Tietoturvainvestoinnit ja uhkatiedon jakaminen taloustieteellisestä näkökulmasta

Anna-Maija Juuso ja Rauli Svento

Tietoturvainvestoinnit ovat taloudellisia päätöksiä, joita toimijat tekevät sen tiedon pohjalta, mitä heillä on käytettävissään. Jatkuvasti muuttuvasta uhkaympäristöstä ja ulkoisvaikutuksista johtuen tämä tieto on usein vajavaista. Tiedon hankkiminen tietoturvauhista ja -hyökkäyksistä voi olla kallista ja aikaa vievää. On ehdotettu, että organisaatiot jakaisivat tiedonhankintakustannuksia tekemällä yhteistyötä ja jakamalla toisilleen tietoturva-aiheista tietoa, eli uhkatietoa. Tällainen avoin tietoturvayhteistyö poikkeaa kuitenkin monin tavoin perinteisestä tietoturvatyöskentelystä. Keväällä 2017 toteutimme tietoturvakyselyn suomalaisille yrityksille Kyberturvallisuuskeskuksen avustuksella. Kyselyn tarkoituksena oli kartoittaa, miten suomalaiset organisaatiot investoivat tietoturvaan sekä tutkia heidän halukkuuttaan ja mahdollisuuksiaan tehdä avoimempaa tietoturvayhteistyötä. Tätä tarkoitusta varten hyödynnämme malleja uusien innovaatioiden hyväksymisestä ja tutkimme, mitkä tekijät kannustavat organisaatioita avoimeen tietoturvayhteistyöhön ja mitkä tekijät aiheuttavat vastustusta. Tässä artikkelissa vertailemme kyselyn tuloksia teoreettisiin tietoturvainvestointimalleihin ja pohdimme, milloin avoin tietoturvayhteistyö kannattaa.

"Maailmassa mikään muu ei ole varmaa, paitsi kuolema, verot ja bugit koodissa", kertoo tietoturva-alalla muokattu vanha sanonta. Veronkannon tehostuminen 1700-luvulla teki veronmaksusta vääjäämätöntä. Uusi digiaika sekä tieto-ja viestintäteknologian (ICT) laaja-alainen käyttöönotto kaikilla talouden eri osa-alueilla on puolestaan tehnyt meidät riippuvaisiksi bugisista eli haavoittuvaisista[1] ohjelmistoista sekä

[1] *Bugit ovat ohjelmointi- ja suunnitteluvirheitä, jotka altistavat järjestelmät mahdollisille hyökkäyksille (Lähde https://cwe.mitre.org). Ohjelmointivirheet ovat puhtaita kirjoitus- tai kielioppivirheitä koodissa. Osa suunnitteluvirheistä on ollut aikoinaan tietoisia suunnittelupäätöksiä, mutta digitaalisen toimintaympäristön nopeiden ja ennaltaarvaamattomien muutosten myötä näistä päätöksistä on tullut tietoturvahaavoittuvaisuuksia.*

KTM Anna-Maija Juuso (anna-maija.juuso@oulu.fi) on tohtorikoulutettava ja FT Rauli Svento (rauli.svento@oulu.fi) on taloustieteen professori Oulun yliopiston kauppakorkeakoulussa. Kiitämme rahoituksesta Suomen Akatemian yhteydessä toimivaa Strategisen tutkimuksen neuvostoa (BCDC Energy AKA292854), Suomen Akatemiaa (*Regulation and dynamic pricing for energy systems* REDYFLEZ 288957) ja Wihurin rahastoa. Kiitämme asiantuntija-avusta Miikka Salosta ja Juhani Erosta Kyberturvallisuuskeskuksesta sekä anonyymia lausunnonantajaa ja aikakauskirjan toimitusta hyödyllisistä kommenteista.

globaaleista viestintäverkoista. Digitalisaatio muokkaa toimintatapoja ja markkinoiden rakenteita luoden uusia mahdollisuuksia yritystoiminnalle, innovaatiolle ja sosiaaliselle kanssakäymiselle. Kehityksen kääntöpuolena ovat globaaliin kybertoimintaympäristöön liittyvät tietoturvaongelmat. ICT-hyödykemarkkinoiden erityispiirteet johtavat siihen, ettei tuotteiden tietoturvallisuus ole aina riittävä. Samanaikaisesti globaalien viestintäverkkojen ansiosta haavoittuvaisia laitteita vastaan voidaan hyökätä pienin kustannuksin mistä päin maailmaa tahansa. Vaikka haavoittuvuudet ohjelmistoissa ovat teknisiä ongelmia, syyt ohjelmistojen haavoittuvaisuuteen ovat usein taloudellisia. Jos järjestelmän tietoturvasta vastaava taho ei kärsi tietoturvan pettäessä, niin sillä ei välttämättä ole riittävän hyvää kannustinta huolehtia tietoturvallisuudesta (Anderson ja Moore 2006). Usein kannustimien puute johtuu epäsymmetrisestä informaatiosta ja ulkoisvaikutuksista (Kox ja Straathof 2013). Seuraavat kaksi esimerkkiä havainnollistavat, kuinka nämä tekijät vaikuttavat toimijoiden tekemiin tietoturvainvestointipäätöksiin.

Keväällä 2017 *WannaCry*-kiristysohjelma halvaannutti Ison Britannian julkisen terveydenhuollon, National Health Servicen palvelut. Tietoturvaongelma olisi ollut ennakoitavissa ja havaittavissa: Haittaohjelma hyödynsi vanhaa haavoittuvuutta Microsoft Windows XP-käyttöjärjestelmässä. Jo käytöstä poistettua käyttöjärjestelmää ei ole enää virallisesti tuettu vuoden 2014 jälkeen, mutta siitä riippuvaisille organisaatioille oli tarjottu mahdollisuus ostaa tuki. Tietoturva-asiantuntijoiden varoituksista huolimatta Britannian terveysministeriö päätti olla maksamatta tuesta 5,5 miljoonaa puntaa (BBC 2017). Se ei myöskään korvannut käyttöjärjestelmää vaan haavoittuvainen järjestelmä jäi käyttöön. Ehkä siitä syystä, että suurella yleisöllä ei ole mitään keinoa todentaa terveyspalveluiden tietoturvallisuutta, National Health Servicen johto katsoi, että siitä pystyttiin säästämään. Suurista haitoista huolimatta *WannaCry*-hyökkäystä ei ollut kohdistettu suoranaisesti National Health Servicen järjestelmiin. vaan kaikkiin haavoittuviin XP-järjestelmiin.

Syyskuussa 2016 suosittu *Krebs on Security* -tietoturvablogi joutui toistaiseksi historian suurimman palvelunestohyökkäyksen kohteeksi. Hyökkääjät tukkivat sivuston lähettämällä yli 600 gigabittiä liikennettä sekunnissa (Krebs 2017). Asiantuntijoiden mukaan hyökkäykseen osallistui jopa satojen tuhansien haittaohjelmien avulla hallittujen orjatietokoneiden muodostama verkosto eli botnetti.[2] Mikä teki tästä hyökkäyksestä poikkeuksellisen – sen koon lisäksi – oli se, että suurin osa orjalaitteista ei ollut perinteisiä tietokoneita vaan erilaisia älykkäitä laitteita ja esineitä, kuten nettikameroita ja diginauhureita. Tällaisiin laitteisiin viitataan usein termillä esineiden Internet (*Internet of Things*, IoT). Yksittäisten IoT-laitteiden suoritusteho on pieni, eikä niiden tietoturvaan investoida juuri lainkaan. Hyökkääjät saivat kaikki laitteet hallintaansa hyödyntämällä muutamaa kymmentä tehdasasetuskäyttäjänimeä ja -salasanaa.

Edelliset esimerkit osoittavat, että keskinäisriippuvaisessa globaalissa kybertoimintaympäristössä tietoturvainvestointien kustannus- ja hyötylaskelmat eivät voi perustua vain

[2] *Botnetti tai bottiverkko on joukko yhteen liitettyjä koneita, joiden avulla voidaan suorittaa koordinoidusti suurta laskentatehoa vaativia tehtäviä. Rikolliset kaappaavat haittaohjelmien avulla muiden koneita omiin bottiverkkoihinsa ja hyödyntävät näitä orjaverkkoja mm. palvelunestohyökkäyksissä ja virtuaalivaluuttojen louhimisessa.*

yhden toimijan laskelmiin. Tietojärjestelmien samankaltaisuudesta johtuen samat tietoturvauhat leviävät nopeasti ja koskettavat toimijoita maailman laajuisesti. Keksittyään toimivan hyökkäyskeinon hyökkääjät hyödyntävät samoja toimintatapoja, työkaluja ja tekniikoita myös muissa hyökkäyksissä. Jakamalla tietoa tietoturvauhista toimijat voivat lyhentää hyökkäyksen hyödyntämisaikaa ja vähentää uhrien määrää. Onkin ehdotettu, että tietoturvahaasteisiin liittyvän tiedon, eli niin kutsutun uhkatiedon, jakaminen voisi parantaa eri toimijoiden tietoturvatietoisuutta ja luoda edellytyksiä turvallisemmalle kybertoimintaympäristölle.

Tässä artikkelissa tarkastelemme organisaatioiden tietoturvainvestointeja sekä teorian että empiirisen aineiston avulla. Aluksi jaksossa 1 käsittelemme tietoturvaan ja kybertoimintaympäristöihin liittyvää sanastoa. Jaksossa 2 käsittelemme tietoturvainvestointimalleja. Kirjallisuuskatsauksen avulla tarkastelemme tietoturvaa hyödykkeenä sekä tutkimme turvallisuusinvestointien ulkoisvaikutuksia ja tiedon epäsymmetrian vaikutuksia tietoturvallisuuteen. Jaksossa 3 puhumme avoimesta tietoturvayhteistyöstä ja jaksossa 4 esittelemme tapoja tutkia uhkatiedon jaon ja muiden teknisten innovaatioiden omaksumista. Kerromme myös, kuinka hyödynsimme näitä malleja kyselytutkimuksessamme. Jaksossa 5 esittelemme kyselytutkimuksen tulokset. Jakso 6 päättää artikkelin esittämällä tutkimuksen pohjalta tehdyt johtopäätökset.

