisesti (Boone, 2017.) Koska strategisilla päätöksillä on vaikutuksia myös teknologiaan, tulisi kaikki yrityksen teknologiset hankinnat evaluoida niiden toiminnallisten hyötyjen lisäksi myös turvallisuusvaikutustensa kautta (Dutta & McCrohan, 2002).

Tietoturvallisuus ei ole pelkästään tekninen asia, vaan on yrityksen johdon vastuulla maksimoida yrityksen henkilöstön sitoutuminen organisaation turvallisuustavoitteisiin ja käytäntöihin (Siponen & Oinas-Kukkonen, 2007). Rothrock ym. (2018) näkevät kyberturvallisuuteen liittyvän niin monen tasoisia riskejä, aina tietovuodoista maineen menetykseen asti, että sen tulisi koskettaa yrityksen jokaista henkilöä, ylintä johtoa myöten. Boonen (2017) mukaan kyberturvallisuutta tulisi johtaa yrityksen ylimmän johdon tasolta siitäkin syystä, että mikäli liiketoimintayksiköille annetaan vastuu oman kyberturvallisuutensa toteuttamisesta, he priorisoivat kuitenkin liiketoimintayksikön oman ydintoimintansa kyberturvallisuuden toteuttamisen edelle. Kirschin ja Bossin (2007) tutkimuksessa tarkasteltiin turvallisuutta yksittäisten työntekijöiden työnkuvausten kautta. Tutkimustulosten mukaan oli epätodennäköistä, että heidän osuutensa tietoturvallisuuden toteuttamisessa otettaisiin huomioon. Tutkimustulokset osoittivat li-

säksi, että johtajien tulisi kiinnittää huomiota mielekkään tietoturvallisuuspolitiikan luomiseen sekä kannustaa työntekijöitä seuraamaan sitä. Johtajien tulisi myös korostaa tietoturvallisuuspolitiikkojen määrittelyä ja poikkeuksien havainnointia sekä kiinnittää vähemmän huomiota palkitsemiseen (Kirsch & Boss, 2007.)

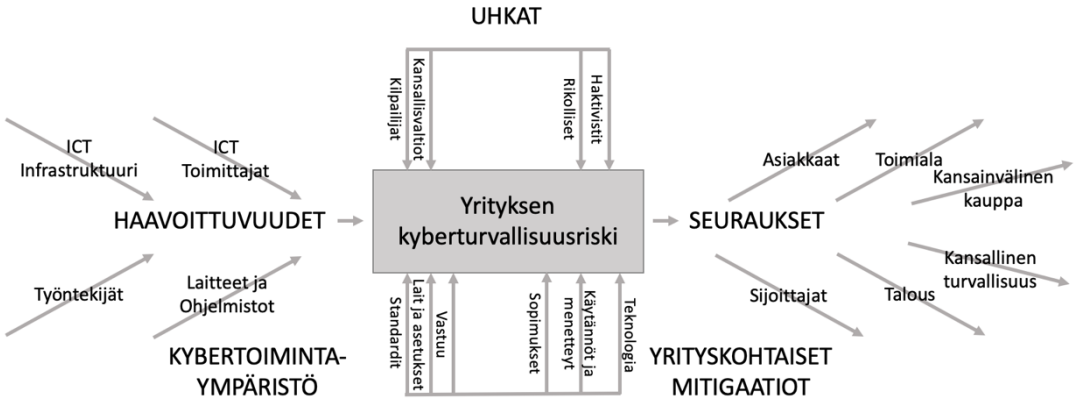
### 3.2.2 Henkilöstön rooli

Inhimillinen tekijä on Gonzalezin ja Sawickan (2002) mukaan tietoturvallisuuden 'Akilleen kantapää'. Gonzalezin ja Sawickan ajatuksiin yhtyy myös Gratian, Bandi, Cukier, Dykstra ja Ginther (2018), joiden tutkimusartikkelissa todetaan ihmisen olevan kyberturvallisuuden heikoin lenkki, sillä kaikki modernit tekniset turvallisuusratkaisutkin ovat edelleen alttiita inhimillisen tekijän aiheuttamille virheille. Kaikki ihmiset ovat tietoturvallisuuden näkökulmasta erilaisia muun muassa demografisten tekijöiden, persoonallisten piirteiden, riskinoton ja päätöksenteon osalta. Nämä erot vaikuttavat osaltaan siihen, miten ihmiset suhtautuvat kyberturvallisuuteen ja millaisia intentioita ihmisillä on havaitessaan poikkeamia erilaisissa kyberympäristöihin kohdistuvissa uhkissa ja poikkeamissa. (Gratian ym., 2018.)

Kim (2017) argumentoi, että vaikka tietoturvallisuuden tekninen toteuttaminen kuuluukin IT-osaston vastuulle, eikä loppukäyttäjille, on kuitenkin tärkeää, että työntekijät ovat tietoisia turvallisuusuhkista, ja että heidät on koulutettu organisaation tietoturvallisuusstrategian mukaisesti. Lisäksi, von Solms ja von Solms (2004) toteavat, että työntekijöitä ei voi saattaa vastuuseen tietoturvallisuuden ylläpitämisestä, jos heitä ei ensin ole koulutettu ymmärtämään mitä tietoturvallisuutta uhkaavat riskit ovat ja mitä huomioimiseksi tulee tehdä. Kyberturvallisuuden kouluttamisen kannalta tulee lisäksi ymmärtää, että erityyppiset ihmiset ovat eri tavalla vastaanottavaisia koulutuksen suhteen eri metodeja ja toimintatapoja käyttäen. Henkilöstön turvallisuuskäyttäytymisen kouluttamisessa voidaan esimerkiksi räätälöidä erityyppisiä koulutuksia tunnollisille, riskejä vältteleville ja rationaalista päätöksentekoa harjoittaville käyttäjille (Gratian ym., 2018.) Albrechtsen ja Hovden (2010) havaitsivat tutkimuksissaan, että henkilöstön aktiivinen osallistuminen tietoturvallisuuskoulutukseen ja tietämyksen kasvattaminen aiheutti myönteisiä muutoksia koko organisaation tietoturvallisuuden tietoisuuden ja tietoturvallisen käyttäytymisen suhteen.

### 3.2.3 Uhkat ja riskit

Yrityksen kyberturvallisuusriski on visualisoitu Hillerin ja Russelin (2013) mukaan kuviossa 4. Yritykseen kohdistuvat uhkat voivat tulla monesta eri lähteestä, mukaan lukien kilpailijoilta, joiden motiiveina on mahdollisesti sabotoida kohdeyrityksen prosesseja tai varastaa yrityssalaisuuksia (Hiller & Russell, 2013).




KUVIO 4 Yrityksen kyberturvallisuusriskin elementit (Hiller & Russell, 2013 mukaan).

