LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tuotetietovuotojen ennaltaehkäisy yhteistyökumppaniverkostossa

Erkkilä Santtu

2013 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Tuotetietovuotojen ennaltaehkäisy yhteistyökumppaniverkostossa

Santtu Erkkilä
Turvallisuusosaamisen
koulutusohjelma
Opinnäytetyö
Huhtikuu, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Yhteiskuntatieteiden, liiketalouden ja hallinnon ala
Turvallisuusosaamisen koulutusohjelma

Santtu Erkkilä

Tuotetietovuotojen ennaltaehkäisy yhteistyökumppaniverkostossa

Vuosi 2013 Sivumäärä 106

Tuotetietovuodot ovat vahingollisia yritysten liiketoiminnalle, koska ne luovat erilaista ja usein negatiivistä sekä huhuihin perustuvaa mielikuvaa yritysten tulevista tuotteista. Negatiivinen ja väärään tietoon perustuvat ensivaikutelma tuotteesta vaikuttaa kuluttajien ostokäyttäytymiseen ja siten vähentää myyntiä. Tuotetietovuodot tulevat kalliiksi yrityksille, koska niiden täytyy investoida lisää markkinointiviestintään pystyäkseen vaikuttamaan kuluttajien mielikuviin. Tuotetietovuotojen määrä on kasvanut merkittävisti viime vuosina, koska bloggerit ovat luoneet markkinat, jotka pyrkivät kaikin keinoin saamaan käsiinsä tietoa julkaisemattomista tuotteista julkaistakseen ne blogisivustollaan. Bloggerit rahoittavat toimintansa mainoksilla, mikä tarkoittaa sitä, että heidän tulonsa ovat riippuvaisia sivuston kävijämääristä. Kävijämäärien suuruus on puolestaan riippuvainen sivuston sisällön houkuttelevuudesta ja tuoreudesta.

Nykyinen liiketoiminta on kansainvälistä ja laajasti verkottoitunutta, mikä tarkoittaa työskentelyä lukuisten eri kulttuureista ja erilaisilta liiketoiminta-alueilta tulevien yhteistyökumppaneiden kanssa. Työskentely pitää sisällään arvokkaan tuotetiedon jakamista yhteistyökumppaneille, jotta nämä voivat tuottaa lisäarvoa yrityksen liiketoiminnalle. Yhteistyökumppaneiden kanssa työskentely lisää tietoriskin toteutumisen todennäköisyyttä, koska yrityksen arvokasta tietoa tullaan käsittelemään useammissa paikoissa ja useampien eri ihmisten toimesta. Yhteistyökumppaniverkostot koostuvat usein sadoista tai jopa tuhansista yrityksistä, mikä tekee turvallisuuden hallinnasta erittäin haastavaa. Yhteistyökumppanien ja ostajayrityksen välillä on sopimus, joka määrittää miten arvokasta tietoa tulee käsitellä ja millaisilla turvallisuuskontrolleilla tulee suojata. Noiden muodollisten kontrollien lisäksi ostajayritys yleensä auditoi yhteistyökumppanin turvallisuusjärjestelyt saadakseen käsityksen heidän turvallisuuskyvykkyydestään. Muita tyypillisiä käytäntöjä ovat yritysten välinen turvallisuusyhteistyö ja yhteistyökumppanin turvallisuustietoisuustason parantaminen.

Opinnäytetyöni pureutuu ylläkuvattuihin haasteisiin Nokian yhteistyökumppaniverkostossa. Työn tavoitteena on selvittää millaisilla menetelmillä voidaan ennaltaehkäistä tuotetietovuotoja Nokian yhteistyökumppaniverkostossa. Työssä hyödynnetään toimintatutkimuksen menetelmää, koska se soveltuu hyvin kehittämistyön tueksi. Osana toimintatutkimusta tehtiin perusteellinen nykytila-analyysi Nokian yhteistyökumppaniverkostosta sekä siihen liittyvistä sidosryhmistä. Myös viime vuosien tuotetietovuototapaukset analysoitiin, jotta ymmärretään, miten ja miksi vuodot syntyvät. Vuotojen taustalla ovat yleensä ihmiset, jotka tietämättömyyttään, vahingossa tai tahallaan vuotavat tietoa paikkoihin, joista bloggerit ne löytävät.

Menetelmien jalkauttamisessä keskityttiin kaikkiin sidosryhmiin ja niissä erityisesti ihmisiin ja uudenlaisen, avoimemman turvallisuuskulttuuriin luomiseen Nokian ja sen yhteistyökumppanien välille. Painopiste oli siis sosiaalisten kontrollien käytön lisäämisessä. Käytetyillä menetelmillä onnistuttiin vähentämään tuotetietovuotoja yhteistyökumppaniverkostossa.

Asiasanat: Tuotetietovuoto, yhteistyökumppani, turvallisuuskulttuuri, muodollinen kontrolli, sosiaalinen kontrolli

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Master's Programme in Security Management

Santtu Erkkilä

Leak prevention in the supplier base

Year 2013 Pages 106

Product information leakages are a current phenomenon. There are numerous bloggers who seek un-launched product information as they want to publish fresh and interesting information at their blog sites. Leaks provide more visitors for their websites enabling bloggers to get more income from advert selling. However, leakages cause severe damages for companies who intend to surprise consumers with their new products. Furthermore, leakages are typically based on incomplete and in many cases rumor based information giving falsified messages to potential consumers.

The business of today is highly networked: companies collaborate with suppliers coming from various cultures globally. As part of the collaboration companies share valuable assets with suppliers allowing them to create added value for the buyer company. Sharing of assets raises the propability of information risk occurrence because the assets will be handled by hundreds or even thousands of suppliers and in some cases their sub-suppliers. This means that there are thousands of people from various cultures with various security cultures handling confidential or secret information. Therefore it is a huge challenge for large corporations to manage information risk related to suppliers.

Most companies manage supppliers by utilizing formal controls meaning agreements including confidentialty clauses and security requirement appendix. Suppliers are expected to comply with security requirements and to follow the confidentiality clauses when handling sensitive information. Compliance with requirements is validated with audits and assessments. Other typical collaboration security methods are security briefings and security relationship activities between the parties.