1. Digitalisaatio ja tietoturva

Digitalisaation myötä suuri osa ihmiskunnan tiedosta on muutettu biteiksi ja uusien viestintäteknologioiden avulla nämä bitit ovat kaikkien saatavilla, muunneltavissa ja kopioitavissa. Sähköinen tiedonkäsittely ja erilaiset tietojärjestelmät ovat alentaneet tiedonhankintaan liittyviä kustannuksia tarjoamalla kustannustehokkaan tavan analysoida ja kerätä tietoa (Gurbaxani ja Whang 1991). Näiden järjestelmien arvo syntyy kuitenkin niiden kyvystä muodostaa kybertoimintaympäristöiksi kutsuttuja verkostoja ja jakaa eri paikoista kerättyä tietoa järjestelmien välillä (Govinazzo 2003, 101). Internet mullisti tiedonvälityksen tekemällä erilaisista kybertoimintaympäristöistä yhteensopivia (Robinson 1999). Syntyi jatkuvasti kasvava, hajautettu, keskinäisriippuvainen verkostojen verkosto eli globaali kybertoimintaympäristö (*cyberspace*).

Internetin suosio kasvoi räjähdysmäisesti 1990-luvulla. Etenkin kehittyneissä maissa huomio alkoi kiinnittyä siihen, että lähes kaikki yhteiskunnan sektorit olivat tulleet riippuvaisiksi sähköisestä tiedonkäsittelystä, viestintäverkoista sekä näitä tukevasta infrastruktuurista (PCCIP 1997; de Leeuw ja Bergstra 2007,19; Sisäministeriö 2017). Internet-protokolla (TCP-IP) oli alun perin kehitetty suljettua keskusteluympäristöä varten. Jo 1980-luvulla, kun Internet avattiin suurelle yleisölle, sen riittämätön turvallisuus aiheutti huolta. Uudet viestintäteknologiat tarjosivat kuitenkin huomattavia säästöjä. Kun verkot kytkettiin Internettiin, ei enää tarvittu kalliita yksityisiä verkkoja (Anderson ja Fuloria 2009; CPNI 2011). Ensimmäisinä toimintaympäristön muutokseen havahduttiin Yhdysvalloissa, jossa tunnistettiin perinteisen fyysisen tason uhkien rinnalle nousseet kyberuhat kriittisen infrastruktuurin suojelussa (PCCIP 1997).

Laitteiden ja järjestelmien yhdistäminen Internettiin ei tehnyt niistä haavoittuvaisia, Internet vain paljasti olemassa olevat haavoit-

tuvaisuudet hyökkäyksille. Anderson (2001) havainnollistaa, miksei ICT-hyödykkeiden turvallisuus ole aina yhteiskunnan kannalta optimaalisella tasolla. Hän kuvaa ICT-markkinoita "voittajien markkinoiksi", joissa muutama johtava yritys hallitsee markkinoita. Tähän on kolme syytä. Ensinnäkin suurin osa ICT-hyödykkeistä on verkostohyödykkeitä, eli kuluttajien tuotteista saama hyöty riippuu muiden käyttäjien lukumäärästä. Toiseksi ICT-hyödykkeiden tuotekehityskustannuksen ovat korkeat, mutta niiden valmistaminen halpaa. Kolmanneksi useimmiten vaihtoehtoiseen teknologiaan siirtymiseen liittyy vaihtokustannuksia. Yrityksillä on siis kova kiire markkinoille, jotta ne ehtivät saamaan takaisin tuotekehitykseen investoimansa varat (Anderson 2001). Toisilla aloilla lukitseminen on fyysistä, esimerkiksi kriittisen infrastruktuurin puolella laitteistojen hinnat liikkuvat useissa miljardeissa ja niitä uusitaan hyvin harvoin (Anderson ja Fuloria 2009). Myös näiden laitteistojen päivittäminen on haastavaa, koska palveluiden tuotantoa ei usein voida keskeyttää (Anderson ja Fuloria 2009).

Tietoturvalla tarkoitetaan digitaalisen tiedon luottamuksellisuuden, käytettävyyden ja eheyden turvaamista niin, etteivät tiedosta riippuvaiset toiminnot häiriinny. Lähes kaikki yhteiskunnan osa-alueet, koululaisten Wilmaympäristöstä Länsimetron ohjausjärjestelmään, toimivat digitaalisen tiedon varassa. Siksi on tärkeää, ettei kukaan pysty tuhoamaan tai luvatta muuttamaan järjestelmissä olevia tietoja. Kun tietojärjestelmien taloudellinen merkitys 1990-luvulla kasvoi, ensimmäiset kaupalliset tietoturvaratkaisut ilmestyivät markkinoille. Useimmat näistä ratkaisuista pystyvät kuitenkin vain havaitsemaan tunnettuja hyökkäyksiä tai muunnelmia niistä. Nykyisessä nopeasti muuttuvassa globaalissa kyberympäristössä, näiden tietoturvaratkaisujen päivitystiheys ei aina riitä, vaan organisaatioiden pitää aktiivisesti hakea tietoa viimeisimmistä tietoturvauhista ja päivittää puolustuksiaan näillä tiedoilla. Tietoturvaaiheisen tiedon eli uhkatiedon jakaminen on yksi tapa täyttää tämä vaatimus.

Tietoturvaa ja kyberturvallisuutta käytetään usein toistensa synonyymeinä. Suomessa kyber-termien käyttöönotolla on pyritty kuvaamaan muutosta, jossa tietoteknisestä toimintaympäristöstä on tullut globaali ja jossa modernit yhteiskunnat ovat voimakkaasti keskinäisriippuvaisia (Sisäministeriö 2017). Tämän muutoksen myötä järjestelmissä olevat haavoittuvuudet altistuivat ulkopuolisille hyökkäyksille ja perinteisten fyysisten uhkien rinnalle nousi kyberuhkia. Kyberturvallisuus kuvaa koko sähköisen järjestelmän turvallisuutta. Se koostuu järjestelmän fyysisestä koskemattomuudesta, bugittomista ohjelmistoista ja hyvästä tietoturvasta. Tavoitetilassa tästä kyberympäristöstä ei aiheudu varaa tai häiriötä digitaalisen tiedon käsittelystä riippuvaiselle toiminnolle (Valtioneuvosto 2013).

2. Tietoturvainvestoinnit

Internetissä olevien palveluiden taloudellisen merkityksen kasvaessa ne alkavat houkutella myös rikollisia. Maailmassa on lähes neljä miljardia Internetin käyttäjää (Internetstatistics 2018) ja yli kaksinkertainen määrä laiteita on kytkettynä kybertoimintaympäristöön (Gartner 2017a). Joidenkin arvioiden mukaan kyberrikollisuuden kustannukset maailmanlaajuisesti tuplaantuvat vuodesta 2015 ja nousevat 6 000 miljardiin dollariin vuoteen 2021 mennessä (Morgan 2018). Samaan aikaan ennustetaan,

että maailmanlaajuisesti tietoturvainvestoinnit nousevat 93 miljardiin vuoden 2018 loppuun mennessä (Gartner 2017b). Suomessa investoidaan muita EU-maita enemmän (noin 0,14 %) tietoturvaan suhteessa bruttokansantuotteeseen (CGI 2015). Tämä on ymmärrettävää, kun otetaan huomioon, että Suomi on myös digitalisaatiossa monia muita maita edellä. Luvut kuulostavat vakuuttavilta, mutta tietoturvainvestointien ja hyökkäysten kustannusten arvioiminen ei kuitenkaan ole yksiselitteistä: tietoturvainvestointeja ja hyökkäysten kustannuksia ei juurikaan raportoida. Otsikoissa pyörivät arviot ovat usein tarkoituksenhakuista spekulaatiota. Kuinka paljon organisaatioiden kannattaa oikeasti investoida tietoturvaan?

Suurin osa malleista, jotka pyrkivät ennustamaan optimaalista tietoturvainvestointia pohjautuvat Gordonin ja Loebin kehittämään uraauurtavaan malliin yrityksen optimaalisesta tietoturvainvestoinnista (Gordon ja Loeb 2002). Mallissa yritys arvioi kannattaako tietyn tietopaketin turvallisuuteen investoida lisää vertailemalla investoinnin hyötyjä sen kustannuksiin (Gordon ja Loeb 2002). Mallissa oletetaan, että päätöksentekijällä on käytettävissään kaikki tarpeellinen tieto tietojärjestelmien haavoittuvaisuuksista, tietoturvauhista sekä hyökkäyksen vaikutuksista (Gordon ja Loeb 2002). Mallissa on kaksi puutetta. Ensinnäkin reaalimaailmassa päätöksentekijöillä ei ole mallin edellyttämää näkyvyyttä vallitsevasta tilanteesta (Bisogni 2011). Toiseksi malli ei huomioi tietoturvainvestoinnin vaikutusta muihin toimijoihin. Kun yritys investoi tietoverkkojensa turvallisuuteen, se samalla pienentää niiden turvattomuuden aiheuttamaa negatiivista ulkovaikutusta muille toimijoille (Heal ja Kunreuther 2003). Myöhempi versio Gordonin ja Loebin mallista ottaa ulkoisvaikutukset huomioon, mutta nyt päätöksentekijällä on kaikki oleellinen tieto ulkoisvaikutuksista käytettävissään (Gordon ym. 2015).

Valtaosa tietoturvainvestoinmalleista tarkastelee investointipäätöstä yksittäisen voittoa tavoittelevan yrityksen näkökulmasta (Böhme 2010). Tämän kirjallisuuden rinnalle on kuitenkin syntynyt toinen kirjallisuuden haara, jossa tietoturva määritellään julkiseksi hyödykkeeksi ja tietoturvainvestointien positiiviset ulkoisvaikutukset mahdollistavat vapaamatkustamisen (Honeyman ym. 2007; Grossklags ym. 2008; Johnson ym. 2010; Naghizadeh ja Liu 2016). Useimmat näistä malleista perustuvat Varianin (2004) malliin, jossa järjestelmän turvallisuus riippuu järjestelmää käyttävien toimijoiden yhteisestä tietoturvatasosta. Yhteinen tietoturvataso määräytyy Hirscleiferin (1987) mallin mukaisesti joko yksittäisten toimijoiden panosten summana (*total effort*), heikoimman suorituksen (*weakest link*) tai suurimman panostuksen (*best shot*) perusteella. Julkinen hyödyke -malli kuvaa erinomaisesti tietoturvaa luotetun kybertoimintaympäristön sisällä, esimerkiksi yritysverkon sisällä. Myös kansallinen kyberpuolustus ja poliisin kybertoiminta voidaan käsittää julkisina hyödykkeinä. Camp ja Wolfram (2004) kuitenkin argumentoivat, että yksityisten organisaatioiden tekemät erilliset tietoturvainvestoinnit eivät muodosta yhtä jakamatonta hyödykettä, siksi tietoturva ei ole julkinen hyödyke, vaikka tietoturvainvestoinnit synnyttävätkin ulkoisvaikutuksen. Suurin osa tietoturvan taloustieteen kirjallisuudesta on tietotekniikan, tekniikan ja oikeustieteen alan asiantuntijoiden kirjoittamaa (Choi ym. 2010). Tämä selittänee ajoittaiset epätarkkuudet taloustieteen termistön käytössä mainitussa kirjallisuudessa.