Uhka voi tulla myös yrityksen sisältä esimerkiksi sitä kautta, että henkilöstö luottaa liikaa intuitioon tehdessään päätöksiä kyberturvallisuuden suhteen (Julisch, 2013). Hillerin ja Russelin (2013) mukaan 'haktivistit' ja rikolliset voivat kohdistaa esimerkiksi palvelunestokampanjoita yrityksen palveluihin tai infrastruktuuriin, sekä aiheuttaa yrityksessä kaaosta, joka voi olla hyökkääjälle hyödyksi. Lisäksi toimijana voi olla kansallisvaltio, joka voi käynnistää kumppaneidensa kanssa yhteishyökkäyksiä ulkomaisia yrityksiä vastaan, hyödyttääkseen oman maansa taloutta, kauppasuhteita tai kansallista turvallisuutta. (Hiller & Russell, 2013).

Hillerin ja Russelin (2013) mukaan haavoittuvuudet ovat yrityksen sisäisiä riskejä, mukaan lukien toimitusketjun tuottamat riskit, sillä toimittajien valinnat ovat osa yrityksen omaa riskienhallintaa. Julisch (2013) argumentoi lisäksi, että monella yrityksellä on aukkoja kyberturvallisuutensa suhteen jo perusteissa ja henkilöstön koulutuksessa. Tietojärjestelmien käytön heikot perustaidot ovat yhteydessä kyberturvallisuusriskien ymmärtämättömyyteen (Huang ym., 2010). Haavoittuvuudet voivat olla peräisin yrityksen työntekijöiden huolimattomasta toiminnasta tai teknisestä haavoittuvuudesta infrastruktuurissa. (Hiller & Russell, 2013). Kyberympäristönsä resilienssiä kasvattaakseen ja ylläpitääkseen yrityksellä tulee olla selkeä, testattu suunnitelma erilaisten skenaarioiden varalle (Rothrock ym., 2018). Lisäksi tulee huomioida 'mitigaatiot' eli yrityskohtaiset suojautumiskeinot, joita yritys voi sisäisesti toteuttaa vähentääkseen tietoverkkohyökkäyksen riskiä. Näitä voivat olla esimerkiksi tekniset ratkaisut, käytännöt ja menettelyt sekä mahdolliset sopimukset toimittajien ja asiakkaiden kanssa, jotka sisältävät erityisiä tietoturvallisuusmäärityksiä. (Hiller & Russell, 2013).

Rothrock ym. (2018) mukaan yritysjohdon vastuulla on evaluoida ja priorisoida yrityksen kybertoimintaympäristössä esiintyvät riskit. Von Solmsin ja von Solmsin (2004) mukaan tyypillisimmät kysymykset tietoturvallisuuspäälliköltä tai -johtajalta ovat: ”mitä riskejä vastaan tietoresurssit tulee suojata?” ja ”mitkä vastatoimenpiteet tarjoavat parhaan suojan näitä riskejä vastaan?”. Kysymykset ovat relevantteja ja niille täytyy löytää vastauksia. Muussa tapauksessa yritys

hukkaa resursseja tehottomiin vastatoimiin (von Solms & von Solms, 2004). Hiller ja Russell (2013) toteavat seurauksista, että tietovuodot tai muut kyberturvallisuusrikkomukset voivat vaikuttaa negatiivisesti monella eri tavalla, kuten esimerkiksi asiakkaiden yksityisyyteen, liikesalaisuuksien vuotamiseen sekä kilpailukyvyn ja työpaikkojen menetykseen. On myös huomattava, että taloudellinen elinvoimaisuus ja vahva kyberturvallisuuden taso yrityksissä vaikuttavat myönteisesti myös kansalliseen turvallisuuteen, kun taas päinvastainen toiminta voi aiheuttaa volatiliteettia kansainvälisissä suhteissa. (Hiller & Russell, 2013.)

# 4 KYBERTURVALLISUUS YRITYSSTRATEGIASSA

Tietoturvallisuuden ja yritysstrategian konvergoidun tutkimuksen alustus nähtiin 2000-luvun taitteessa, kun Basie von Solms (2001) kirjoitti tiiviin artikkelin aiheesta, tarkoituksenaan tutkimusyhteyden luominen yrityksen hallinnon ja tietoturvallisuuden välille. Hallinnollisen tietoturvallisuuden standardoituna perustana voidaan pitää tietoturvallisuuden standardia BS7799-1:1999, joka sisältää muun muassa kymmenen kohdan suositukset tietoturvallisuuden kontrolleiksi (BSI, 1999).

Monissa tietoturvallisuuden hallinnan kansainvälisissä standardeissa ja parhaissa käytännöissä (kuten esimerkiksi BS7799-1, ISO/IEC 27001, NIST CSF) korostetaan, että asianmukainen tietoturvallisuuspolitiikka on kaikkien onnistuneiden tietoturvallisuuden hallintajärjestelmien ydin ja perusta. Von Solmsin & von Solmsin (2004) mukaan yrityksen tietoturvallisuuden strategiat, käytännöt ja menettelyt tulee lähtökohtaisesti perustua tämänkaltaiseen tietoturvallisuuspolitiikkaan. Ylimmän johdon sitoutuminen yrityksen tietoturvallisuuden hallintajärjestelmään on näkyvin tapa, jolla yrityksen ylin johto osoittaa sitoutumisensa koko yrityksen tietoturvallisuuteen. (von Solms & von Solms, 2004.) Tieto-, ICT- ja kyberturvallisuutta sekä strategista johtamista – yhdessä ja erikseen – on tutkittu ja kehitetty tieteellisestäkin näkökulmasta varsin laajalti.

Tämä tutkielman sisältöluku yhdistää kyberturvallisuuden ja yritysstrategian. Lisäksi tässä sisältöluvussa tarkastellaan yritysjohdon vastuuta ja sitoutumista, hallinnon ja johtamisen viitekehystä, kyberturvallisuuden varsinaista implementointia yritysstrategiaan, vaikutusten arviointia, sekä mahdollisia hyötyjä, joita kyberturvallisuuden ja yritysstrategian integraatiolla voidaan saavuttaa. Lopuksi osoitetaan tutkimusaineistoon perustuen strategisen viitekehyksen avulla strategiakehityksen ja kyberturvallisuuden kehittämisen yhtymäkohtia ja eroja.