As part of the thesis project, leakages and types of challenges were analysed which arise from sharing sensitive product assets with suppliers coming from different cultural backgrounds globally. The objective was to identify effective leak prevention methods that help to reduce product leakages in Nokia's supplier base. The action research method was utilized due to its good useablity in cases where there is a need to develop various activities. A detailed current state analysis was conducted to understand existing challenges and types of root causes behind the product leakages. The current state analysis showed clearly that leakages are caused by people either by mistake or maliciously.

Subsequently, improvement activities were implemented among various stakeholder groups to ensure harmonized practices among people working in the supplier interface. The main focus was on people's awareness and on creating a new security culture between Nokia and its suppliers. Social controls were mainly utilized for motivating people and for changing the supplier's attitude towards security matters. The implemented methods functioned succesfully and aided Nokia in reducing product leakages in the supplier base.

Keywords: Product information leakage, supplier, security culture, formal control, social control

Sisällys

1 Johdanto

Tuotetietovuotojen määrä on kasvanut viime vuosina, koska laajentunut internetin ja sosiaalisen median käyttö on luonut markkinat teknologiablogisivustoille, joiden ydintehtävänä on houkuttelevan tiedon ja huhujen julkaisu. Tämä on ilmiönä varsin uusi, eikä kovin hyvin ymmärretty yrityksissä ja yhteisöissä, jotka eivät ole kärsineet siitä. @Evleaks on loistava esimerkki bloggerista, jonka päätyönä on vuotaa tuotetietoa. Hänellä on noin 20000 seuraajaa Twitterissä, mikä osaltaan kertoo ilmiön vaikuttavuudesta. Houkuttelevin tieto on yleensä sellaista, mitä muut eivät ole vielä julkaisseet, eli jonkin yrityksen luottamuksellista tuotetietoa. Markkinoiden olemassaolo merkitsee sitä, että huonosti suojattu tuotetieto vuotaa helposti internettiin, jossa se pienessä hetkessä saavuttaa koko maailman ja vie yritykseltä mahdollisuuden yllättää markkinat uudella tuotteellaan.

Tietovuodot vahingoittavat yrityksiä monin eri tavoin - ja voivat jopa estää niitä pääsemästä strategisiin tavoitteisiin. Nokian liiketoiminta on viime vuosina kärsinyt tuotetietovuodoista. Nykyisin liiketoiminta on laajasti verkostoitunutta, tarkoittaen työskentelyä lukuisten yhteistyökumppaneiden kanssa. Työskentely pitää yleensä sisällään luottamuksellisen tiedon jakamista toimittajien kanssa, jotta nämä voivat tuottaa lisäarvoa yritykselle. Arvokkaan tiedon jakaminen yhteistyökumppaneiden kanssa nostaa yleensä vahinkoriskin todennäköisyyttä, koska tiedon käyttäjämäärä kasvaa ja suojaaminen jää kumppanin vastuulle. Yrityksissä ajatellaan usein, että yhteistyökumppanit hoitavat tiedon suojaamisen kunhan heille vain annetaan paksu nippu vaatimuksia ja sitten homma hoituu kuin itsestään. Mikäli jokin menee pieleen, niin vikahan on yhteistyökumppanissa, ei yrityksen tavassa toimia. Tuotetietovuotojen ennaltaehkäisyä yhteistyökumppaniverkostossa ei ole tutkittu aikaisemmin.

Opinnäytetyössäni pureudun yllämainittuihin haasteisiin, sekä pyrin löytämään Nokian liiketoimintaa tukevia ratkaisuita, joiden avulla voidaan ennaltaehkäistä tuotetietovuotoja yhteistyökumppaniverkostossa. Tavoitteisiin pääseminen vaatii suurta muutosta useiden sidosryhmien ajattelutavassa ja toiminnassa, mutta onnistuessaan tulee auttamaan yritystä strategisiin tavoitteisiin pääsemisessä ja vähentämään tietovuotojen aiheuttamia vahinkoja. Tämä työ on osa Nokian tuotetietovuotojen ennaltaehkäisyohjelmaa, joka pyrkii sisäisistä ja ulkoisista tekijöistä johtuvien vuotojen vähentämiseen ja ennaltaehkäisemiseen. Aiheeni on laaja, koska vuotoja tapahtuu erilaisissa prosesseissa, jotka liittyvät useisiin erilaisiin liiketoimintoihin. Keskeisenä yhteisenä nimittäjänä tietovuotodoille voidaan pitää ihmisiä, jotka vuotavat tietoa joko vahingossa tai tahallaan. Tästä johtuen pyrin pääasiassa löytämään sellaisia ennaltaehkäiseviä menetelmiä, joilla voidaan vaikuttaa ihmisten turvallisuuskäyttäytymiseen, niin että he olisivat motivoituneita suojaamaan arvokasta tietoa ja että heillä olisi tarvittavat tiedot sekä taidot toimia oikein hektisessä työelämässä.

2 Kohteen esittely

Nokian ydintehtävä on ”connecting people”, jolla tarkoitetaan lisäarvon tuottamista ihmisten elämään mobiilituotteita hyödyntäen. Nokian liiketoiminnan perustana on upeiden ja innovatiivisten mobiilituotteiden tuominen markkinoille. Toiminta-alueena on koko maailma, joten tuotteita löytyy useille eri kohderyhmille Nigeriasta Yhdysvaltoihin. Maailmanlaajuinen toiminta-alue tarkoittaa myös sitä, että Nokian valmistus-, tuotekehitys-, myynti- ja markkinointitoiminnot on sijoitettu keskeisimmille markkina-alueille. Nykyisin mobiiliin liiketoimintaan liittyy läheisesti termi ekosysteemi, jolla tarkoitetaan useiden toimijoiden muodostamaa kokonaisuutta, jonka tehtävä on tuottaa lisäarvoa kuluttajille. Mobiilissa liiketoiminnassa ekosysteemejä on muodostunut muun muassa Applen, Androidin ja viimeisimpänä Windows Phone:n ympärille. Mobiilissa liiketoiminnassa ekosysteemiin kuuluvat yleensä laitevalmistajat, sovelluskehittäjät, ohjelmistotalot, operaattorit ja erilaiset palveluntarjoajat. Nokian organisaatio koostuu neljästä liiketoimintayksiköstä ja niitä tukevista toiminnoista. (Nokia 2012).