Hollantilaiset taloustieteilijät Kox ja Straathof (2013) esittävät, että suurimmat syyt organisaatioiden tietoturvan ali-investointeihin ovat informaation epäsymmetrisyys ja ulkoisvaikutukset. Tietoturvainvestointi on yksityinen päätös, jossa ei välttämättä huomioida päätöksen vaikutuksia muihin toimijoihin (Kox ja Straathof 2013). Jos ulkoisvaikutuksen olemassaolo tiedetään (*tietoisuus*), sen aiheuttaja tunnetaan (*attribuutio*) ja vaikutus on politiikkatoimin hinnoiteltu, niin markkinoiden toimiessa aiheuttaja sisäistää ulkoisvaikutuksen. Yleensä kybertoimintaympäristössä asianlaita ei kuitenkaan ole näin. Se osapuoli, johon haitta kohdistuu, ei välttämättä itse havaitse haittaa. Myöskään haitan aiheuttaja ei välttämättä ole ongelmasta tietoinen, ja vaikka olisikin, niin ongelman korjaamisesta ei välttämättä ole hänelle mitään hyötyä. Jotta toimijat voisivat tehdä valveutuneita tietoturvapäätöksiä, heidän pitäisi pystyä hankkimaan tietoturva-aiheista tietoa kustannustehokkaasti (Rowe ja Gallaher 2006).

Rowe ja Gallaher (2006) puolestaan väittävät, että uhkatieto on julkinen hyödyke ja siksi sitä tuotetaan liian vähän. Gordon, Loeb ja Lucyshyn (2003) ovat samoilla linjoilla. Heidän kahden yrityksen mallissaan uhkatiedon jako johtaa vapaamatkustamiseen ja tietoturvainvestointien pienentymiseen. Jos toinen yritys jakaa uhkatietoa, niin toisen yrityksen ei enää tarvitse itse investoida saman asian selvittämiseksi. Uhkatiedon jaosta syntyvä *spillover*-vaikutus voidaan myös nähdä hyvänä asiana. Gal-Orin ja Ghosen (2006) mallissa uhkatiedon jako parantaa tietoturvainvestointien kustannustehokkuutta. Molemmat organisaatiot hyötyvät toistensa tietoturvaosaamisesta ja heillä on pienemmillä kustannuksilla suhteellisesti enemmän tietoa käytettävissään. Malli huomioi myös sen, että uhkatiedon jaosta voi aiheutua vuotokustannuksia, jos jaettu uhkatieto joutuu ulkopuolisten käsiin. On myös esitetty, että toimijoiden välinen keskinäisriippuvuus vaikuttaisi heidän halukkuuteensa jakaa uhkatietoa ja/tai siitä saatavaan hyötyyn (Hausken 2007; Laube ja Böhme 2015).

Teoreettisten tietoturvainvestointimallien käytännön merkitys on kuitenkin rajallinen (van der Meulen 2015). Ensinnäkin mallien hyödyntämiseen tarvittavia tietoja, kuten tehdyn tietoturvainvestoinnin suuruutta, voi olla yllättävän hankala kerätä. Tietoturvainvestointeja käsittelevää raporttiaan varten van der Meulen (2015) haastatteli 27 kriittisen infrastruktuurin toimijaa Alankomaista. Yhtenä tutkimuksen tavoitteista oli arvioida toimijoiden tekemien tietoturvainvestointien suuruutta. Tämän osoittautui kuitenkin hankalaksi. Raportissaan hän listasi syitä, miksi tietoturvainvestointien arvioiminen on jopa oman organisaation kohdalla hyvin vaikeaa. Ensinnäkin tietoturvakustannuksia ei välttämättä kirjata nimenomaan tietoturvakustannuksiksi. Tämä johtuu etupäässä siitä, että tietoturva on kiinteä osa organisaation eri toimintoja, prosesseja ja tuotteita eikä tietoturvakulujen erottaminen ole mahdollista. Toiseksi tietoturvaa ei voida tarkastella vain investointien näkökulmasta, sillä pelkkä rahallisen investoinnin suuruus ei kerro kaikkea organisaation tietoturvallisuudesta. Tietoturva onkin pikemminkin laadullista kuin kvantitatiivista.

Tietoturvan taloustieteessä tietoturva kuvataan usein kissa ja hiiri -pelinä (Laszka ym. 2014) tai jopa taisteluna (Grossklags ym. 2008) puolustajien ja hyökkääjän välillä. Puolustaja ja hyökkääjä kohtaavat yhden tai useamman kerran ottelussa, jonka lopputulema määräytyy sen perusteella, minkälaiset kannustimet pe-

laajilla on puolustautua ja hyökätä (Moore ja Anderson 2012). Puolustaja-hyökkääjä -malli kuvaa erinomaisesti tietoturvatyöskentelyä tietoturvatiimin näkökulmasta. Useat organisaatiot kuitenkin ulkoistavat tietoturvatoimintojaan eli siirtävät tietoturvatoimintoja ulkopuoliselle palvelun tarjoajalle, joka hoitaa toimintoja korvausta vastaan sovitun määräajan t(Rowe 2007). Tällöin organisaatio ei ole enää aktiivinen puolustaja vaan tietoturvalaitteiden ja -palveluiden ostaja, jolla ei välttämättä ole riittävää osaamista tietoturvatason todentamiseen. Anderson (2001) kuvailee tietoturvamarkkinoita "sitruunoiden markkinoiksi", mutta siinä missä Akerlofin (1970) mallissa kuluttajat vielä arvostivat autojen laatua, halpojen IoT-laitteiden maailmassa tietoturvallisuus ei välttämättä vaikuta lainkaan ostopäätökseen.

3. Avoin tietoturvayhteistyö ja uhkatiedon jako

Puolustajan näkökulmasta tiedustelutieto on tietoa, jonka avulla hyökkäyksiä voidaan estää nopeammin ja tehokkaammin (CPNI 2015). Uhkatieto on organisaatioiden eri lähteistä keräämää tiedustelutietoa niiden kohtaamista tietoturvauhista. Tämän tiedon avulla ne pystyvät havaitsemaan uhkia sekä vastaamaan niihin paremmin. Sekä van der Meulen (2015) että Mooren ym. (2016) tekemissä kyselytutkimuksissa haastateltavat suhtautuivat lähes poikkeuksetta positiivisesti uhkatiedon vaihtoon. Saatujen 40 vastauksen pohjalta Moore ym. havaitsivat, että korkeamman tason tiedon vaihdon lisäksi osallistujat hyötyivät toisten jakamista kokemuksista eri tietoturvatyökaluista ja -palveluista. Van der Meulenin haastateltavat puolestaan kertoivat arvostavansa yhteistyöportaaleja, joiden avulla oli helpompi saada laajempi kuva tietoturvahaasteista oman organisaation ulkopuolella.

Tarve tietoturvayhteistyölle ja uhkatiedon vaihdolle kumpuaa alati muuttuvasta uhkaympäristöstä. Internet on hajautettu, autonominen ja hallitsematon (Koivunen 2010). Tietoturvahyökkäyksiä ei voida aukottomasti ennustaa eikä ole olemassa ratkaisuja, joilla hyökkäykset voitaisiin täysin estää. Tarvitaan siis ajantasaista uhkatietoa eli tietoa tietoturvauhista, jolla olemassa olevia puolustuksia voidaan päivittää. Useat tietoturva-asiantuntijat suosittelevat uhkatiedon jakoa kustannustehokkaana tapana parantaa organisaation tietoturvallisuutta. Nopean teknologisen muutoksen, monimutkaisten järjestelmien ja jatkuvasti muuttuvan uhkaympäristön myötä kattavan tilannekuvan ylläpitäminen tietoturvauhista on yhä haastavampaa. Jakamalla uhkatietoa organisaatiot voisivat hyötyä toistensa tietoturvaosaamisesta.

Tuotekehityspuolella useat yritykset jo myöntävät yhteistyön ja tiedon jakamisen tarpeen. Harvalla yrityksellä on resursseja hankkia yksinään kaikki uusien innovaatioiden synnyttämiseen tarvittava osaaminen (Michelino ym. 2015). Avoimen innovaation kautta yritykset pystyisivät myös jakamaan jatkuvasti kasvavia tietoturvakustannuksia. Chesbrough ja Appleyard (2007) määrittelevät, että avoin innovaatio on organisaatioiden välillä tapahtuvaa tarkoituksellista tiedonvaihtoa. Organisaatiossa hyödynnetään muiden ideoita omassa tuotekehityksessä ja jaetaan muille organisaation sisällä kehitettyä tietoa, jota nämä voivat hyödyntää omissa tuotekehitysprosesseissaan. Samalla tavoin avoimessa tietoturvayhteistyössä organisaatiot hyödyntävät yhteistyökumppa-

neiltaan saamaansa uhkatietoa oman tietoturvansa parantamiseksi ja jakavat yhteistyökumppaneilleen omia tietoturvahavaintojaan, joita nämä puolestaan pystyvät hyödyntämään tietoturvansa parantamisessa.

4. Kannustimet ja esteet tietoturvayhteistyölle

Avointa innovaatiota sekä yleisesti innovaatioiden omaksumista on tutkittu kartoittamalla omaksumisen esteitä ja kannustimia haastatteluiden ja kyselytutkimusten avulla (Chesbrough ja Crowther 2006; Laukkanen ym. 2008; Al Awadhi ja Morris 2008). Yksi käytetyimmistä innovaatioiden hyväksymismalleista on UTAUT-malli (*Unified Theory of Acceptance and Use of Technology*), joka koostuu kahdeksasta aikaisemmasta teknologian hyväksymismallista (Venkatesh ym. 2003). Innovaatioiden vastustamista tutkivat kyselytutkimukset pohjautuvat puolestaan usein Ramin ja Sethin (1989) kehittämään innovaatioiden vastustusmalliin. Kyselytutkimuksia on myös hyödynnetty tietoturvayhteistyön tutkimuksessa. Vaikka ENISA (2010) ja Koepke (2017) keräsivät molemmat alle 25 vastausta, ne tarjoavat silti erinomaista näkyvyyttä uhkatiedonjaon esteisiin ja kannustimiin. Omassa kyselytutkimuksessamme halusimme hyödyntää innovaatioiden hyväksymis- ja vastustusmalleja uhkatiedon jaon esteiden ja kannustimien kartoittamiseen.