## 4.1 Yritysjohdon vastuu ja sitoutuminen

Organisaation ylimmän johdon olisi johtajuutta osoittamalla edistettävä organisaation toiminta-ajatuksen (strategian), vision, arvojen ja kulttuurien käyttöönottoa sekä luotava sisäinen ympäristö, joka sitouttaa ja osallistaa ihmiset organisaation tavoitteiden saavuttamiseen. Lisäksi ylimmän johdon olisi kannustettava ja tuettava olennaisilla tasoilla olevia esimiehiä edistämään ja ylläpitämään organisaation ylimmän johdon määrittelemää yhteistä tarkoitusta ja suuntaa. (ISO, 2018.) Von Solms (2001) korostaa artikkelissaan, että yrityksen ylimmällä johdolla ei ole muuta vaihtoehtoa, kuin olla sitoutunut ja vastuullinen tietoturvallisuuden suhteen. Perusteluissaan von Solms (2001) vetoaa muun muassa lakiin, joka edellyttää, että yrityksen johto on sitoutunut ja vastuussa hyvästä hallinnosta yrityksessään viitaten siis epäsuorasti siihen, että hyvä hallinto sisältää myös tietoturvallisuuden huomioimisen. Myös Suomen lakiin (Osakeyhtiölaki 2006/624 § 8) on kirjattu: "yhtiön johdon on huolellisesti toimien edistettävä yhtiön etua". Tämän lisäksi tieto- ja kyberturvallisuuden näkökulmasta yritysten toimintaa velvoittaa muun muassa GDPR[2], joka ohjaa yritysjohdon sitoutumista tietosuojan ja -turvallisuuden toteuttamiseen myös sanktioilla, kuten määräämällä tietosuojaloukkauksista "hallinnollisen sakkorangaistuksen, joka on enintään 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi". (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016, Artikla 83 kohta 4.)

Tietoturvallisuuden tärkeyden perustelemiselle von Solms (2001) ei näe tarvetta, sillä hänen mukaansa sen tulisi olla itsestään selvää kaikille. Strategisen merkityksen lisäksi von Solms (2001) argumentoi useaan otteeseen eri sanankääntein, kuinka tärkeää on, että yrityksen johto on sitoutunut ja vastuullinen tietoturvallisuuden strategiseen implementointiin, tiivistäen:

> Tietoturvallisuuden huolehtimisesta on suora yrityshallinnollinen vastuu yrityksen johtoryhmän harteilla.

Kyberturvallisuuden strategiselle suunnittelulle keskeistä on varmistaa, että yrityksen ylin johto ymmärtää täysin, miten teknologiat auttavat liiketoimintatavoitteiden saavuttamisessa ja millainen sietokyky organisaatiolla on kestää teknologiasta johtuvia menetyksiä. Tämä on suora keino sitouttaa yritysjohtoa kyberturvallisuuden huomioimiseen strategisessa kontekstissa. (Islam & Stafford, 2017.)

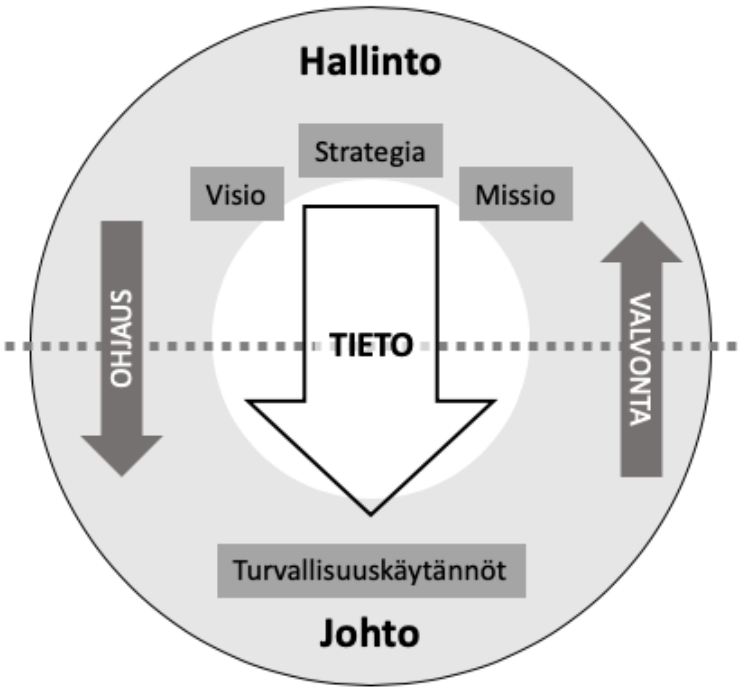
Kwonin, Ulmerin ja Wangin (2013) tutkimustulokset osoittavat, että tietohallintojohtajan kuuluminen yrityksen ylimpään johtoon sekä osallistuminen strategiseen suunnitteluun vaikuttaa negatiivisesti tietoturvallisuusloukkausten

[2] GDPR = EU:n yleinen tietosuoja-asetus, 2016/679 (engl. General Data Protection Regulation).

todennäköisyyteen. Tutkimuksessa kävi myös ilmi, että tulosperusteisesti palkattujen IT-johtajien yrityksissä tietoturvallisuusloukkausten riskit kasvoivat, kun taas kuukausipalkattujen IT-johtajien yrityksissä tietoturvallisuusloukkausten riskit pienenivät. Tutkijat argumentoivat tämän johtuvan siitä, että tietoturvallisuuden hallintatehtävät ovat usein luonteeltaan epävarmoja, jolloin kuukausipalkalla on tärkeämpi rooli IT-johtajien motivoinnissa pitkällä aikavälillä verrattuna tulosperusteisesti palkattuihin IT-johtajiin. (Kwon ym., 2013.)

## 4.2 Kyber- ja tietoturvallisuuden hallinnan viitekehys

Higgsin, Pinskerin, Smithin & Youngin (2016) mukaan kyberturvallisuuden hallinto (engl. governance) ja johtaminen (engl. management) tulisi erottaa toisistaan. Posthumus ja von Solms (2004) jakavat myös tietoturvallisuuden hallinnan viitekehyksessään hallintoon ja johtamiseen. Hallinto nähdään yrityksen ylimmän johdon sekä johtoryhmän osallistavana strategisena suunnannäyttäjänä (Posthumus & von Solms, 2004) ja kokonaisvastuullisena vaikuttajana (Higgs ym., 2016). Johtaminen keskittyy viitekehyksen mukaan enemmän strategian implementointiin ja toteuttamiseen (Posthumus & von Solms, 2004) sekä raportointiin operatiivisten toimenpiteiden onnistumisesta hallinnolle (Higgs ym., 2016). Tämä hallinnan viitekehys on visualisoitu kuviossa 5.




KUVIO 5 Yrityksen hallinnon ja johdon viitekehys tietoturvallisuuteen (Posthumus & von Solms, 2004 mukaan).

### 4.2.1 Hallinto

Johnson ym. (2008, s. 401) mukaan yrityksen ylimmän johdon ja johtoryhmän vastuulla on luoda yritykselle hallinnollinen kokonaisstrategia ja kehittää sitä jatkuvasti. Whitman ja Mattford (2003) tarkentaa, että johtoryhmän tulisi tuottaa sellainen tietoturvallisuuspolitiikka, joka osoittaa yrityksen johdon sitoutumisen tietoturvallisuuden toteuttamiseen ja joka tukee yrityksen missiota ja tavoitteita. Tietoturvallisuuspolitiikan kehittäminen osoittaa Posthumusin ja von Solmsin (2004) mukaan yrityksen ylimmän johdon tuen kokonaisvaltaiselle tietoturvallisuusstrategian perustamiselle ja implementoinnille. Julisch (2013) näkee hallinnon roolin tärkeänä päätettäessä turvallisuuden prioriteeteista, resursoinnista, panostuksista ja esimerkiksi siitä, mitkä prosessit ovat minkäkin omaisuuserän tai informaation riskienhallinnan takeina.