2.1 Nokian liiketoimintayksiköt

Älypuhelinyksikön tehtävänä on uusien älypuhelinten kehittäminen yhteistyössä Microsoftin kanssa. Matkapuhelinyksikön tehtävänä on tarjota ajanmukaisia ja kohtuuhintaisia mobiilikokemuksia ihmisille kaikkialla maailmassa. Innovatiivisuuttaan ja kasvumarkkinaosaamistaan hyväksikäyttäen yksikkö keskittyy tarjoamaan ihmisille mahdollisuuden internet-yhteyteen ja sovellusten käyttöön. Location & Commerce yksikössä kehitetään integroituja, sijaintiin perustuvia tuotteita ja palveluja kuluttajille sekä alustaan ja paikalliseen liiketoimintaan liittyviä palveluja laitevalmistajille, sovelluskehittäjille, verkko-operaattoreille, kauppiaille ja mainostajille. Myynti- ja markkinointiyksikkö vastaa kaikkien Nokia-tuotteiden osalta myynnistä, vetovoimaisen markkinoinnin ja viestinnän toteuttamisesta, kilpailukykyisen paikallisen ekosysteemin luomisesta, hankinnasta, asiakaspalvelusta, valmistuksesta, IT-palveluista sekä logistiikasta. Muita toimintoja ovat muun muassa muotoiluyksikkö, tutkimuskeskus ja tukitoiminnot, kuten talous- ja henkilöstöhallinto sekä turvallisuusyksikkö. (Nokia 2012).

2.2 Nokian strategiset päätavoitteet

Nokian vuonna 2011 julkistettu strategia on jaettu kolmeen päätavoitteeseen: markkina-johtajuuden palauttaminen älypuhelimissa, seuraavan miljardin yhdistäminen internetiin ja investointi seuraavan sukupolven käänteentekeviin tekniikoihin. Neljäntenä päätavoitteena voidaan pitää muutoksen läpiviemistä, jossa Nokiasta tehdään paremmin vastuullisuuteen, nopeuteen ja tuloksellisuuteen keskittyvä yritys. Saavuttaakseen tavoitteensa älypuhelimissa

Nokia aloitti strategisen yhteistyön Microsoftin kanssa, minkä se uskoo auttavan saavuttamaan menetetyt markkina-asemat. Nokian ja Microsoftin yhteisenä tavoitteena on rakentaa yhdessä globaali ekosysteemi, joka on parempi kuin jo olemassa olevat. Matkapuhelimissa Nokian strategiana on hyödyntää innovaatiotaan ja vahvuuttaan kasvavilla markkinoilla voidakseen tarjota miljoonille ihmisille ensimmäisen internet- ja sovelluskokemuksen. Tavoitteena on tuoda internet seuraavan miljardin kuluttajan ulottuville tarjoamalla mielenkiintoisia, edullisia ja paikallisesti räätälöityjä kokemuksia, erityisesti kehittyvillä markkinoilla. Nokia haluaa turvata tulevaisuutensa investoimalla uuden sukupolven innovatiitioihin, joiden tarkoituksena on tuoda uusia ominaisuuksia tuleviin tuotteisiin tai luoda jopa täysin uusia alustoja mobiilin liiketoiminnan pohjaksi. (Nokia 2012).

2.3 Kilpailuedut

Nokialla on useita kilpailuvaltteja, jotka auttavat sitä tavoitteiden saavuttamisessa. Nokian merkittävimpänä kilpailuvalttina on pidetty viimeiseen asti hiottua toimitusketjua, joka on samalla nopea ja kustannustehokas. Toimitusketjulla on merkittävä asema kilpailuedun tuottajana, mutta on Nokialla muitakin ässiä hihassaan. Globaali toiminta-alue mahdollistaa liiketoiminnan sijoittamisen yritykselle eniten hyötyä tuottaviin kohteisiin. Tästä esimerkkinä voidaan pitää viime aikaista tiedotetta laitteiden valmistuksen keskittämistä Aasiaan, jossa suurin osa komponenttivalmistuksestakin sijaitsee. Aasian lisäetuna voidaan myös pitää pienempiä työntekijäkustannuksia, jotka mahdollistavat suuremmat katteet ja paremman kilpailukyvyn edullisesten matkapuhelimien markkinoilla. Maailmanlaajuinen liiketoimintamalli tuo mukanaan globaalisti tunnetun brändin eli tuotemerkin ja mahdollisuuden tuottaa laitteita ja palveluita lähellä asiakkaitaan. Tästä hyvänä esimerkkinä ovat vahvat asiakassuhteet matkapuhelinoperaattoreihin ympäri maailmaa. Nokialla on myös erittäin vahva patenttisalkku, mikä tuo sille kahdenlaista etua: lisenssituloja kilpailijoilta ja mahdollisuuden tuoda uusia teknologioita markkinoille nopeammin kuin sen kovimmat kilpakumppanit. Useista eri kulttuureista tulevat ihmiset ja heidän osaamisensa ovat myös Nokian selkeä vahvuus. Nokia on jo vuosia sitten ymmärtänyt ulkoistamisen merkityksen ja tämän seurauksena se osaa hankkia tarvitsemaansa osaamista yhteistyökumppaneilta. Tämä mahdollistaa tarvittaessa nopeatkin liiketoiminnan muutokset.