UTAUT-mallin seitsemästä tekijästä keskitymme neljään tekijään, jotka vaikuttavat käyttöaikomuksiin. Nämä tekijät ovat käyttö- ja vaivannäköodotukset, sosiaaliset vaikutukset ja helpottavat olosuhteet (Venkatesh ym. 2003). Käyttöönotto-odotukset liittyvät siihen, kuinka käyttäjä uskoo hyötyvänsä uudesta innovaatiosta tai järjestelmästä (Venkatesh ym. 2003). Toimijoiden osallistumishalukkuutta uhkatiedon jakamiseen on aiemmin selitetty mahdollisuuksilla hyödyntää muiden osaamista oman tietoturvan parantamiseen sekä auttaa muita omalla osaamisellaan (Gal-Or ja Ghosh 2005). Käyttöodotukset voivat myös liittyä koko verkoston tietoturvallisuuteen. Auttamalla muita, organisaatio voi vähentää paitsi muille myös itselleen tietoturvaongelmista aiheutuvia kustannuksia. Useissa tietoturvainvestointimalleissa organisaatioiden välinen keskinäinen riippuvuus on myös keskeinen syy tehdä tietoturvayhteistyötä ja jakaa uhkatietoa (Hausken 2007, Laube ja Böhme 2015).

Vaivannäköodotukset liittyvät siihen, kuinka vaikeaa tai helppoa käyttäjä kuvittelee innovaation hyödyntämisen olevan (Venkatesh ym. 2003). Uhkatiedon hyödyntämistä voi estää ajatus ajan tuhlaamisesta vanhentunutta ja päällekkäistä tietoa läpikäydessä. Koepken (2017) haastattelemien tietoturva-asiantuntijoiden mukaan uhkatiedon jako kannattaa vain, jos jaettava tieto on hyödyllistä ja tärkeää. Innovaation hyödyntämistä voidaan helpottaa olosuhteilla, kuten automatisoiduilla työkaluilla ja paremmalla koordinoinnilla (Venkatesh ym. 2003). Sosiaaliset odotukset puolestaan liittyvät siihen, miten käyttäjä kuvittelee muiden näkevän hänet, mikäli hän hyödyntää tai ei hyödynnä innovaatiota (Venkatesh ym. 2003). Esimerkiksi organisaatiot voivat kokea tietoturvayhteistyön vaikuttavan toimialansa ja organisaationsa maineeseen muiden toimijoiden ja asiakkaiden silmissä.

Ram ja Seth (1989) tutkivat miksi innovaatioita vastustetaan. He jakavat esteet kahteen eri ryhmään, toiminnallisiin ja psykologisiin esteisiin. Toiminnalliset esteet liittyvät innovaatioiden käyttöön, arvoon ja riskeihin. Ylei-

sin syy innovaation käytön vastustamiseen on sen yhteensopimattomuus aikaisempien toimintatapojen kanssa (Ram ja Seth 1989). Mikäli avoin tietoturvayhteistyö vaatii suuria muutoksia rutiineissa, sen omaksuminen voi kestää kauankin. Toinen toiminnallinen este liittyy innovaation arvoon ja hinta-hyöty-suhteeseen (Ram ja Seth 1989). Jos tietoturvayhteistyön ja uhkatiedon vaihdon kustannustehokkuus ei ole hyvä verrattuna muihin vastaaviin toimintatapoihin, ei niiden käyttöönotolle ole perusteita.

Kolmas toiminnallinen este käsittää riskit (Ram ja Seth 1989). Kaikkiin uusiin innovaatioihin liittyy riskejä ja epävarmuutta. Tutkimuksessamme tarkastelimme kolmea erilaista riskiä: luottamuspulaa, vuotokustannuksia ja hukattua aikaa. Koepken (2017) tutkimuksessa luottamuspula nousi tärkeimmäksi esteeksi uhkatiedon jaolle. ENISA:n (2010) tutkimuksessa luottamus oli vain jokseenkin tärkeä kannustin uhkatiedon jaolle. Toimijoiden haluttomuutta jakaa uhkatietoa perustellaan usein vuotokustannuksilla eli sillä, että tiedot päätyvät vääriin käsiin tai että salassa pidettäviä tietoja, kuten asiakastietoja, leviää uhkatiedon mukana (Bisogni 2011; Gal-Or ja Ghosh 2005). Sekä Koepke (2017) että ENISA (2010) tutkivat, toimiiko pelko maineen menetyksestä esteenä uhkatiedon jaolle. ENISA:n (2010) tutkimuksessa maineeseen liittyvät riskit olivatkin toiseksi merkittävin este jaettavan uhkatiedon hyödyttömyyden jälkeen. Muita merkittäviä esteitä Koepken (2017) tutkimuksessa olivat vastavuoroisuuden ja hyvien yhteistyökumppaneiden puute.

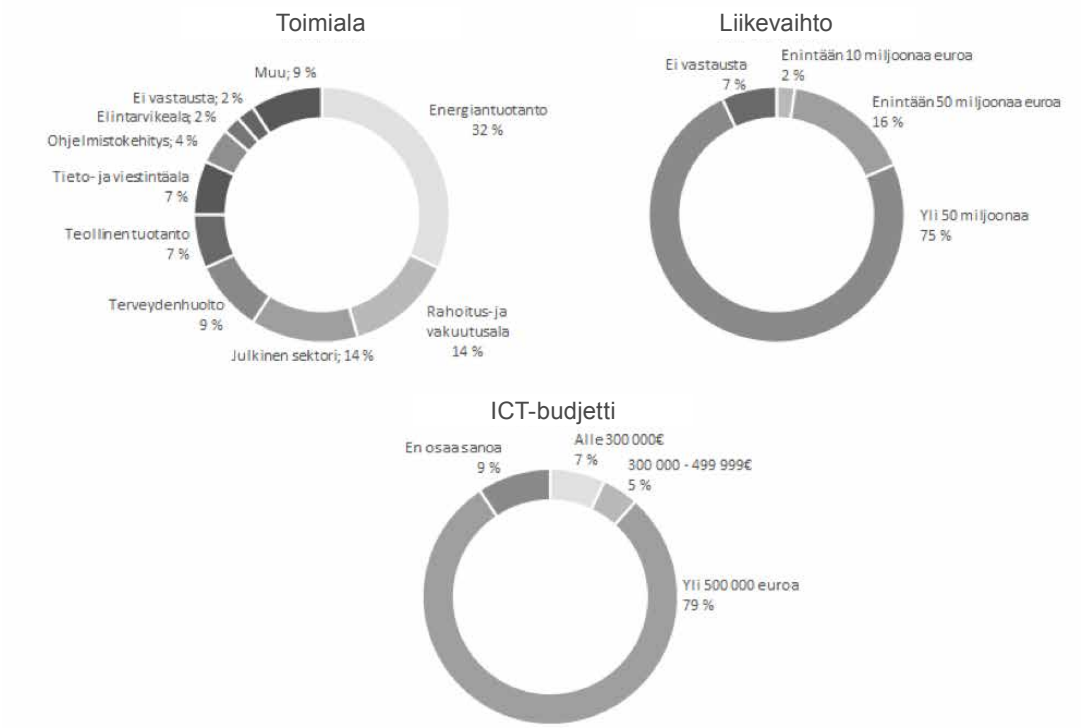
Psykologiset esteet syntyvät, jos uudet innovaatiot ovat ristiriidassa aikaisempien uskomusten kanssa (Ram ja Seth 1989). Mitä enemmän avoin tietoturvayhteistyö poikkeaa aikaisemmista toimintatavoista ja perinteistä, sitä hankalampi sitä on omaksua. Myös epäsuotuisa mielikuva uudenlaisesta työtavasta saattaa estää sen omaksumisen, vaikka hyödyt olisivatkin muuten tiedossa.

5. Tulokset

Kyselyyn vastasi 43 tietoturva-asiantuntijaa, jotka olivat saaneet kutsun tutkimukseen, joko Viestintäviraston Kyberturvallisuuskeskuksen toimialakohtaisten sähköpostilistojen kautta tai henkilökohtaisena kutsuna. Kyberturvallisuuskeskuksen sähköpostilistojen kautta kysely tavoitti noin 500 asiantuntijaa. Kyselyyn vastanneista kolme neljäsosaa edusti suuria organisaatioita, joiden liikevaihto on yli 50 miljoonaa euroa vuodessa (kuvio 1). Lähes kolmannes vastaajista työskenteli energiantuotannon parissa. Myös rahoitus- ja vakuutusala sekä julkinen sektori olivat hyvin edustettuina kyselyssä. Tutkimuksen aineisto ei siis ole yleistettävissä, mutta tuloksia voidaan silti pitää suuntaa antavina. Samalla ne tarjoavat näkyvyyttä aihepiiriin, josta on verrattain vähän aineistoa saatavilla. Tutkimus herättää myös useita kysymyksiä siitä, miten tietoturva-aihetta tulisi lähestyä pienten ja keskisuurten yritysten ja organisaatioiden näkökulmasta.

Organisaatioiden koosta johtuen myös ICT-budjetit olivat suuria. Kolme neljäsosaa vastaajista edusti suuria organisaatioita, joiden vuotuinen ICT-budjetti on yli 500 000 euroa ja tietoturvabudjetti keskimäärin 100 000 euroa vuodessa. Kyselyn perusteella keskimääräinen suuri organisaatio investoi tietoturvaan korkeintaan kaksi promillea liikevaihdostaan ja 20 prosenttia ICT-budjeteistaan.