Hallitakseen ja ohjatakseen yrityksen tietoturvallisuusstrategian kehitystä ylin johto tarvitsee säännöllisiä valvontaraportteja (ks. kuvio 5) eri liiketoimintayksiköiden operatiivisilta johtajilta. Tämä antaa ylimmälle johdolle ja johtoryhmälle mahdollisuuden arvioida strategian vaikuttavuutta sekä säännellä ja parantaa tietoturvallisuusstrategiaa niiltä osin kuin se on tarpeen. (Posthumus & von Solms, 2004.)

### 4.2.2 Johtaminen

Tieto- ja kyberturvallisuuden johtaminen ilmenee turvallisuuspolitiikkojen (engl. security policy) määrittelynä hallinnon ohjaustoimien perusteella sekä näiden implementointina organisaation operatiiviseen toimintaan (Posthumus & von Solms, 2004). Johtamisen vastuualueisiin kuuluu niin strategian varsinainen jalkauttaminen ja toiminnan seuranta kuin myös raportointi takaisin ylimmälle johdolle jatkuvan strategiakehityksen tueksi. Johtamisen keskeinen osuus on myös eri liiketoimintayksiköiden johtajien sitoutuminen raportoimaan tietoturvallisuuspolitiikan toteutumisesta ja mahdollisista poikkeamista kussakin yksikössä. (Posthumus & von Solms, 2004.)

## 4.3 Implementointi

Onnistunut yritysstrategisen tieto- ja kyberturvallisuuden implementointi vaatii, että jokainen organisaation jäsen sitoutuu ja panostaa organisaation tietopääoman suojaamiseen ja turvaamiseen (Merete Hagen ym., 2008). Merete Hagen ym. (2008) argumentoivat lisäksi, että tietoturvallisuus voi jopa olla mekanismi kasvattamaan yrityksen tuottavuutta ja vähentämään kustannuksia. Posthumus ja von Solms (2004) näkevät edellä mainitut syyt tärkeiksi sille, että yritysten ylimmän johdon tulee käyttöönottaa tietoturvallisuuden hallinnon viitekehys osaksi strategista suunnittelua.

Bergeron, Raymond ja Rivard (2004) huomauttavat, että mikäli strateginen suunnittelu on implementoinnin liikkeellepaneva voima, on johdon huolehdittava siitä, että uuden tai tehostetun strategian implementointi toteutetaan samanaikaisesti IT-strategian kanssa. Tämä on keskeistä siksi, että IT-strategia voi tukea uuden yritysstrategian teknologisia vaatimuksia ja edellytyksiä, joita kyberturvallisuuden implementointi strategisella tasolla ja koko yrityksen laajuudessa edellyttää (Bergeron ym., 2004).

Rothrock ym. (2018) on koostanut lukuisista tutkimuksista 'parhaita käytäntöjä' kyberturvallisuuden implementoinnin edistämiseksi. Yritysjohdon on ymmärrettävä yksiselitteisesti turvallisuuden ja resilienssin avaintekijät sekä hyväksyttävä luottamustehtäviensä sisältämät vastuukysymykset. Tehtäviensä hoitamiseen johtajat tarvitsevat koulutusta, joka tarjoaa riittävästi tietoa ja ymmärrystä kyberturvallisuudesta, yrityksen kyvystä ylläpitää toimintakykyä muuttuvissa olosuhteissa, valmiudesta kohdata häiriöitä ja kriisejä sekä toiminnan palautumisesta. Johtajien tulee ymmärtää myös kyberturvallisuusriskien oikeudelliset vaikutukset. (Rothrock ym., 2018.)

Rothrockin ym. (2018) tutkimuskoosteiden puolesta argumentoivat myös von Solms ja von Solms (2004), joiden mukaan tietoturvallisuuden hallintaa koskevien kansainvälisten parhaiden käytäntöjen perusteella yritykset voivat oppia toisten yritysten menestyksekkäistä tietoturvallisuuskokemuksista, jotka ovat syntyneet todellisissa tilanteissa. Suuri osa kaikista tietoturvallisuusuhkista, niistä aiheutuvista riskeistä ja valituista vastatoimista ovat von Solmsin ja von Solmsin (2004) mukaan samoja kaikille yrityksille. Tietoturvallisuuden strategisen implementoinnin avuksi tulisi siis ottaa jokin valmis 'parhaiden käytäntöjen' kokoelma tai viitekehys (von Solms & von Solms, 2004).

Lukuisilla johdon toiminnoilla ja erityisesti tietoturvallisuuspolitiikan kehittämisellä, toteuttamisella, tietoisuuden lisäämisellä, vaatimuksenmukaisuuskoulutuksella, tehokkaan yritystietojärjestelmän kehittämisellä, teknisen infrastruktuurin hallinnalla, liiketoiminnan ja teknologian linjaamisella sekä henkilöstöhallinnolla on merkittävä vaikutus tietoturvallisuuden hallinnan laatuun (Soomro, Shah & Ahmed, 2016). Henkilöstön kouluttamisen ei kuitenkaan tarvitse olla monimutkainen prosessi, vaan selkeä polku aloittaen tietoisuuden lisäämisestä, siirtyen koulutusten kautta valvontaan ja ylläpitävään vaiheeseen (Kim, 2017).

Lisäksi tavanomaisesta IT-osaston toiminnasta poikkeavat, kyberturvallisuudelle spesifit operatiiviset tehtävät, kuten verkon valvonta ja analysointi tulisi mahdollisuuksien mukaan osoittaa erityiselle tietoturvallisuudesta vastaavalle osastolle (Ben-Asher & Gonzalez, 2015). Yritysorganisaation IT-osaston tekninen osaaminen on merkittävässä roolissa kyberturvallisuuden kannalta, mutta aivan yhtä tärkeää – jos ei jopa tärkeämpää – on antaa näille asiantuntijoille tarpeeksi vapauksia ja resursseja tutkia kyberturvallisuuden teknologioita, trendejä, ilmiöitä ja suunnitella prosesseja sekä työkaluja, jotta organisaatio voi varautua myös tulevaisuuden haasteisiin (Kim, 2017).