2.4 Nokian Yritysturvallisuusyksikkö

Yritysturvallisuusyksikön ydintehtävänä on suojella Nokian henkilökuntaa, liiketoimintaa ja arvoja, mikä toteutetaan kehittämällä ja pitämällä esillä yrityksen yhteistä turvallisuuskulttuuria. Käytännössä tämä tarkoittaa sitä, että yrityksen johto määrittää liiketoimintastrategian vaativan turvallisuustason, jota liiketoimintayksiköt toteuttavat. Yritysturvallisuusyksikön tehtävänä on tuottaa turvallisuustietoa johdon päätöksenteon tueksi

ja auttaa liiketoimintayksiköitä tavoitetason saavuttamisessa sekä levittää monipuolista turvallisuustietoutta Nokian sisällä. Yritysturvallisuusyksikkö koostuu globaalista tietoturvallisuustiimistä ja viidestä alueorganisaatiosta. Tämän lisäksi yritysturvallisuusyksikkö on määritellyt kuusi keskeistä palvelua, jotka kertovat asiakkaille eli liiketoimintayksiköille, millaisissa asioissa yksikkö heitä tukee. Nämä kuusi palvelua ovat toimitilaturvallisuus, henkilöturvallisuus, kriisinhallinta, toimitusketjunturvallisuus, tuotannonturvallisuus ja tietoturvallisuus. Palvelujen toimittamiseen liittyy usein konsultointia, turvallisuustietoisuuden parantamista, turvallisuuskatselmointeja ja yhteistoimintaa eri sidosryhmien kanssa. Yritysturvallisuusyksikön vahvuutena on läsnäolo merkittävimmissä toimintamaissa. Yksikön henkilökunta koostuu useista eri kansallisuuksista, mikä auttaa luomaan paremman ymmärryksen keskeisten liiketoimintamaiden turvallisuuskulttuureihin ja ominaisiin riskeihin. Henkilökunnan turvallisuusosaaminen on hyvällä tasolla ja maailman mittakaavassa huippuasiantuntemusta löytyy kaikilta yritysturvallisuuden osa-alueilta.

Yritysturvallisuusyksikkö luo oman yksikkökohtaisen strategian, joka pohjautuu yrityksen ydinstrategiaan. Keskeiset vaikuttimet turvallisuusstrategiaa luodessa ovat: yrityksen strategiset tavoitteet, yritysturvallisuusyksikön ydintehtävä, käytettävissä olevat resurssit ja merkittävimmät tunnistetut riskit keskeisimmillä liiketoiminta-alueilla. Strategian määrittelyn seurauksena puolivuosittain tai vuosittain valitaan neljä-viisi keskeistä strategista tavoitetta, jotka merkittävimmin tukevat Nokian ydinstrategiaa, edellä mainitut vaikuttimet huomioiden. Nykyisessä strategiassa tuotetietovuotojen ennaltaehkäisy on yritysturvallisuusyksikön keskeinen strateginen painopistealue. Tietovuodolla tarkoitetaan yrityksen omistaman tiedon päätymistä vääriin käsiin ja sitä kautta vuotamista internettiin tai kilpailijalla. Tietovuodoilla on yleensä negatiiviset seuraukset. Perusteet saadaan edellä mainituista turvallisuusstrategian keskeisistä vaikuttimista.

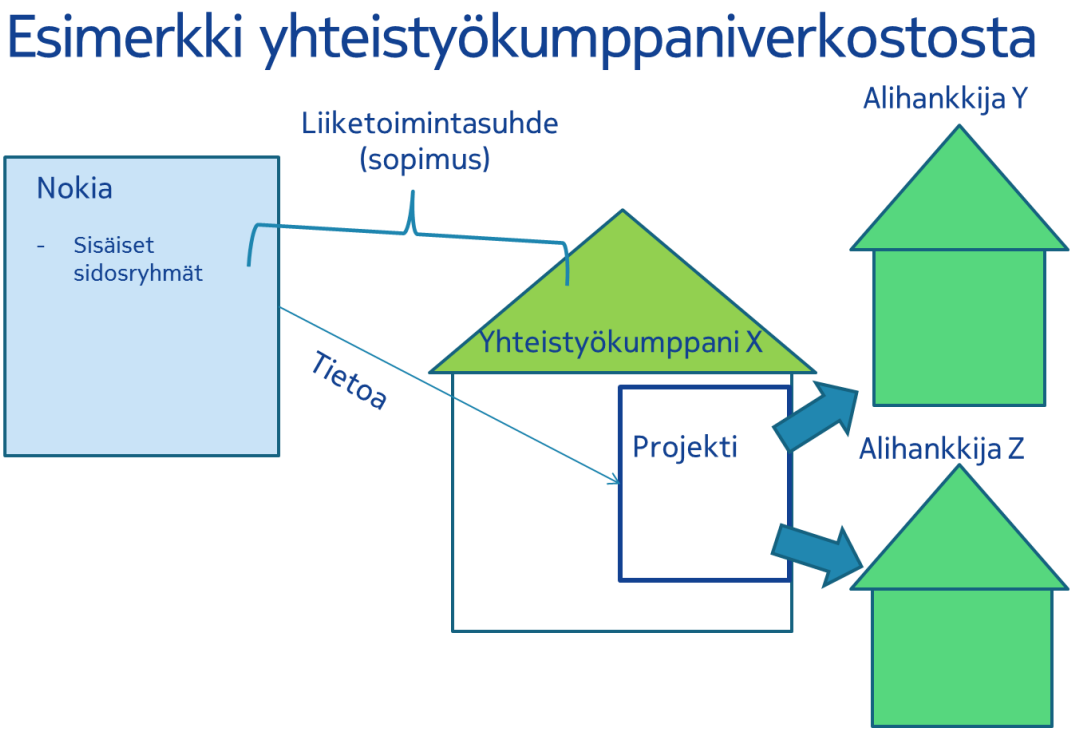
Nokian kolme keskeisintä strategista tavoitetta ovat: markkinajohtajuuden palauttaminen älypuhelimissa, internetin tuominen seuraavalle miljardille ja investointi seuraavan sukupolven käänteentekeviin tekniikoihin. Uusien tuotteiden kehittämiseen liittyy tuotetietoa, jota voidaan yrityssalaisuuksikin kutsua. Tuotetiedolla tarkoitetaan esimerkiksi tuotteen uusia ominaisuuksia, uutta teknologiaa, tuotteen ulkoasua, uudistettua käyttäjäkokemusta tai hintaa. Tämä tieto on yleensä sellaista, mitä sen kilpailijoilla ei ole käytettävissään, mikä puolestaan tuo yritykselle kilpailuetua. Luonnollisesti markkinatkaan eivät ole tietoisia tällaisestä tiedosta, kunnes se julkaistaan virallisesti osana uutta tuotetta. Tuotetiedon ennenaikaisella vuotamisella on monenlaisia seurauksia, joista merkittavimmät ovat tulevan tuotteen saama negatiivinen ja huhuihin pahjautuva maine, osittaisen kilpailuedun menetys, sekä markkinointiviestintäkyvyn osittainen menetys. Tehokas tietovuotojen ennaltaehkäisy auttaa Nokiaa suojaamaan kilpailuetujaan ja mahdollista kyvyn

yllättää markkinat positiivisesti ja sitä kautta myyntimäärien nousun myötä kasvattaa markkinaosuuttaan suhteessa kilpaijoihinsa.