Kuvio 1. Vastaajien toimiala, liikevaihto ja ICT-budjetti



Tietoturvayhteistyö

Tässä tutkimuksessa tietoturvayhteistyö määritellään laaja-alaisesti muiden organisaatioiden auttamiseksi tietoturva-asioissa. Yhteistyö voi olla esimerkiksi omien kokemusten kertomista kollegoille sekä hyvien toimintatapojen ja uhkiin liittyvien tunnistetietojen jakamista. Tällöin organisaatio tekee tietoturvayhteistyötä, jos sen edustajat keskustelevat tietoturva-asioista muiden toimijoiden kanssa. Tämän määritelmän mukaan 36 vastaajaa eli 84 % kaikista vastaajista ilmoitti edustamansa organisaation osallistuvan jonkinlaiseen tietoturvayhteistyöhön (kuvio 2). Tutkimme myös tietoturvayhteistyöhön liittyviä tietovirtoja. Jaottelemme vastaajat heidän edustamiensa organisaatioiden tekemän tietoturvayhteistyön mukaan kolmeen ryhmään. Vastaajista 56 % kertoi organisaationsa jakavan ja vastaanottavan uhkatietoa, 28 % vain vastaanotti uhkatietoa ja 16 % ei osallistunut lainkaan uhkatiedon vaihtoon (kuvio 2).

Merkittävimpiä yhteistyökumppaneita olivat alihankkijat ja muut kumppanit, viranomaiset, kaupalliset toimijat sekä oman toimialan edustajat. Yli 90 % tietoturvayhteistyöhön osallistuvista vastaajista kertoi alihankkijoiden

Kuvio 2. Tietoturvayhteistyö ja uhkatiedon jakaminen

ja muiden kumppanien olevan heille merkittäviä yhteistyökumppaneita. Vastauksissa korostuu useiden vastaajien viranomaisyhteistyö: 91 % tietoturvayhteistyötä tekevistä vastaajista piti Kyberturvallisuuskeskusta merkittävänä ja peräti 72 % erittäin merkittävänä tietoturvayhteistyökumppanina. Kolme neljäsosaa yhteistyötä tekevistä vastaajista piti myös muita viranomaisia merkittävinä yhteistyökumppaneina. Lähes 90 % yhteistyötä tekevistä organisaatioista koki myös kaupalliset toimijat merkittäviksi tietoturvayhteistyökumppaneiksi.

Avoimen innovaation kirjallisuudessa yhteistyötä on perinteisesti arvioitu tarkastele-

malla sekä yhteistyö-kumppanuuksien laajuutta (*breadth*) että niiden syvyyttä (*depth*) (Laursen ja Salter 2006). Tässä tutkimuksessa laajuutta arvioidaan kumppanuuksien määrällä ja syvyyttä luotettujen yhteistyökumppanien määrällä. Kuvio 2 kertoo, että niistä 36 vastaajasta, jotka ilmoittivat edustamansa organisaation tekevän tietoturvayhteistyötä, puolet teki yhteistyötä alle 10 toimijan kanssa. Luotettuja yhteistyökumppaneita heillä oli alle puolet tästä eli korkeintaan neljä. Yllättäen osa yhteistyökumppanuuksista oli hyvinkin laajoja: 11 % vastaajista ilmoitti yhteistyökumppaneiden määräksi yli 30 toimijaa ja jopa 8 % vastaajista kertoi saman luvun luotettujen tietoturvayhteistyökumppaneiden määräksi. Kaikki tietoturvayhteistyöhön osallistuneet organisaatiot harjoittivat myös vapaaehtoista tietoturvayhteistyötä. Vapaaehtoisuudesta ja vastaajien edustamien organisaatioiden aktiivisuudesta kertoo se, että enemmistö vastaajista kertoi edustamansa organisaation olleen ainakin yksi tietoturvayhteistyön alulle panijoista.

Suurimpia esteitä tietoturvayhteistyölle ovat luottamuspula ja huono kustannus-tehokkuus (taulukko 1). Lähes kaikki vastaajat olivat sitä mieltä, että tietoturvayhteistyö ei onnistu ilman hyvää keskinäistä luottamusta. Heistä 77 % piti tietoturvayhteistyötä kustannustehokkaana tapana parantaa tietoturvaa. Esimerkin puute omalta toimialalta ja haaste löytää kumppaneita toimivat esteenä tietoturvayhteistyölle. Myös toimialaerot näkyivät vastauksissa. Tietoturvayhteistyöhön osallistuvia organisaatioita edustavista vastaajista 70 % oli sitä mieltä, että tietoturvayhteistyö on heidän toimialallaan yleistä. Tietoturvayhteistyöhön osallistumattomien organisaatioiden edustajista kukaan ei ollut tämän väitteen kanssa samaa mieltä. Vastaajista vain 23 % koki, että tietoturvaongelmat tulisi ratkaista sisäisesti. Tulos on hieman yllättävä, mutta johtunee ainakin osittain siitä, että vastaajiksi valikoitui etupäässä sellaisten yritysten edustajia, jotka osallistuvat aktiivisesti tietoturvayhteistyöhön.

Suurin kannustin yhteistyölle oli molemminpuolinen hyöty. Yli 80 % vastaajista oli sitä mieltä, että tietoturvayhteistyö parantaa koko toimialan mainetta tietoturva-asioissa. He myös kokivat hyötyvänsä muiden osaamisesta ja auttavansa muita (Taulukko 1). Myös hyvä koordinointi sekä halu kasvattaa oman organisaation mainetta tietoturva-asioissa kannustivat tietoturvayhteistyöhön. Hieman yllättäen vain 21 % vastaajista piti toimijoiden riippuvuutta toistensa tietoturvallisuudesta tarkoituksenmukaisen tietoturvayhteistyön edellytyksenä.

Uhkatiedon vaihto

Tutkimuksessamme määrittelemme uhkatiedoksi kaiken tiedon, jonka avulla voidaan havaita ja estää tietoturvahyökkäyksiä. Tällöin organisaatio jakaa uhkatietoa, jos sen edustajat jakavat yhteistyöorganisaatioille tietoa, jota nämä voivat käyttää tietoturvansa parantamiseen. Vastaavasti organisaatio vastaanottaa uhkatietoa, jos sen yhteistyökumppanit jakavat sille tietoa, jota se voi käyttää tietoturvansa parantamiseen. Vastaajista 24, eli 56 % kaikista vastaajista, kertoi edustamansa organisaation jakavan uhkatietoa ja 36 vastaajaa, eli 84 % kaikista vastaajista, kertoi organisaationsa vastaanottavan uhkatietoa. Tästä lähtien kutsumme uhkatietoa jakavia organisaatiota *jakajiksi* ja uhkatietoa vastaanottavia organisaatioita *vastaanottajiksi*. Niitä organisaatioita, jotka jättäytyvät uhkatiedon jaon ulkopuolelle, kutsumme *ei-osallistujiksi*.

Taulukko 1. Tietoturvayhteistyön kannustimet ja esteet

Tietoturvayhteistyö	Esteet *Osuus kaikista vastaajista*	Kannustimet *Osuus kaikista vastaajista*
Yleinen	1. Luottamuspula, 95 %	1. Hyöty muiden osaamisesta, 83 %
	2. Huono kustannustehokkuus, 77 %	2. Muiden auttaminen, 82 %
		3. Hyvä koordinointi, 79 %
Melko yleinen	3. Toimialan maine, 85 %	4. Oma maine, 65 %
	4. Muiden esimerkki, 53 %	
	5. Haaste löytää kumppaneita, 54 %	
Harvinainen	6. Sisäinen asia, 23 %	5. Keskinäinen riippuvaisuus, 21 %

Taulukko 2. Uhkatietotyypit

Uhkatietotyyppi	Kuvaus
Strateginen uhkatieto	Analysoitua tietoa liiketoimintapäätöksiin liittyvistä tietoturvariskeistä.
Taktinen uhkatieto	Ajantasaista tietoa hyökkääjien toimintavoista, työkaluista ja taktiikoista.
Tekninen uhkatieto	Hyökkäyksiin liittyviä tunnistetietoja kuten IP-osoitteita
Hyökkäysvaroitukset	Varoitus toiselle yritykselle heidän verkossaan käynnissä olevasta hyökkäyksestä
Kokemukset	Onnistumiset, epäonnistumiset, hyvät toimintatavat ja muu tukimateriaali

Tutkimuksessamme erottelemme viisi eri uhkatietotyyppiä (taulukko 2). Kyselyyn vastanneista jakajista yli 80 % jakoi kokemuksia ja taktista uhkatietoa luotetuille kumppaneille ja viranomaisille. Kokemuksia jaetaan eniten: 60 % jakajista kertoi jakavansa kokemuksia ja 40 % taktista uhkatietoa joko toistuvasti tai melko usein. Noin kaksi kolmasosaa kertoi myös jakavansa varoituksia viranomaisten kautta, strategista uhkatietoa luotetuille kumppaneille ja teknistä uhkatietoa viranomaisille ja luotetuille kumppaneille. Lähes kaikki vastaanottajat saivat yhteistyökumppaneiltaan taktista uhkatietoa eli tietoa hyökkääjien toimintatavoista, työkaluista ja taktiikoista. Melkein yhtä moni ilmoitti vastaanottavansa myös strategista uhkatietoa, hyökkäysvaroituksia ja kokemuksia. Teknistä uhkatietoa sai kaksi kolmasosaa vastaanottajista. Lähes kaikki vastaanottajat olivat sitä mieltä, että kaikki vastaan-

Taulukko 3. Esteet ja kannustimet uhkatiedon jaolle (kaikki vastaajat)

Jakaminen	**Esteet** *Osuus kaikista vastaajista*	**Kannustimet** *Osuus kaikista vastaajista*
Yleinen	1. Uhkatiedon hyödyttömyys, 84 %	1. Koordinointi, saavuttaa vastaanottajan, 87 %
		2. Koordinointi, alhaisemmat vuotokustannukset, 83 %
		3. Muiden esimerkki omalla toimialalla, 69 %
Melko yleinen	2. Käsityön tarve, 65 %	4. Kilpailijoiden tietoturvan vaikutus asiakkaisiin, 65 %
	3. Vastavuoroisuuden puute, 51 %	5. Oma maine tietoturva-asioissa, 56 %
	4. Vuotokustannukset (uhkatieto), 49 %	6. Mahdollinen pakollisuus, 44 %
Harvinainen	5. Vuotokustannukset (asiakastieto), 28 %	7. Automatisoitujen työkalujen hyöty, 28 %
	6. Sisäinen asia, 5 %	

otettu uhkatieto on tietotyypistä riippumatta heidän organisaationsa tietoturvan kannalta merkittävää. Tärkein ja samalla myös pääasiallinen uhkatiedon lähde kaikille uhkatietotyypeille oli viranomaiset: lähes kaikki vastaanottajat saivat uhkatietoa viranomaisilta.