Implementoitua kyberturvallisuusstrategiaa tulee mitata ja valvoa jatkuvaluonteisesti, jotta sen vaikutuksia voidaan arvioida ja arvioiden perusteella ohjata strategiaa korjaavia toimenpiteitä. Käytännössä yrityksen kyberturvallisuudesta vastaavan johdon tulee saada säännöllisesti raportti siitä, mitä tietoturvapolitiikkoja noudatetaan ja mitkä ovat mahdollisesti uhattuina tai toimenpiteiden ulkopuolella. (von Solms & von Solms, 2004.)

## 4.4 Vaikuttavuuden arviointi ja saavutettavat hyödyt

Dhillon ja Backhouse (2001) ovat yritysjohdon suhtautumista tietoturvallisuuteen tutkiessaan havainneet käänteisen suhteen muodollisten järjestelmien, kuten tietoturvallisuuspolitiikkojen, -menettelyiden ja -valvonnan kehittämisessä sekä tietoisuutta lisäävien toimien välillä. Dhillonin ja Backhousen (2001) tutkimustulokset saavat tukea Merete Hagenin ym. (2008) tekemästä tutkimuksesta, jonka mukaan vähiten toteutetut, tietoisuutta lisäävät toimenpiteet ovat arvioitu olleen vaikuttavimpia toimenpiteitä edistämään tietoturvallisuutta yrityksessä. Vastavuoroisesti teknishallinnollisia, eli niin sanotusti muodollisia toimenpiteitä (politiikat; menettelyt; valvonta ja muut hallinnon työkalut) on toteutettu eniten, mutta niiden arvioidaan kuitenkin olevan vähemmän vaikuttavia yrityksen tietoturvallisuuden edistämisessä kuin tietoisuutta lisäävät toimenpiteet (Merete Hagen ym., 2008). Tämän yritysorganisaation tietoturvallisuustoimien toteuttamisen ja toimenpiteiden vaikuttavuuden arvioinnin välisen käänteisen suhteen viitekehyksen Merete Hagen ym. (2008) esittävät metaforisena, neliportaisena listana:

1. tietoturvallisuuspolitiikka;
2. menettelyt ja valvonta;
3. työkalut ja menetelmät; ja
4. tietoisuuden luominen (ja lisääminen) tietoturvallisuudesta.

Mitä korkeampi asema käsitteellä tai toimenpiteellä on listalla, sitä vaikuttavampaa tietoturvallisuuden hallinta on ja vastavuoroisesti, mitä matalampi asema on, sitä vaikuttavampaa on tietoisuuden lisääminen tietoturvallisuudesta yritysorganisaatiossa (Merete Hagen ym., 2008). Dhillonin ja Backhousen (2001) mukaan tietoturvallisuuden hallinta on perinteisesti korostanut muodollisia hallintatapoja, jotka ovat listan yläpäässä ja jopa siten, että tietoturvallisuuden on katsottu olevan kunnossa, kun muodolliset toimenpiteet ovat suoritettu. Merete Hagen ym. (2008) korostavat, että tietoturvallisuuden inhimillisen puolen huomioiminen ja sitä kautta tietoturvallisuuden tietoisuuden lisääminen on keskeisessä asemassa yritykseen kohdistuvien tietoturvallisuusriskien vähentämisessä.

Khansa ja Liginlal (2009) ovat tutkimuksessaan osoittaneet suoria hyötyjä yrityksen tietoturvallisuuteen kohdistuvista investoinneista, joista merkittävin on yleisesti ottaen parempi suojaus ja kyky kestää hyökkäyksiä. Tästä seuraa se,

että yritykseen kohdistuvien hyökkäysten vaikutukset ovat vähäisempiä, mistä seuraa entistä vähemmän rahallisia menetyksiä ja negatiivista julkisuutta (Khansa & Liginlal, 2009). Boonen (2017) mukaan hyvin toteutettuna ja ylläpidettynä kyberturvallisuus ei siis ole pelkästään puolustusstrategia, vaan koko yrityksen suorituskyvyn kannalta merkittävä mahdollistaja. Organisaatiot, joiden ylin johto priorisoi kyberturvallisuutta, eivät pelkästään minimoi riskejä vaan myös edistävät ja mahdollistavat yrityksen liiketoiminnallisia tavoitteita (Boone, 2017). Khansa ja Liginlal (2009) havaitsivat tutkimuksessaan, että edellä mainitut hyödyt vaikuttavat myönteisesti yrityksen arvostukseen osakemarkkinoilla ja välillisesti myös osakekurssiin.

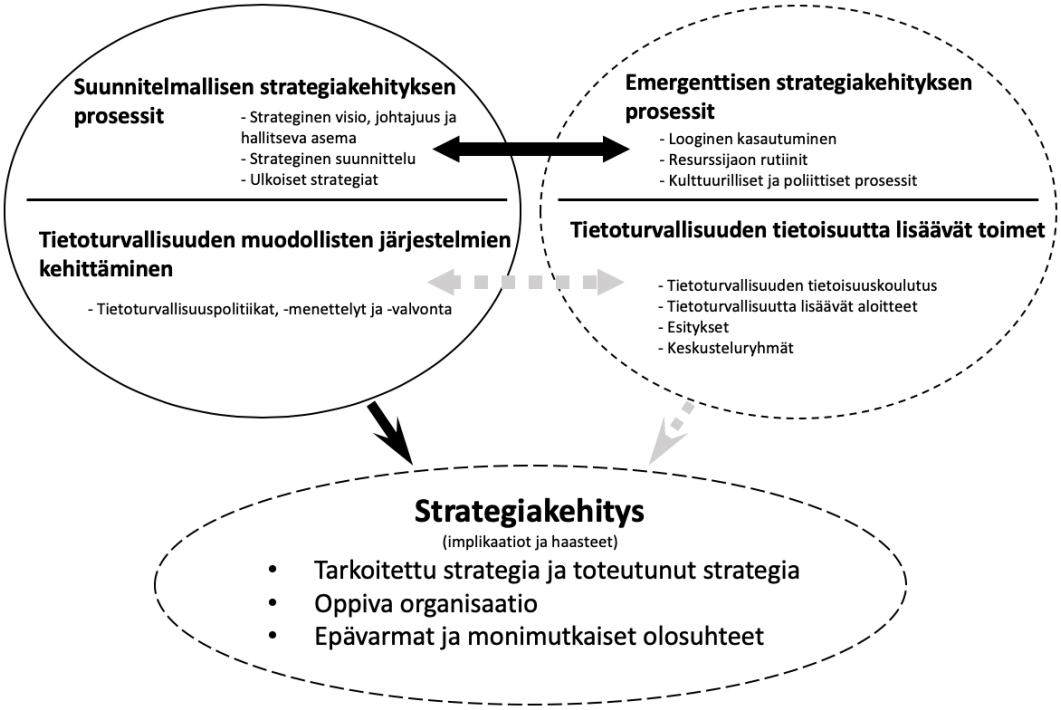
Khansan ja Linginlalin (2009) tutkimustulokset saavat tukea Merete Hagenin ym. (2008) tutkimuksesta, jonka mukaan tietoturvallisuustoimet vaikuttavat positiivisesti sijoituksen tuottoon (ROI[3]) ja viittaavat tietoturvallisuuden taloudelliseen lähestymistapaan, johon Gordon ja Loeb (2002) ovat kehittäneet taloudellisen mallin. Gordon ja Loeb (2002) argumentoivat, että yrityksen tulisi maksimoida odotetut tuotot sijoituksilleen, jotka ovat toteutettu tietoturvallisuuden parantamiseksi ja tiedon suojaamiseksi. Tässä mielessä tietoturvallisuustoimien tehokkuutta ymmärretään kyseessä olevien toimenpiteiden kyvyksi antaa sijoitukselle positiivinen tuotto suhteessa investointiin (Gordon & Loeb, 2002).