Tuotetietovuotojen ennaltaehkäisy liittyy ensisijaisesti liiketoiminnan suojaamiseen, joka on osa Nokian yritysturvallisuusyksikön missiota. Yritysturvallisuusyksiköllä on kohtuulliset henkilöresurssit tuotetietovuotojen ennaltaehkäisyyn. Etuna on henkilöresurssien sijainti lähellä merkittäviä toimintoja, kuten tuotekehityskeskuksia. Viime vuosina on tapahtunut useita merkittäviä tuotetietovuotoja, jotka ovat osaltaan vaikuttaneet negatiivisesti Nokian myyntiin ja joissain tapauksissa myös epäsuorasti osakkeen arvoon. Tällä hetkellä vuotoriskin todennäköisyys on suuri, minkä vuoksi ennaltaehkäisy on yritysturvallisuusyksikön keskeisin strateginen tavoite. Nokian sisäisten analyysien perusteella voidaan todeta, että vuotojen määrän kasvuun on useita eri syitä, joiden taustalla on Nokian tulevien tuotteiden ja niihin liittyvän tiedon kiinnostavuuden kasvu. Internet on täynnä mobiiliin liiketoimintaan vihkiytyneitä www-sivustoja ja blogeja, jotka käyttävät monenlaisia keinoja saadakseen mielenkiintoista tietoa sivustoilleen. Nokian vuototilastojen perusteella tietoa vuotaa ulos muun muassa inhimillisten virheiden, tietämättömyyden ja huonojen prosessien seurauksena sekä laiminlyöntien johdosta. Yritysvakoilun mahdollisuuttakaan ei voi sulkea pois syistä puhuttaessa. Vuotojen taustalla on eri sidosryhmien edustajia, joista suurimmat ryhmät ovat sisäiset työntekijät ja yhteistyökumppanit.

2.5 Yhteistyökumppaniverkosto

Nokia työskentelee laajan yhteistyökumppaniverkoston kanssa, jonka yritykset tulevat ympäri maailmaa. Yhteistyökumppanit työskentelevät lukuisilla eri liiketoiminta-alueilla, toimittaen Nokialle erilaisia palveluita, komponetteja, sopumusvalmistusta, markkinointihyödykkeitä ja niin edelleen. Yhteistyökumppaneiden ja Nokian välillä on olemassa sopimus, joka määrittää yhteistyön sisällön ja kumppanilta edellytettävät tuotokset. Osana sopimusta on salassapitopykälät, jotka määrittävät kuinka arvokasta tulee käsitellä. Nokian yleiset turvallisuusvaatimukset ovat sopimuksen liitteenä. Turvallisuusvaatimusten tarkoituksena on varmistaa, että yhteistyökumppanin turvallisuuskyvykkyys on riittävällä tasolla. Nokia antaa yleensä tuotetietoa tai muuta arvokasta omaisuutta yhteistyökumppanien käyttöön, jotta nämä voivat tuottaa siitä lisäarvoa Nokian liiketoiminnalle. Nykyisessä liiketoiminnassa on yleistä, että yhteistyökumppanit käyttävät omia alihankkijoitaan tuottamaan osan Nokian tilaamista tuotoksista. Tämä tarkoittaa sitä, että jo yhden kumppanin kanssa toimiessa, yrityksen omistama tieto saattaa päätyä useiden eri maissa toimivien alihankkijayritysten haltuun. Tällainen laajasti verkottunut liiketoimintamalli kasvattaa tietovuotojen todennäköisyyttä, koska tieto altistetaan useiden eri kullttuureista tulevien ihmisten haltuun.



Kuvio 1: Esimerkki tieto-omaisuuden liikkeistä yhteistyökumppaniverkostossa

3 Tutkimuksen tausta

Yritysturvallisuusyksikön tärkein strateginen tavoite on tuotetietovuotojen ennaltaehkäisy, joka osaltaan tukee yrityksen liiketoiminnan strategisia tavoitteita. Tällä hetkellä vahingollisia vuotoja tapahtuu paljon ja niiden taustalla on useita syitä, mikä tarkoittaa sitä, että ei ole olemassa vain yhtä keinoa, jolla tuotetietovuodot voidaan ennaltaehkäistä. Ratkaisuksi tarvitaan perusteellista keinovalikoiman analysointia ja testausta käytännössä, jotta löydetään toimivimmat keinot. Tietovuodot ovat usein myös yrityskulttuurikysymys, minkä vuoksi kehitystoiminta vaatii täydellisen tai osittaisen turvallisuuskulttuurin muutoksen, jonka luominen ja läpivieminen vie paljon aikaa. Kokonaisvaltaisen tuotetietovuotojen ennaltaehkäisyohjelman läpivienti on liian laaja kokonaisuus, joten työtehtävieni ohjaamana rajaan aiheekseni tuotetietovuotojen ennaltaehkäisyohjelman luomisen ja jalkauttamisen Nokian yhteistyökumppaniverkostoon. Yhteistyökumppaniverkosto pitää sisällään tuhansia yrityksiä, joilla on tuhansia työntekijöitä käsittelemässä Nokian tuotetietoa. Opinnäytetyössäni pyrin analysoimaan kohdeympäristön perusteellisesti ja toimintatutkimuksen avulla löytämään hyviä menetelmiä tuotetietovuotojen ennaltaehkäisyyn yhteistyökumppaniverkostossa.

3.1 Tulevaisuustietoa tuotetietovuotojen näkökulmasta

Tulevaisuus ei ole ennalta määrättyä eikä varsinaisesti ennustettavissa, mutta on mahdollista muodostaa mielikuvia ja jonkinlaisia käsityksiä siitä, mitä voi olla edessä. Tulevaisuuden ennakointi vaatii tietoa asiantilasta, historiasta, tavoitteista ja kehityssuunnista. Tulevaisuus koostuu erilaisten asioiden välisistä tapahtumista, trendeistä, ilmiöistä ja tulevaisuudenkuvista. Viestintävirasto (2012,3).