Esteet ja kannustimet uhkatiedon jaolle

Suurimmat esteet uhkatiedon jaolle olivat jaettavan tiedon hyödyttömyys ja jakamisen työläys (taulukko 3). Yli 80 % vastaajista kertoi, että uhkatietoa kannattaa jakaa vain, jos se on tärkeää ja ajantasaista. Kaksi kolmasosaa vastaajista oli sitä mieltä, että uhkatiedon jako vaatii liikaa käsityötä. Niistä vastaajista, jotka kuuluivat ei-osallistujiin, kaikki olivat samaa mieltä näiden kahden väitteen kanssa. Yllättäen vain noin puolet vastaajista oli huolissaan vastavuoroisuuden puutteesta tiedon jaossa ja uhkatiedon joutumisesta vääriin käsiin. Vielä harvempi oli huolissaan asiakastietojen vuotamisesta uhkatiedon jaon yhteydessä. Perinteisesti etenkin vuotokustannuksia on pidetty suurimpana esteenä uhkatiedon jaolle.

Taulukko 4. Jakajien esteet ja kannustimet

Jakaminen	Jakajien esteet *Osuus kaikista jakajista*	Jakajien kannustimet *Osuus kaikista jakajista*
Yleinen	1. Luottamuspula, 83 %	1. Verkoston tietoturva, 75 %
	2. Valtuutuksen puute omalta organisaatiolta, 79 %	2. Jaettua uhkatietoa käytetään, 71 %
Melko yleinen	3. Laadukkaan uhkatiedon puute, 62 %	3. Kumppanit eivät muuten olisi havainneet, 42 %
	4. Tärkeän uhkatiedon puute, 54 %	4. Kumppaneille olisi aiheutunut kustannuksia, 33 %
		5. Meille olisi muuten aiheutunut kustannuksia, 33 %
Harvinainen	5. Vastavuoroisuuden puute, 13 %	

Jakajien vastauksissa korostui luottamuksen merkitys sekä uhkatiedon jaon hyödyt tietoturvan parantamisessa (taulukko 4). Tietoturvayhteistyölle ei ole edellytyksiä, ellei kumppaneiden välillä ole luottamusta eikä organisaation edustajalla luottoa johdolta. Jakajista 83 % kertoi voivansa luottaa yhteistyökumppaneihinsa ja 79 % kertoi saavansa luottamusta myös organisaationsa johdolta. Mielenkiintoista on, että kaikille yhteisissä kysymyksissä puolet jakajista, kertoi uhkatiedon jaon perustuvan vastavuoroisuuteen, mutta silti vain 13 % heistä kertoi mitoittavansa jakamansa uhkatiedon määrän ja laadun muiden jakaman tiedon mukaan.

Suurimpina kannustimina uhkatiedon jaolle toimivat yhteistyön koordinointi, muiden esimerkki sekä halu vaikuttaa toimialan tietoturvallisuuteen (taulukko 4). Yli 80 % kaikista vastaajista uskoi, että koordinoidussa yhteistyössä uhkatieto saavuttaa paremmin sitä tarvitsevan vastaanottajan ja että riski vuotaa uhkatietoa ulkopuolisille on tällöin myös pienempi. Oman toimialan organisaatioiden esimerkki ja halu vaikuttavat asiakkaiden mielipiteisiin toimialan tietoturvallisuudesta kannustivat kahta kolmasosaa vastaajista uhkatiedon jakamiseen. Myös halu kasvattaa oman organisaation mainetta tietoturva-asioissa, uhkatiedon jaon pakollisuus sekä automatisoitujen työkalujen saatavuus kannustivat uhkatiedon jakamiseen.

Kartoittaessamme uhkatiedonjaon kannustimia kysyimme jakajilta uhkatiedon jakami-

seen liittyvistä käyttöodotuksista (taulukko 4). Yli 70 % jakajista uskoi, että heidän yhteistyökumppaninsa hyödyntävät heidän jakamaansa uhkatietoa ja että jakamalla uhkatietoa he olivat paranteet koko verkostonsa turvallisuutta. Noin 40 % jakajista kertoi auttaneensa yhteistyökumppaniaan havaitsemaan tietoturvaloukkauksen, jota he eivät muuten olisi havainneet ja kolmannes kertoi auttaneensa kumppaneitaan löytämään tietoturvaongelman, josta olisi aiheutunut kumppanille ja myös heille itselleen kustannuksia tai muuta harmia.

Esteet ja kannustimet uhkatiedon hyödyntämiselle

Suurimpia esteitä uhkatiedon hyödyntämiselle ovat huono kustannustehokkuus ja vastaanotetun uhkatiedon hyödyntämisen työläys (taulukko 5). Uhkatiedon vastaanoton suosiosta vastaajien keskuudessa kertoo se, että lähes 80 % kyselyyn vastanneista piti kustannustehokkaampana hyödyntää yhteistyöverkostossa jaettua uhkatietoa kuin vastaavan tietomäärän hankkimista muualta. Itseasiassa vain 9 % vastaajista kertoi voivansa hankkia vastaavat tiedot muualta. Puolet vastaajista kertoi tiedon läpikäymisen olevan aikaa vievää. Vastaanotetun uhkatiedon arvo selittänee halukuutta osallistua tietoturvayhteistyöhön. Kaikista vastaajista vajaa neljännes koki, että vastaanotetun uhkatiedon joukossa on liikaa vanhentunutta, päällekkäistä tai muuten puutteellista tietoa. Eiosallistujien joukosta kaikki, jotka vastasivat kysymykseen (kolmannes ei-vastaajista), olivat tätä mieltä. He olivat myös sitä mieltä, ettei jaetulle uhkatiedolle ole selkeätä käyttötarkoitusta heidän organisaatiossaan. Kaikista vastaajista vain 14 % oli tätä mieltä.

Suurimpia kannustimia uhkatiedon hyödyntämiselle ovat tarve saada tukea päätöksenteolle sekä parantaa tietoturvauhkien havainnointia (taulukko 5). Lähes 90 % vastaajista on sitä mieltä, että vastaanotetun uhkatiedon avulla he pystyvät priorisoimaan tietoturvatoimenpiteitä sekä perustelemaan niiden tarpeellisuutta. Kolme neljäsosaa vastaajista on sitä mieltä, että jaetun uhkatiedon avulla voidaan havaita tietoturvaloukkauksia aikaisemmassa vaiheessa. Kaksi kolmasosaa uskoo, että jaetun uhkatiedon avulla voi havaita hyökkäyksiä, joita muuten ei olisi havaittu. Myös toimialalla on merkitystä uhkatiedon käyttöönotossa. Jakajista kolme neljäsosaa ilmoittaa, että heidän toimialallaan jaettua uhkatietoa hyödynnetään yleisesti. Kun taas eiosallistujista vain kolmannes on samaa mieltä. Puolet vastaanottajista kertoo hyödyntävänsä vain pienen osan vastaanottamastaan uhkatiedosta. Läpikäymisen vaivasta huolimatta jaetusta uhkatiedosta on hyötyä: Puolet vastaanottajista kertoo estäneensä jaetun uhkatiedon avulla hyökkäyksen, josta olisi aiheutunut heidän edustamalleen organisaatioille kustannuksia tai muuta haittaa.

Ulkoistukset ja sisäinen tiimi

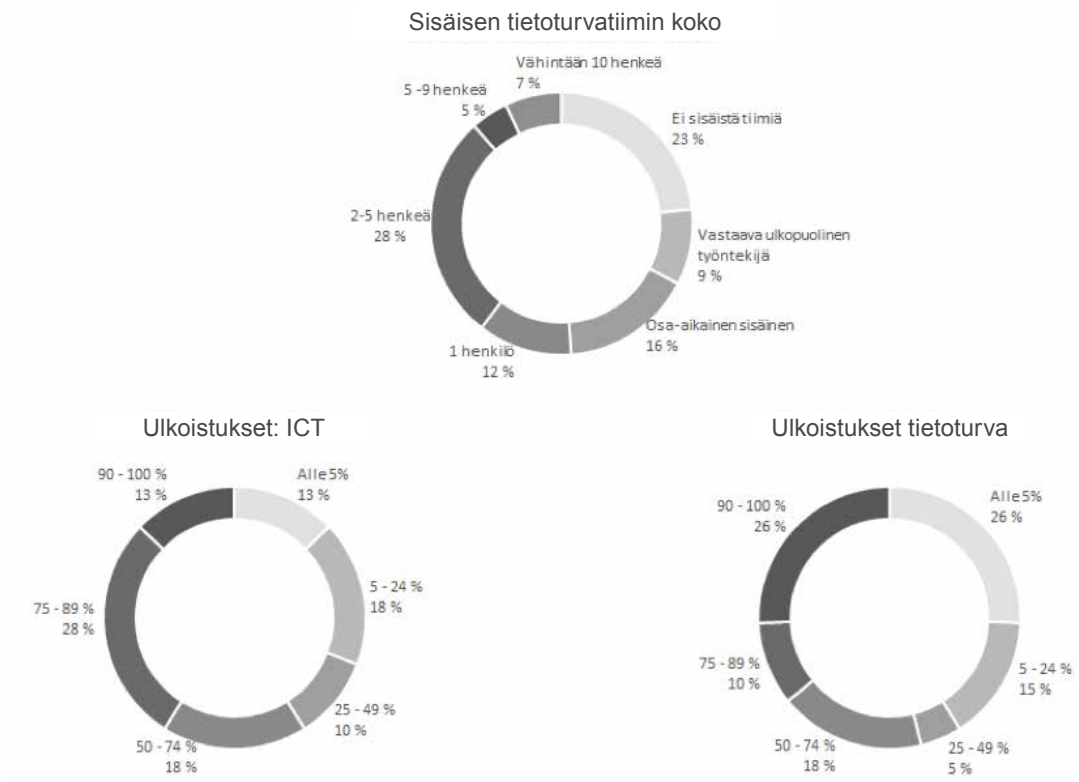
Ulkoistukset muodostavat huomattavan osan useiden vastaajien edustamien organisaatioiden ICT- ja tietoturvabudjeteista (Kuvio 3). Kaksi viidesosaa vastaajista (n=39) kertoi, että ulkoistusten osuus heidän organisaationsa ICT-kuluista ja investoinneista oli vähintään 75 %. Vastaukset ulkoistusten osuuksista tietoturvakuluissa ja -investoinneissa ovat kahtiajakautuneita: Neljänneksessä organisaatioista ulkoistusten osuus tietoturvakuluista ja -investoinneista on yli 90 % ja toisessa neljänneksessä ulkoistukset muodostavat alle 5 % kaikista