## 4.5 Strateginen viitekehys

Dhillonin ja Backhousen (2001) tutkimustuloksia tietoturvallisuuden muodollisten järjestelmien kehittämisen ja tietoisuutta lisäävien toimien välillä voidaan yhdistää Johnsonin ym. (2008, s. 400-416) näkemyksiin strategian kehitysprosessista. Samaan tapaan kuten Dhillon ja Backhouse (2001) näkevät tietoturvallisuuden hallinnan korostavan perinteisesti tietoturvallisuuden muodollisten järjestelmien kehittämistä, osoittavat Johnson ym. (2008, s. 401-407) suunnitelmallisen strategiakehityksen prosesseissa samankaltaisia perinteisiä, muodollisia tapoja.

Johnsonin ym. (2008, s. 407-416) näkemys emergentistä strategiakehityksestä pohjautuu loogiseen kasautumiseen, resurssijaon rutiineihin sekä kulttuurillisiin ja poliittisiin prosesseihin. Nämä menetelmät ja havainnot ovat hyvin samankaltaisia Dhillonin ja Backhousen (2001) informaation käsittelyyn liittyvien kulttuuristen havaintojen kanssa, joiden mukaan sosiaalinen maailma – jota Johnsonin ym. (2008, s. 407-416) emergentti strategiakehityksen näkemys edustaa – on myös emergentti ja yksittäisten organisaation jäsenten kontribuutioiden kautta kehittyvä. Tämä on havainnollistettu kuviossa 6.

[3] ROI = Engl. Return on Investment. Sijoitetun pääoman tuottoaste, joka kertoo, kuinka paljon sijoitettu pääoma on tuottanut.




KUVIO 6 Strateginen viitekehys visualisoituna (Johnson ym. 2008, s. 400, muokattu; Dhillon & Backhouse, 2001)

Johnson ym. (2008, s. 419-422) käsittelevät strategiakehitysprosessin tarkoitettua sekä toteutunutta strategiaa ja toteavat etteivät suunnitelmalliset ja emergentit strategiakehityksen prosessit sulje toisiaan pois strategisessa suunnittelussa, vaan ovat pikemminkin komplementaarisia toisilleen (Johnson ym., 2008, s. 400). Tietoturvallisuuden osalta Merete Hagenin ym. (2008) viitekehys kuitenkin osoittaa, että tietoturvallisuuden muodollisten järjestelmien kehittäminen ja tietoturvallisuuden tietoisuutta lisäävien toimien välillä vallitsee käänteinen suhde, jota kuviossa 6 kuvataan harmaalla katkoviivalla.

Yksittäisten työntekijöiden toiminnalla on tärkeä rooli turvallisuusriskien huomioimisessa (Huang ym., 2010). Työntekijöiden tulee olla tietoisia turvallisuusuhkista, heidät tulee kouluttaa organisaation tietoturvallisuusstrategian mukaisesti ja tietoisuutta tulee pitää yllä säännöllisillä täydennyskoulutuksilla (Kim, 2017). Kun tarkastellaan lisäksi Kirschin ja Bossin (2007) tutkimustulosta, jonka mukaan on epätodennäköistä, että yksittäisten työntekijöiden osuus tietoturvallisuuden toteuttamisessa otetaan huomioon, voidaan osoittaa, että strategisen viitekehyksen mukaista tietoturvallisuuden tietoisuutta lisäävät toimet eivät tuo arvoa varsinaiseen strategiakehitykseen parhaalla mahdollisella tavalla.

Julischin (2013) mukaan monella yrityksellä on aukkoja kyberturvallisuutensa suhteen henkilöstön koulutuksen osalta. Hillerin ja Russelin (2013) ajatukset tukevat tätä näkemystä osana yrityksen kyberturvallisuusriskin elementtejä toteamalla, että haavoittuvuuksia aiheuttaa myös yritysten työntekijöiden huolimaton toiminta. Inhimillisen tekijän vaikutus on merkittävä tieto- ja kyberturvallisuuden riskien toteutumisessa (Gonzalez & Sawicka, 2002; Gratian ym., 2018),

ja tämän takia yritysjohdon tulisi strategisessa suunnittelussaan huomioida tietoturvallisuuden tietoisuutta lisäävät toimet tasavertaisena strategiakehityksen kannalta. Albrechtsenin ja Hovdenin (2010) sekä Merete Hagenin ym. (2008) tutkimustulokset henkilöstön aktiivisen osallistumisen positiivisista vaikutuksista tietoturvallisuuden tietoisuuden sekä tietoturvallisen käyttäytymisen suhteen tukevat tätä ajatusta.

# 5 YHTEENVETO

Tässä tutkielmassa tarkasteltiin kyberturvallisuuden ilmenemistä yritysstrategiassa. Lisäksi tutkielman tavoitteena oli selvittää miten kyberturvallisuutta tulisi johtaa ja hallita yritysstrategisesti, sekä tarkastella millaisia hyötyjä yritys voi kyberturvallisuuden yritysstrategisen aseman kautta saavuttaa. Tässä tutkielmassa strategiaa tarkasteltiin nimenomaisesti yritysstrategian näkökulmasta, määriteltiin yritysstrategian elementtejä sekä käytiin läpi yritysstrategian tutkimusta ja sen haasteita. Aineiston perusteella osoitettiin myös, että strategian tutkimus on kehittynyt valtavasti 1960-luvun parhaista käytännöistä ja nykyaikaiset strategiat on jaettu usealle eri tasolle, joita hallitaan yritysstrategian tasolta. Kyberturvallisuuden kehittäminen on jatkuvaa työtä, ja siksi yritysten ja organisaatioiden tuleekin innovoida rikollisia nopeammin turvatakseen toimintansa. Lisäksi on hyvä ymmärtää, että informaatioteknologiaa hyödyntävät yritykset ovat verkottuneet palveluketjuiksi, joissa yhden ketjun jäsenen heikko kyberturvallisuuden taso vaikuttaa kaikkiin ketjun jäseniin. Valtioiden ja hallitusten kriittistä huoltovarmuutta ylläpitävä infrastruktuuri on usein yksityisten yritysten hallussa.