Yksi menetelmä tulevaisuuden ennakoimiseksi on skenaarioprosessi, jossa toimintaympäristön muutosvoimia ja epävarmuuksia analysoidaan. Tämä haastaa strategisen ajattelun kun todennäköisesti tapahtuvan selvittämiseksi tutkiaan megamegatrendejä ja nykytilaa. Mahdollisuuksien kartoittamiseksi etsitään heikkoja signaaleja. Skenaariotyöskentely on keino ottaa haltuun erilaisia mahdollisuuksia, vaihtoehtoja ja tulevaisuuden epävarmuutta. Erityisesti tulevaisuustieto on merkityksellistä tälle työskentelytavalle. Täytyy siis määritellä suunta niillä tiedoilla, joita on mahdollista saada vaikuttavista tekijöistä. Loisa (2005, 2).

Megatrendit ovat suuria aaltoja, joilla on tunnistettava suunta. Ne pitävät sisällään myös heikkoja signaaleja ollen tekijä, joka auttaa hahmottamaan tapahtumia ja merkityksiä. Heikot signaalit, joilla ei ole historiaa voivat jälkikäteen katsottuna olla selviöitä, vaikkakin usein merkityksettömiä. Niihin reagointi saattaa aiheuttaa epävarmuutta, mutta oikea-

aikaisesti reagoituna merkityksellisiin heikkoihin signaaleihin saatetaan luoda etulyöntiasema suhteessa kilpailijoihin. Loisa (2005, 12).

3.2 Tuotetietovuotojen tulevaisuus - skenaarioharjoituksen aikana havaittuja trendejä

Soveltavan tehtävän tulevaisuustieto on kerätty seuraavista lähteistä: Viestintävirasto, Tekes, Tampereen Teknillinen Yliopisto, Nokia, Socialwavelenght, Työ-ja Elinkeinoministeriö, Topi-portaali, Lappeenrannan teknillinen yliopisto ja World Economic Forum. Tulevaisuustiedon keräämisen keskiössä oli internet, koska sillä on keskeinen rooli tuotetietovuotojen lisääntymisessä. Megatrendit, trendit ja hiljaiset signaalit on esitetty taulukko-muodossa, koska se selkeyttää niiden läpikäymistä. Alla olevien taulukoiden sisältö on muunnettu yllä olevien lähteiden trenditiedon pohjalta. Sisältö on tuotettu osana tulevaisuuden skenaarioharjoitusta, joka toteutettiin vuonna 2012 Santtu Erkkilän ja Jarmo Puistovirran toimesta.

3.2.1 Megatrendit

Tunnistetut megatrendit tekevät tuotetietovuotojen ennaltaehkäisytyön haasteelliseksi tulevaisuudessa, koska arvokasta tietoa jaetaan teknologian avulla ympärimaailmaa. Ihmiset ovat tottuneet jakamaan elämänsä sosiaalisille verkostoilleen internetin välityksellä. Monilla aloilla, kuten luovalla-alalla on välttämätöntä näyttää työnsä jälki internetissä, saadakseen uusia toimeksiantoja. Tämä saattaa houkutella paljastamaan arvokasta tuotetietoa, esimerkiksi tuotekuvia internetin portfolio-sivustoilla. Internetin laajentunut käyttö on synnyttänyt uudenlaista liiketoimintaa, joka rahoitetaan internet-sivuilla olevilla mainoksilla. Blogit ovat hyvä esimerkki tällaisesta uudesta liiketoiminnasta. Suosittu bloggerit voi ansaita leipänsä, julkaisemalla mielenkiintoista tietoa tai houkuttelevia huhuja. Internet mahdollistaa myös monenlaiset väärinkäytökset ja rikokset.

Megatrendi	Tuotetietovuotonäkökulma
Talouden globalisaatio	Liiketoimintaa harjoitetaan ympäri maailmaa, mikä tarkoittaa, että myös Nokian tuotetietoa käsitellään vaihtelevissa turvallisuuskulttuureissa.
Verkostoituminen	Ihmiset ja yritykset ovat verkostoituneet ympäri maailmaa. Tietoa siirretään suuria määriä realiaikaisesti eri tahojen välillä. Suuri määrä toimijoita ja heikosti suojatut järjestelmät mahdollistavat tietovuotoja.
Työn murros	Uudenlaiset tavat tehdä töitä ja tietynlainen vapaus työnteossa saattavat antaa työntekijöille vääränlaisen turvallisuuden tunteen, mikä taas johtaa turvallisuusepäkohtien syntymiseen.
Teknologinen kehitys	Teknologinen kehitys mahdollistaa arvokkaan tiedon paremman suojauksen. Toisaalta myös suojausten murtamiskeinot kehittyvät samaa tahtia. Teknologinen kehitys on laajentanut tiedonkäsittely pinta-alaa. Nyt arvokasta tietoa säilytetään eri päätelaitteissa ympäri maailmaa.
Kasvottomuus, abstraktisuus	Internetissä voi toimia kasvottomasti, ilman omaa nimeään. Tämä mahdollistaa väärinkäytökset, koska tekijää ei ole helppoa saada vastuuseen teoistaan.
Yhteisöllisyys ja käyttäjien osallistuminen lisääntyvät	Vuodettua tietoa julkaisevat bloggerit ovat perustaneet yhteisöjä ja verkostoja. Osa ihmisistä vuotaa tietoa, koska haluavat näin olla osa jotain yhteisöä.
Globaali etiikka	Globaalisti toimittaessa täytyy huomioida, mikä on oikein ja mikä on väärin missäkin kulttuurissa. Joissakin kulttuureissa ei tunneta salaisuuden käsitettä.
Käyttäytymisen muutos	Ihmisten käyttäyminen on muuttunut intenetin myötä. Käyttäytymiseen ei pystytä vaikuttamaan enää kielloilla, vaan asiat on pystyttävä perustelemaan paremmin.

Taulukko 1. Megatrendejä ja niiden yhteys tuotetietovuotoihin.