Taulukko 5. Esteet ja kannustimet uhkatiedon hyödyntämiselle

Hyödyntäminen	**Esteet** **Osuus kaikista vastaajista*	**Kannustimet** **Osuus kaikista vastaajista*	**Vastaanottajien kannustimet** ***Osuus kaikista vastaanottajista**
Yleinen	1. Huono kustannus-tehokkuus, 79 %	1. Apu priorisointiin, 88 % 2. Apu perusteluun, 86 % 3. Havainnointi aikaisemmin, 77 % 4. Yhteistyöportaali helpottaisi, 70 % 5. Ei muuten olisi havaittu, 67 %	
Melko yleinen	2. Tiedon läpikäyminen on aikaa vievää, 49 %	6. Meille olisi muuten aiheutunut kustannuksia, 50 % 7. Hyödynnämme vain pienen osan, 50 %	Vain jos helposti hyödynnettävää, 30 %
Harvinainen	3. Ajantuhlausta 16 % 4. Turhaa tietoa, 5 % 5. Voin itse kerätä muualta, 10 %		

tietoturvamenoista ja -investoinneista. Kolmannes vastaajista kertoi, ettei heidän organisaatiossaan ollut sisäistä tietoturvatiimiä lainkaan tai tietoturvasta vastasi ulkopuolinen työntekijä (kuvio 3). Yllättäen kyselyn tulosten perusteella sisäisen tietoturvatiimin puute ja korkea ulkoistusaste eivät olleetkaan esteenä tietoturvayhteistyölle ja uhkatiedon vaihdolle. Jakajista 17 % kertoi, että ulkoistukset muodostavat yli 90 % heidän tietoturvakuluistaan ja -investoinneistaan. Viidennes jakajista kertoi myös, ettei heillä ole organisaatiossaan sisäistä tietoturvatyöntekijää. Vaikka tulos saattaa osittain johtua kyselyssä käytetystä laajasta uhkatiedon määritelmästä, se kertoo myös, ettei sisäisen asiantuntijan puute ole este tietoturvan kannal-

Kuvio 3. Ulkoistukset ja sisäinen tietoturvatiimi



ta merkittävän uhkatiedon jakamiselle ja hyödyntämiselle.

Tietoturvaosaamisen kartoittamisessa hyödynsimme Yhdysvaltojen energiaviraston kehittämää C2M2-kybervalmius maturiteettimallia (*Cybersecurity Capability Maturity Model*). Vastausten perusteella organisaatioiden tietoturvaosaaminen on hyvällä tasolla. Ainoastaan resurssipula ja henkilöstön kouluttaminen aiheuttivat jonkin verran haasteita. Puolet vastaajista kertoi, ettei heillä ole riittäviä resursseja tietoturvahaasteiden ratkaisemiseen ja kolmannes oli sitä mieltä, ettei henkilöstö ole sisäistänyt heidän organisaationsa tietoturvapolitiikkaa. Hieman yllättäen, korkea ulkoistusaste saattoi myös olla merkki johdon tuesta tietoturvatyölle. Niiden organisaatioiden edustajista, joissa ulkoistukset muodostivat alle neljänneksen tietoturvakuluista, viidennes koki, ettei heidän organisaationsa tietoturvapolitiikalla ollut johdon tukea. Yli kolme neljäsosaa ulkoistavista yrityksistä yksikään ei kokenut samoin. Käytettävissä olevat resurssit selittävät pitkälti organisaatioiden mahdollisuuksia osal-

listua tietoturvayhteistyöhön. Jakajista puolet kertoi, että heillä on käytettävissään riittävät resurssit. Ei-osallistujista samaa mieltä oli vain kuudennes. Resurssien puute vaikuttaa myös organisaation tietoturvaosaamiseen ja sitä kautta mahdollisuuksiin tehdä tietoturvayhteistyötä. Kolmannes ei-osallistujista kertoi, että työtehtävät on heillä selkeästi määritelty. Jakajista samoin koki yli 80 %. Kolme neljästä ei-osallistujista tunnusti, ettei heidän organisaatiossaan tietoturvatoimenpiteitä suunniteltu etukäteen. Jakajista vain 4 % koki samoin. Lisäksi vain kolmannes ei-osallistujista oli sitä mieltä, että heidän henkilöstönsä on sisäistänyt organisaation tietoturvapolitiikan. Jakajista tätä mieltä oli puolet.

6. Pohdintaa ja johtopäätöksiä

Tutkimuksen tuloksia tulkittaessa on syytä muistaa, että kyselyyn vastasi vain 43 tietoturva-asiantuntijaa, joista kolme neljäsosaa edusti suuria organisaatioita. Muihin tietoturvainvestointikyselyihin verrattuna vastausten määrä on kohtuullinen. Tutkimuksen tulokset eivät siis ole yleistettävissä, mutta niitä voidaan silti pitää suuntaa antavina ja samalla ne tarjoavat näkyvyyttä aihepiiriin, josta on verrattain vähän aineistoa saatavilla. Yksi syy alhaisiin vastausprosentteihin on, ettei aiheesta vielä tiedetä riittävästi sellaisen kyselyn laatimiseksi, joka olisi relevantti laajemmalle vastaajajoukolle. Kyselyn tulosten vertailu kirjallisuuskatsauksessa esitettyihin tietoturvainvestointimalleihin antaa viitteitä siitä, miten olemassa olevia malleja voisi jatkossa kehittää. Ensimmäinen havainto liittyy siihen, minkälaisiksi hyödykkeiksi tietoturva ja kyberturvallisuus koetaan. Toinen havainto kuvastaa organisaatioiden tapaa investoida tietoturvaan. Kolmas havainto koskee organisaatioiden tietoturvayhteistyöstä ja uhkatiedon vaihdosta saatavia tuottoja (*payoffs*).

Tietoturvan taloustieteen kirjallisuudessa ollaan melko yksimielisiä siitä, että organisaatioiden tekemät tietoturvainvestoinnit luovat positiivisia ulkoisvaikutuksia muille toimijoille. Tästä syystä useat tutkijat määrittelevät tietoturvainvestoinnit julkisiksi hyödykkeiksi ja selittävät liian alhaisia tietoturvainvestointeja vapaamatkustamisella (Gordon ym. 2003; Johnson ym. 2011; Grossklags ym. 2008). Camp ja Wolfram (2004) kritisoivat määritelmää jo vuonna 2004 toteamalla, ettei yritysten yksityisistä investoinneista omaan tietoturvaansa muodostu jakamatonta julkista hyödykettä. Taloustieteellisen määritelmän mukaan julkisen hyödykkeen kulutuksesta ei voi sulkea ketään pois ja yhden toimijan kulutus ei pienennä muiden mahdollisuutta käyttää hyödykettä. Julkiset hyödykkeet voidaan myös tuottaa keskitetysti. Jos tietoturva on julkinen hyödyke, niin uhkatiedon jaolle ei ole tarvetta, koska tiedon jakava organisaatio voisi tehdä tarvittavat toimenpiteet myös itse. Kyselyyn vastanneista 56 % kertoi jakavansa uhkatietoa. Heistä kolmannes oli uhkatietoa jakamalla estänyt tietoturvaloukkauksen, josta olisi aiheutunut heille itselleen kustannuksia tai muuta harmia. Jos tietoturva olisi julkinen hyödyke, he olisivat voineet tuottaa tarvittavan tietoturvan itse turvautumatta yhteistyökumppaniin.

Ulkoistukset muodostivat huomattavan osuuden useiden vastaajien edustamien organisaatioiden ICT- ja tietoturvabudjeteista. Puolustajat-hyökkääjät-mallit eivät kuvasta useimpien organisaatioiden arkea. Tarvitaan malleja, joissa organisaatiot ovat tietoturvahyödykkeiden myyjiä ja ostajia. Korkeakaan ul-

koistusaste ICT- ja tietoturvahankinnoissa tai sisäisen tietoturvatiimin puute eivät estäneet tietoturvayhteistyötä tai edes uhkatiedon jakoa. Jakajien uhkatiedon arvo pohjautunee sisäiseen tietoturvaosaamiseen tai organisaation koon mukana tuomaan tilannekuvaan. Pienemmille organisaatioille, joille ei ole sisäistä tietoturvatiimiä, uhkatiedon jakaminen lienee harvemmin ajankohtaista. Kyselyn tulokset tietoturvayhteistyöstä ja uhkatiedon vaihdosta ovat hyvin samanlaisia kirjallisuuskatsauksessa esitettyjen aikaisempien tulosten kanssa. Osallistumalla tietoturvayhteistyöhön toimijat hyötyvät toistensa osaamisesta. Toimivan yhteistyön ja uhkatiedon jaon edellytyksenä on kuitenkin luottamus. Tietoturvayhteistyöhön pakottamalla ja ryhmäkokoja nopeasti kasvattamalla ei välttämättä saada parhaita tuloksia aikaan. Uhkatiedon koettu hyödyttömyys on suurin este uhkatiedon jaolle: Jos ei ole mitään arvokasta jaettavaa niin ei ole mitään syytä jakaa tietoa muille. Hyvä koordinointi oli suurin kannustin uhkatiedon jaolle, joten toimivat yhteistyöratkaisut ovat avainasemassa, kun uusia organisaatioita halutaan osallistuttaa uhkatiedon jakoon.

Jaetusta uhkatiedosta haettiin apua tietoturvatoimenpiteiden perusteluun ja priorisointiin. Useimmissa organisaatioissa on runsauden pula uhkatiedosta, tällöin yhteistyökumppaneilta saadut neuvot auttavat keskittymään tärkeimpiin asioihin. Jaettu uhkatieto koettiin myös kustannustehokkaana tapana parantaa tietoturvaa. Opetuksena on, ettei tietoturvan saralla kaikkea kannata tehdä itse. Pienemmät organisaatiot, joilla ei ole resursseja osallistua tietoturvayhteistyöhön, pystyvät hyötymään muiden osaamisesta ulkoistamalla osan tietoturvan toiminnoistaan. Ulkoistusten onnistuminen riippuu kuitenkin siitä, mitä ulkoistetaan. Scheneierin (2002) mukaan organisaatioiden kannattaa ulkoistaa asiantuntijuutta, muttei johtamista. □

Kirjallisuus

Al Awadhi S. ja A. Morris, "The Use of the UTAUT Model in the Adoption of E-Government Services in Kuwait", teoksessa *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (HICSS 2008): 219–219.

Anderson, R. (2001), "Why information security is hard – an economic perspective", *Proceedings 17th Annual Computer Security Applications Conference* (ACSAC 2001), New Orleans, LA, USA, http://ieeexplore.ieee.org/document/991552/ (viitattu 2.2.2018).