Useat tutkijat ovat yksimielisiä siitä, että kyberturvallisuus ei ole pelkästään tekninen asia, vaan yrityksen johdon tulee myös sitoutua sen toteuttamiseen sekä ottaa vastuu myös koko henkilöstön sitouttamisesta. Yritysten kyberturvallisuudessa henkilöstön kouluttaminen on keskeisessä asemassa, ja eri tyyppisille ihmisille tuleekin räätälöidä eri tyyppisiä koulutuksia, jotta oppimiskokemus olisi mahdollisimman vaikuttava. Koulutuksen tulee olla säännöllistä ja myös itse koulutuksen vaikuttavuutta tulee mitata ja kehittää.

Yrityksen tieto- ja kyberturvallisuuden hallintajärjestelmän lähtökohdaksi tulee valita valmis 'parhaiden käytäntöjen' kokoelma, kuten esimerkiksi jokin kansainvälisesti vakiintunut ja yleisesti käytetty informaatioturvallisuuden hallintajärjestelmän standardi. Vastauksena ensimmäiseen tutkimuskysymykseen "miten kyberturvallisuus ilmenee yritysstrategiassa?", havaittiin aineiston perusteella kyberturvallisuuden ilmenevän yritysstrategiassa erityisesti yrityksen ylimmän johdon vastuunkannon ja sitoutuneisuuden kautta, niin hallinnon kuin johtamisenkin ulottuvuuksissa. Aineiston perusteella tässä on kuitenkin vielä parannettavaa etenkin tietohallinnossa, joka on tietoturvallisuuden käytännön toteuttamisesta yleensä päävastuussa. Tietohallinnon osallistumisella

strategiseen päätöksentekoon on merkittävä rooli tietoturvallisuuden paranemiseen organisaatiossa. Tämä on keskeinen tekijä linjatessa yritysstrategiaa ja tietoturvallisuutta yhteiseen päämäärään.

Toiseen tutkimuskysymykseen, eli ”millaisia hyötyjä yritys voi saavuttaa integroimalla kyberturvallisuuden osaksi yritysstrategiaa?” vastauksena havaittiin aineiston perusteella yrityksen tieto- ja kyberturvallisuuden parantuminen yleisesti niin tietoisuuden kuin suojautumiskyvyn kannalta. Kyberturvallisuuden strategisen johtamisen tavoitteena on parantaa ja ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä parantaa valmiuksia kohdata häiriöitä ja kriisejä. Lisäksi yritysten tarkoituksena on kehittää ja ylläpitää kyvykkyyttä palautua poikkeustilanteista. Hyökkäysten sietokyvyn parantumisesta seuraa vähäisempiä rahallisia menetyksiä ja vähemmän negatiivista julkisuutta. Kyberturvallisuuden huomioiminen yritysstrategisella tasolla mahdollistaa ja voi jopa edistää yrityksen liiketoiminnallisia tavoitteita. Aineistosta havaittiin myös, että kyberturvallisuuden yritysstrategisen integraation kautta yritys voi saavuttaa konkreettisia, rahassa ja arvossa mitattavia hyötyjä, kuten esimerkiksi yrityksen arvonnousua osakemarkkinoilla.

Strategisessa suunnittelussa sekä perinteinen että emergenttinen strategiaprosessi ovat komplementteja toisilleen, kun taas tietoturvallisuudessa perinteiset, teknishallinnolliset toimenpiteet sulkevat pois emergenttejä, sosiaalisuuteen ja yrityksen kulttuuriin liittyviä tietoturvallisuuden tietoisuutta lisääviä toimia. Tämä vaikuttaa negatiivisesti tietoturvallisuusstrategian kehittymiseen ja kattavuuteen. Tilanne kuvaa tieteelliseen aineistoon perustuen sitä, miten yritysjohto on perinteisesti ajatellut tietoturvallisuuden olevan kunnossa, kun muodolliset järjestelmät kuten politiikat, menettelyt ja valvonta on paikallaan.

Tutkielman aineistosta havaittiin, että yritysjohdon motiivina on usein välttää epävarmuutta ja monimutkaisia olosuhteita. Usein kuitenkin menestyksekkäimmät strategiat ovat niitä, joiden syntytarina ei ollut lainkaan varma, yksinkertainen tai suoraviivainen. Aineistosta kävi myös ilmi, että nykyisessä kyberturvallisuuden ja yritysstrategian tietämyksessä olevat puutteet ovat nimenomaisesti kyberturvallisuuden osuudessa yrityksen kokonaisstrategiassa. Kyberturvallisuus nähdään valitettavasti edelleen muista toiminnoista erillisenä asiana, joka huomioidaan erikseen IT-osaston toimesta. Kyberturvallisuus tulisi nähdä enemmän myös strategisena, kaikkialle kuuluvana asiana, joka edesauttaa kyberturvallisuuden integraatiota yritysstrategiaan samalla menestyksen kannalta merkittävällä tasolla, jolla esimerkiksi liiketoiminta nähdään yritysstrategiassa.

Tutkielman rajoitteista mainittakoon, että tutkielmasta oli rajattu pois kyberturvallisuuden osalta teknologiat, trendit ja ilmiöt, sillä ne ovat omia kokonaisuuksiaan ja laajentaisivat tutkielmaa liikaa tavoitteen kannalta epäolennaiseen suuntaan. Myös viestintä, joka on tietoturvallisen yrityskulttuurin kehittämisen yksi keskeisimpiä kysymyksiä, oli rajattu tämän tutkimuksen ulkopuolelle. Lisäksi tutkielma rajattiin strategian osalta kattamaan vain yritysstrategia.

Nämä rajoitukset rajoittivat tutkielman soveltamisalaa, mutta toisaalta auttoivat keskittymään tutkimuskysymysten kannalta oleellisiin asioihin.

Jatkotutkimusaiheina mielenkiintoisia ja hyödyllisiä olisivat yritysten kyberturvallisuuden toteuttamiseen liittyvien ulkoistusten ja alihankintojen toimivuus, vaikuttavuus sekä mahdolliset riskitekijät. Lisäksi edellä mainittujen toteutusmallien soveltuvuudesta ja implementoinnista yritysstrategian näkökulmasta voisi olla kysyntää niin akateemisten kuin elinkeinoelämän toimijoiden keskuudessa. Myös kyberturvallisuuden hallintajärjestelmien implementointien vaikutusten arviointi olisi mielenkiintoinen ja tarpeellinen jatkotutkimusaihe. Viestinnän merkitys etenkin tietoturvallisuuden tietoisuutta lisäävien toimien kehittämisessä olisi myös potentiaalinen jatkotutkimusaihe.

# LÄHTEET

Andrews, K. R. (1997). A reader in the resource-based perspective. Foss, N. J. (toim.), (pp. 52-59). New York, NY, United States: Oxford University Press. ISBN-13: 978-0198781790.

Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432-445.

Alreemy, Z., Chang, V., Walters, R. & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). International Journal of Information Management, 36(6), 907-916.

Ben-Asher, N. & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61.

Bergeron, F., Raymond, L. & Rivard, S. (2004). Ideal patterns of strategic alignment and business performance. Information & management, 41(8), 1003-1020.

Boone, A. (2017). Cyber-security must be a C-suite priority. Computer Fraud & Security, 2017(2), 13-15.

Bouhali, R., Mekdad, Y., Lebsir, H. & Ferkha, L. (2015). Leader roles for innovation: Strategic thinking and planning. Procedia-Social and Behavioral Sciences, 181, 72-78.

BSI (1999). BS7799-1:1999, Information Security Management Part 1: Code of Practice for Information Security Management. British Security Institute: UK.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

Conti, M., Dargahi, T. & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities (pp. 1-6). Springer International Publishing.

Dhillon, G. & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.

Dutta, A. & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87.

Euroopan parlamentti ja Euroopan unionin neuvosto. (2016). EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679 luonnollisten

henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). EUR-Lex.

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

Grant, R. M. & Jordan, J. (2015). Foundations of strategy (2. ed.). John Wiley & Sons. ISBN-13: 978-0470971277.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. computers & security, 73, 345-358.

Gonzalez, J. J. & Sawicka, A. (2002). A framework for human factors in information security. In Wseas international conference on information security, Rio de Janeiro (pp. 448-187).

Henderson, B. D. (1989). The origin of strategy. Harvard business review, 67(6), 139-143.

Heracleous, L. (1998). Strategic thinking or strategic planning? Long range planning, 31(3), 481-487.

Higgs, J. L., Pinsker, R. E., Smith, T. J. & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. Journal of Information Systems, 30(3), 79-98.

Hiller, J. S. & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. Computer Law & Security Review, 29(3), 236-245.

Huang, D. L., Rau, P. L. P. & Salvendy, G. (2010). Perception of information security. Behaviour & Information Technology, 29(3), 221-232.

Hutzschenreuter, T. & Kleindienst, I. (2006). Strategy-Process Research: What Have We Learned and What Is Still to Be Explored. Journal of Management, 32(5), 673–720.

Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

ISO/IEC. (2004). ISO/IEC TR 13335-1:2004. Information technology security techniques management of information and communications technology security part 1: concepts and models for information and communications

technology security management. ISO/IEC, JTC 1, SC27, WG 1 2004. ISO, Geneva.

ISO/IEC. (2018). ISO 9004:2018 Quality Management. Quality of an organization. Guidance to achieve sustained success. ISO, Geneva.

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

Johnson, G., Scholes, K. & Whittington, R. (2008). Exploring corporate strategy (8. ed.). Harlow; Munich: Prentice Hall Financial Times. ISBN-13: 978-0273711919.

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. Computer Networks, 57(10), 2206-2211.

Kayworth, T. & Whitten, D. (2012). Effective Information Security Requires a Balance of Social and Technology. MIS Quarterly Executive, Vol. 9, No. 3, 2010; Mays Business School Research Paper No. 2012-52.

Khansa, L. & Liginlal, D. (2009). Quantifying the benefits of investing in information security. Communications of the ACM, 52(11), 113-117.

Kim, J. (2017). Cyber-security in government: reducing the risk. Computer Fraud & Security, 2017(7), 8-11.

Kirsch, L. & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. ICIS 2007 proceedings, 103.

Kwon, J., Ulmer, J. R. & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. Journal of Information Systems, 27(1), 219-236.

Lehto, M. & Kähkönen, A. (2015a). Kyberturvallisuuden kansallinen osaaminen. Jyväskylä: Jyväskylän yliopisto.

Lehto, M. & Neittaanmäki, P. (Eds.). (2015b). Cyber security: Analytics, technology and automation. Switzerland: Springer International Publishing.

Libicki, M. C. (2007). Conquest in cyberspace: National security and information warfare. Cambridge University Press. ISBN-13: 978-0521692144.

Merete Hagen, J., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377-397.

Mintzberg, H. (1994). The fall and rise of strategic planning. Harvard Business Review, 72(1), 107-114.

Minzberg, H., Lampel, J., Quinn, J. B. & Ghoshal, S. (2003). The strategy process: Concepts, contexts, cases (4th ed.). Harlow, England: Pearson Education Ltd. ISBN-13: 978-0273651208.

Osakeyhtiölaki 2006/624. (2006). Annettu Helsingissä 21.7.2006.

Pettigrew, A. M. (1992). The character and significance of strategy process research. Strategic management journal, 13(S2), 5-16.

Porter, M. E. (1985). Competitive advantage (25. print. ed.). New York: Free Press.

Porter, M. E. (1996). From competitive advantage to corporate strategy. In M. Goold & K. Sommers Luchs (Eds.), Managing the multibusiness company: Strategic issues for diversified groups (pp. 285-314). London, UK: Routledge. ISBN-13: 978-0415132695.

Posthumus, S., von Solms, R. (2004). A framework for the governance of information security. Computers & Security, Volume 23, Issue 8, 2004, Pages 638-646, ISSN 0167-4048.

Rothrock, R. A., Kaplan, J. & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. MIT Sloan Management Review, 59(2), 12-15.

Sanastokeskus TSK (2013). Tietohuollon sanasto, TSK 20. Sanastokeskus TSK ry. ISBN-10: 952-9794-00-2.

Sanastokeskus TSK. (2018). Kyberturvallisuuden sanasto, TSK 52. Sanastokeskus TSK ry. Huoltovarmuuskeskus. Turvallisuuskomitea. ISBN-13: 978-952-5608-49-6.

Siponen, M., Mahmood, M. A. & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.

Siponen, M. T. & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38(1), 60-80.

Soomro, Z. A., Shah, M. H. & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Suomen kyberturvallisuusstrategia. (2013). Turvallisuus- ja puolustusasiain komitean sihteeristö. Forssa print. Helsinki. ISBN-13: 978-951-25-2433-4.

Szulanski, G., Porac, J. F. A. & Doz, Y. L. (2005). Strategy process. Amsterdam: JAI Press Inc. ISBN-13: 978-0762312009.

Van de Ven, A. H. (1992). Suggestions for studying strategy process: A research note. Strategic management journal, 13(S1), 169-188.

von Solms, B. (2001). Corporate Governance and Information Security. Computers & Security, Volume 20, Issue 3, 2001, Pages 215-218, ISSN 0167-4048.

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, Volume 38, 2013, Pages 97-102, ISSN 0167-4048.

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.

Whitman, M. E. & Mattord, H. J. (2011). Principles of information security. Cengage Learning. ISBN-13: 978-1-111-13821-9.

Whittington, R. (2007). Strategy practice and strategy process: family differences and the sociological eye. Organization studies, 28(10), 1575-1586.