3.2.2 Trendit

Havaintojemme pohjalta voidaan todeta, että tuotetietoa jaetaan eri tavoin, sekä sitä tallennetaan useisiin erilaisiin paikkoihin. Monet jako tavat ja tallennuspaikat ovat ilmaisia tai erittäin halpoja, mikä voi myös tarkoittaa heikkoja turvallisuusjärjestelyitä. Ihmiset tykkäävät käyttää mahdollisimman helppokäyttöisiä ja edullisia tietojenkäsittelypalveluita. Heikosti suojatut palvelut lisäävät usein tietoriskin todennäköisyyttä, koska tämä mahdollistaa haavoittuvuuksien hyödyntämisen hakkereiden toimesta. Internetin käyttö on kasvanut merkittävästi Aasiassa. Käyttäjien turvallisuuskoulutusten sisältö ei ole pysynyt mukana tässä kasvussa, mikä tarkoittaa osaltaan sitä, että ihmiset eivät tiedä millaista tietoa on luvallista jakaa esimerkiksi sosiaalisessa mediassa ja mitä taas ei.

Trendi	Tuotetietovuotonäkökulma
Pilvipalvelut	Suuria määriä arvokasta tietoa tallennetaan heikosti suojattuihin pilvipalveluihin.
Koko elämänsä jakaminen sosiaalisessa mediassa	Useat ihmiset jakavat elämänsä verkostoilleen sosiaalisen median välityksellä. Usein myös työhön liittyvää arvokasta tietoa vuodetaan sosiaalisen median välityksellä. Ymmärrys työn ja vapaa-ajan asioiden eroista on hämärtynyt.
Cyber-security ja siihen liittyvät uhat	Cyber-turvallisuudella tarkoitetaan tietojärjestelmiin liittyvien uhkien torjuntaa. Tietomurrot ovat yleisiä.
Älypuhelinten kuvien vuotaminen internettiin	Bloggereita kiinnostavat erityisesti älypuhelinten kuvat. Niitä vuodetaan paljon enemmän, kuin matkapuhelinten kuvia.
Sosiaalisen median hyödyntäminen markkinoinnissa	Sosiaalista mediaa hyödynnetään paljon markkinoinnissa. Huonosti suunnitelluista kampanjoista vuotaa tietoa ulos.
Internetin käytön kasvu Aasiassa	Internetin käytön kasvu Aasiassa näkyy siinä, että vuotojen määrä esim. Kiinassa on kääntynyt kovaan kasvuun. Taustalla on internet-kulttuurin nuoruus Aasian maissa, mikä näkyy pelisääntöjen epäkypsyytenä.

Taulukko 2. Trendejä ja niiden yhteys tuotetietovuotoihin.

3.2.3 Heikot signaalit

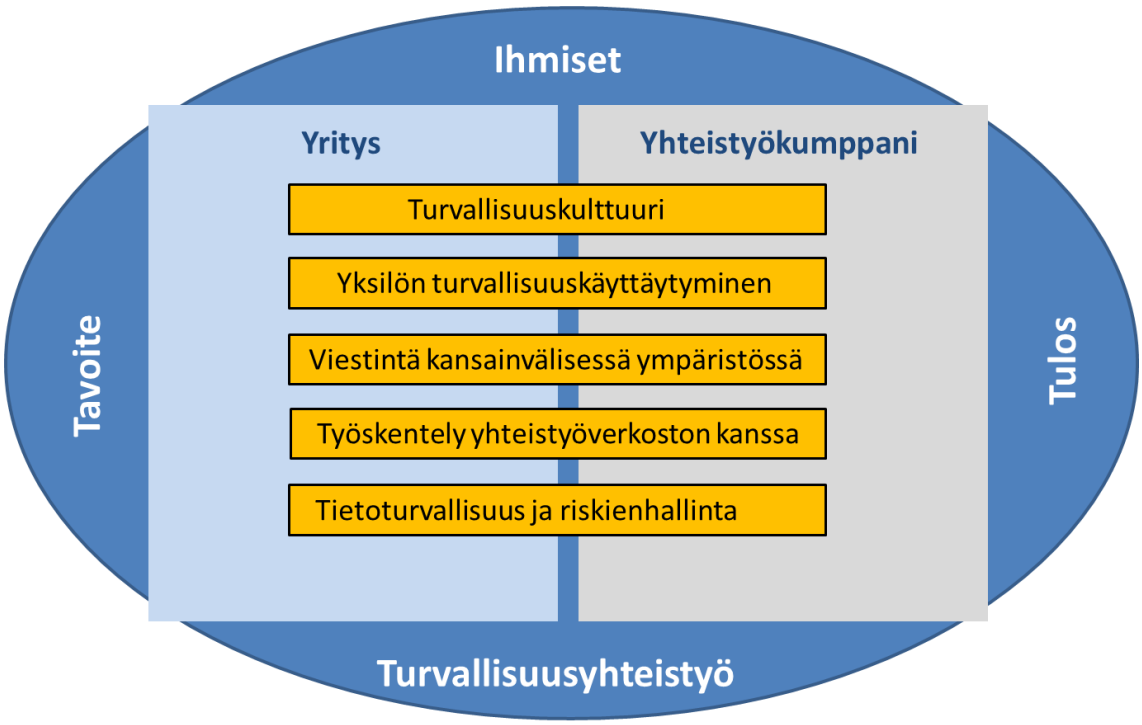
Olemme havainneet useita heikkoja signaaleita, jotka liittyvät Nokian yhteistyökumppaniverkostoon ja tuotetietovuotoihin. Vuototilastoidemme mukaan tuotetietojen määrä on kasvamassa Aasiassa. Olemme havainneet, että perinteisellä, kieltoihin perustuvalla turvallisuusohjeistuksella ei voida vaikuttaa nykyajan ihmisiin, jotka ovat tottuneet vapauteen jakaessaan tietoa internetissä. On ollut mielenkiintoista havainnoida, kuinka osa teknologiabloggereista on ajanut perinteisen median ohi. Tämä näkyy siinä, että bloggerit julkaisevat monesti uutta tietoa, johon sitten perinteinen media puolestaan viittaa tunteja tai jopa päiviä myöhemmin. Tämä puolestaa ohjaa markkinointituloja medialta bloggereille.