Anderson, R. ja Moore, T. (2006), "The Economics of Information Security", *Science* 314(5799): 610–613.

Anderson, R., ja Fuloria, S. (2009), "Security economics and critical national infrastructure", The Eighth Workshop on the Economics of Information Security (WEIS 2009), University College London, England, http://www.cl.cam.ac.uk/rja14/Papers/econ-cni09.pdf (viitattu 2.2.2018).

Akerlof, G. A.(1970) "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism", *Quarterly Journal of Economics* 84: 488–500.

BBC (2017), "NHS could have prevented WannaCry ransomware attack", http://www.bbc.com/news/technology-41753022 (viitattu 2.2.2018).

Bisogni, F., Cavallini, S., ja Trocchio, S. (2011), "Cybersecurity at European level: The role of information availability", *Communications & Strategies* 1: 105–124.

Böhme R. (2010), "Security Metrics and Security Investment Models", teoksessa Echizen I., Kunihiro N., Sasaki R. (toim.), *Advances in Information and Computer Security. IWSEC 2010. Lecture Notes in Computer Science*, Vol 6434. Springer: 10–24.

Camp, L.J. ja Wolfram, C. (2004), "Pricing Security: Vulnerabilities as Externalities", teoksessa Camp, L.J. ja Lewis, S. (toim.), *Economics of Information Security: Advances in Information Security*, 12, Academic Publishers.

CGI (2015), "Is a cyber breach inevitable? Cyber security challenges in the Netherlands", https://automatie-pma.com/wp-content/uploads/2015/05/CGI-Cyber-Security-White-Paper-Final.pdf (viitattu 2.2.2018).

Chesbrough, H. ja Appleyard, M. (2007), "Open innovation and strategy", http://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1021\&context=busadmin_fac (viitattu 2.2.2018).

Chesbrough, H., Crowther, A.K. (2006), "Beyond high tech: early adopters of open innovation in other industries", *R&D Management* 36: 229–236.

Choi, J.P., Freshtam, C. ja Gandal, N. (2010), "Network Security: Vulnerabilities and Disclosure Policy", *Journal of Industrial Economics*, 58(4):868-894.

CPNI (2015), "Threat intelligence infographic CPNI", Centre for the protection of national infrastructure (archive), https://www.ncsc.gov.uk/guidance/threat-intelligence-executive-summary-infographic (viitattu 2.2.2018).

Leeuw,d. D ja Bergstra, J. (2007), *The History of Information Security: A Comprehensive Handbook*, Elsevier Science.

DOE (2014), "Cybersecurity Capability Maturity Model (C2M2)", Department of Energy, http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf (viitattu 2.2.2018).

ENISA (2010), "Incentives and challenges for information sharing in the context of network and information security", European Network and Information Security Agency, https://www.enisa.europa.eu/news/enisa-news/incentives-challenges-for-cyber-security-information-sharing-in-europe-identified (viitattu 2.2.2018).

Gal-Or, E. ja Ghose, A. (2005), "The economic incentives for sharing security information", *Information Systems Research* 16: 186–208.

Gartner (2017a), "Gartner says 8.4 billion connected 'things' will be in use in 2017, up 31 percent from 2016", https://www.gartner.com/newsroom/id/3598917 (viitattu 2.2.2018).

Gartner (2017b), "Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017", https://www.gartner.com/newsroom/id/3784965 (viitattu 2.2.2018).

Giovinazzo, W. (2003), *Internet-enabled Business Intelligence*, Prentice Hall Professional.

Gordon, L. ja Loeb, M. (2002), "*The economics of information security investment*", ACM Transactions on Information and System Security 5: 438–457.

Gordon, L., Loeb, M. ja Lucyshyn, W. (2003), "Sharing information on computer systems security: An economic analysis", *Journal of Accounting and Public Policy* 22: 461–485.

Gordon, L., Loeb, M., Lucyshyn, W. ja Zhou, L. (2015), "Externalities and the magnitude of cybersecurity underinvestment by private sector firms: A modification of the Gordon-Loeb model", *Journal of Information Security* 6: 24–30.

Grossklags, J.,Christin, N. ja Chuang, J. (2008), "Secure or Insure? A Game-Theoretic Analysis of Information Security Games", Proceeding of the 17th International Conference on World Wide Web 2008, WWW 2008, Beijing: 209–218. https://www.andrew.cmu.edu/user/nicolasc/publications/GCC-WWW08.pdf (viitattu 23.4.2018).

Gurbaxani, V. ja Whang, S. (1991), "The impact of information systems on organizations and markets", https://dl.acm.org/citation.cfm?id=99990 (viitattu 2.2.2018).

Hausken, K. (2007), "Information sharing among firms and cyber attacks", *Journal of Accounting and Public Policy* 26: 639–688.

Heal, G. ja Kunreuther, H. (2004), "Interdependent security: A general model", NBER Working Paper 10706.

Hirshleifer, J. (1987), "From weakest link to best-shot: The voluntary provision of public goods", *Public Choice* 41: 371–386.

Honeyman, P., Schwartz, G. ja Van Assche A. (2007), "Interdependence of Reliability and Security", Economics of Information Security (WEIS), Pittsburg, http://www.econinfosec.org/archive/weis2007/papers/71.pdf (viitattu 23.4.2018).

Internetworldstats (2018), "Internet user statistics", http://www.internetworldstats.com/stats.htm (viitattu 2.2.2018).

Johnson, B., Böhme, R. ja Grossklags, J. (2011), "Security Games with Market Insurance", teoksessa Baras, J.S, Katz, J. ja Altman, E. (toim.), *Decision and Game Theory for Security*, Springer: 117–130.

Koepke, P. (2017), "Cybersecurity information sharing incentives and barriers", Technical report, Cyber-security Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, http://web.mit.edu/smadnick/www/wp/2017-13.pdf (viitattu 2.2.2018).

Koivunen, E. (2010), "Why wasn't I notified? Information security incident reporting demystified", teoksessa Aura, J., Järvinen, K. ja Nyberg, K. (toim.), *Information Security Technology for Applications*, Springer.

Kox, H. ja Straathof, B. (2013), "Economic aspects of internet security", Background Report, Netherlands Bureau for Economic Policy Analysis (CPB), http://www.cpb.nl/en/publication/economic-aspects-internet-security (viitattu 2.2.2018).

Krebs, B. (2017), "Krebsonsecurity hit with record DDoS", https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (viitattu 2.2.2018).

Laszka, A., Felegyhazi, M. ja Buttyan, L. (2014), "A Survey of Interdependent Information Security Games", ACM Computing Surveys, 47(2): Article 23.

Laube, S. & Böhme, R. (2016), "The economics of mandatory security breach reporting to authorities", *Journal of Cybersecurity* 2: 29–41.

Laukkanen, P., Sinkkonen, S., ja Laukkanen, T. (2008), "Consumer resistance to Internet banking: Postponers, opponents and rejecters", *The International Journal of Bank Marketing* 26: 440–455.

Laursen, K. ja Salter, A. (2006), "Open for innovation: the role of openness in explaining innovation performance among U.K. manufacturing firms", *Strategic Management Journal* 27: 131–150.

Michelino, F., Lamberti, E., Cammarano, A. ja Caputo, M. (2015), "Measuring open innovation in the bio-pharmaceutical industry", *Creativity and Innovation Management* 24: 4–28.

Moore, T. ja Anderson, R. (2012), "Internet Security", teoksessa Peitz, M., Waldfogel, J. (toim.), *The Oxford Handbook of the Digital Economy*, Oxford University Press: 572–599.

Moore, T., Dynes, S. ja Chang, F. (2016), "Identifying how firms manage cybersecurity investment", Workshop on the Economics of Information Security (WEIS), University of California Berkeley, https://tylermoore.utulsa.edu/weis16ciso.pdf (viitattu 2.2.2018).

Morgan, S. (2018), "2018 Cybersecurity Market Report", Cybersecurity Ventures, https://cybersecurityventures.com/cybersecurity-market-report/ (viitattu 30.4.2018).

Naghizadeh, P. ja Liu, M. (2016), "Opting Out of Incentive Mechanisms: A Study of Security as a Non-Excludable Public Good", *IEEE Transactions on Information Forensics and Security* 11: 2790–2803.

PCCIP (1997), "Critical foundations. Protecting America's Infrastructures", President's commission on critical infrastructure protection, https://www.nist.gov/sites/default/files/documents/2017/04/26/keyes_part2_032613.pdf (viitattu 2.2.2018).

Ram, S. ja Seth, J. (1989), "Consumer resistance to innovations: the marketing problem and its solution", *The Journal of Consumer Marketing* 6: 5–14.

Robinson, C. (1999), "Network effects in telecommunications mergers – mci worldcom merger: Protecting the future of the internet", https://www.justice.gov/atr/speech/network-effects-telecommunications-mergers-mci-worldcom-merger-protecting-future-internet (viitattu 2.2.2018).

Rowe, B. ja Gallaher, M. (2006), "Private sector cyber security investment strategies: An empirical analysis", https://pdfs.semanticscholar.org/a188/0f3fc72ab11f5eca24fa6970eb2a8ab69c4f.pdf (viitattu 2.2.2018).

Rowe, B. (2007), "Will Outsourcing IT Security Lead to a Higher Social Level of Security?", Workshop on the Economics of Information Security (WEIS), Pittsburg, http://www.econinfosec.org/archive/weis2007/papers/47.pdf (viitattu 23.4.2018).

Schneier, B. (2002). "The Case for Outsourcing Security", Supplement to *IEEE Computer Magazine* 35: 20–21, 26.

Sisäministeriö (2017), *Tietoverkkorikollisuuden torjuntaa koskeva selvitys*, Sisäministeriön julkaisu 14/2017, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1 (viitattu 2.2.2018).

van den Meulen, N. (2015), "Investing in cybersecurity", Technical report, RAND Europe, WODC, https://english.wodc.nl/onderzoeksdatabase/2551-investeren-in-cyber-security.aspx (viitattu 2.2.2018).

Valtioneuvosto (2013), "Suomen kyberturvallisuusstrategia", *Valtioneuvoston periaatepäätös*.

Varian, H. (2204), "System Reliability and Free Riding", http://people.ischool.berkeley.edu/~hal/Papers/2004/reliability (viitattu 2.2.2018).

Venkatesh, V., Morris, M., Davis, G. ja Davis, F. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly* 27: 425–478.