Heikko signaali	Tuotetietovuotonäkökulma
Työskentelyolosuhteet ovat heikentyneet Kiinassa, mikä on suututtanut työntekijät	Kiinan heikentyneet työskentelyolosuhteet ovat näkyneet työntekijöiden kapinoina ja epälojaalisuuden kasvuna. Epälojaalit työntekijät haluavat usein vahingoittaa työnantajaansa. Arvokkaan tiedon vuotaminen on oiva keino tähän.
Tuotetietovuotojen määrä kasvaa Aasiassa	Tilastoidemme mukaan vuotojen määrä Aasiassa on kasvanut kovasti ja jatkaa kasvuaan.
Ihmisille maksetaan väärän tiedon levittämisestä (kilpailutekijä)	Tuleviin tuotteisiin liittyvät vääränlaiset huhut vahingoittavat yrityksen imagoa. Kilpailijat saattavat levittää huhuja parantaakseen asemaansa kovasti kilpailluilla markkinoilla.
Bloggereilla enemmän valtaa kuin perinteisellä medialla	Bloggerit saavat usein nopeammin uutta tietoa käsiinsä, kuin perinteinen media. Monilla aloilla bloggerit ovat jo vahvempia, kuin mediatalot.
Uusi sukupolvi ei ymmärrä luottamuksellisuuden käsitettä	Uusi sukupolvi on tottunut kaiken jakamiseen verkostoilleen sosiaalisen median kautta. Heidän on vaikea ymmärtää, että yrityksen arvovasta tietoa ei saa jakaa kavereilleen sosiaalisessa mediassa.

Taulukko 3. Heikkoja signaaleja ja niiden yhteys tuotetietovuotoihin

4 Teoreettinen tausta

Olen rakentanut teoreettisen viitekehykseni siten, että siinä on ihminen keskiössä. Keskeisenä syynä tälle valinnalle ovat olleet syyt tuotetietovuotojen taustalla. Nokian vuototilastojen perusteella voidaan sanoa, että vuodot johtuvat pääsääntöisesti siitä, että ihmiset eivät osaa toimia oikein, ovat huolimattomia tai laiminlyövät ohjeita tietoisesti. Organisaation turvallisuuskulttuurilla on keskeinen asema siinä miten työntekijät kokevat turvallisuuden ja kuinka vastuullisesti he toimivat erilaisissa tilanteissa. Yhteistyökumppaneiden kanssa toimittaessa on tärkeää ymmärtää olevansa tekemisissä erilaisten turvallisuuskulttuureiden kanssa. Yrityksillä on useita erilaisia tapoja kommunikoida turvallisuusvaatimuksensa yhteistyökumppaneille. Usein tämä tapahtuu muodollisesti ja on yleensä osa sopimusneuvotteluvaihetta. Näin toimittaessa yrityksen turvallisuusviesti ei yleensä saavuta niitä ihmisiä, jotka käsittelevät arvokasta tietoa. Kansainvälisesti toimittaessa on mahdollista, että yhteistyökumppani ei edes ymmärrä turvallisuusviestiä, koska sitä suunniteltaessa ei ole ymmärretty toista kulttuuria. Viitekehityksen osana nostetaan esiin potentiaalisia tietoturvallisuuskäytäntöjä, joiden avulla on mahdollista vähentää tuotetietovuotoja sekä parantaa ihmisten turvallisuuskäyttäytymistä.



Kuvio 2: Tutkimuksen teoreettinen viitekehys.

4.1 Tietoturvallisuuteen ja tuotetietovuotojen ennaltaehkäisyyn liittyviä keskeisiä käsitteitä

ISO 27001 (2005, 2) standardin mukaan tietoturvallisuus on tiedon suojaamista ja turvaamista sen kaikissa olomuodoissa. Tieto on arvokasta, kuin mikä tahansa muu yrityksen omistama omaisuus. Tämän vuoksi sen suojaamiseen tulee panostaa riittävällä tavalla. Tietoturvallisuuden merkitys on kasvanut nykyisessä verkottuneessa yhteiskunnassa ja liike-elämässä. Tietoa jaetaan ja käsitellään laajasti sekä monipuolisesti, mikä on osaltaan lisännyt tiedon altistumista erilaisille uhille ja haavoittuvuuksille. Tietoa on erilaisissa fyysisissä ja loogisissa muodoissa, joita kaikkia tulee suojata riittävällä tavalla. Tietoturvallisuus saavutetaan jalkauttamalla kontrolleja, jotka pitävät sisällään muun muassa toimintatapoja, ohjeita ja teknisiä menetelmiä. Tietoturvallisuus voi hyödyttää yrityksiä monin eri tavoin. Yrityksen kilpailukykyä, tuottavuutta, kassavirtaa, yrityskuvaa ja toiminnan lainmukaisuutta voidaan parantaa toimivilla tietoturvallisuusjärjestelyillä. ISO 17799 (2005).

Tietoturvallisuustoiminta käynnistetään tunnistamalla organisaation toimintaan liittyvät turvallisuusvaatimukset. Vaatimukset saadaan kolmesta eri lähteestä. Ensimmäisenä lähteenä on itse organisaation toiminta sekä siihen liittyvät riskit. Toisena lähteenä on yrityksen toimintaan tai toiminta-alueeseen liittyvät säädökset, määräykset ja sopimusvaatimukset. Kolmantena lähteenä on organisaation tietojen käsittelylle määrittämät tavoitteet, esimerkiksi tiedon käytettävyyden muodossa. ISO 17799 (2005).

Seuraavaksi arvioidaan organisaation toimintaan liittyvät riskit, jotta voidaan suunnata turvallisuustoimenpiteet oikeisiin paikkoihin. Kun toimintaan liittyvät vaatimukset ja riskit on selvitetty, on aika valita kontrollit joilla sitten itse tietoa tullaan suojaamaan. Kontrollien valinnan jälkeen ne jalkautetaan erilaisia menetelmiä hyödyntäen. Kontrollien toimivuutta seurataan säännöllisesti ja niitä muutetaan tarpeen vaatiessa. Tietoturvallisuuteen liittyvät uhat ja haavoittuvuudet muuttuvat jatkuvasti, joten on tärkeää, että toiminnan tasoa arvioidaan säännöllisesti. ISO 17799 (2005).

4.1.1 Suojattava kohde

On tärkeää, että organisaatiot määrittelevät ne asiat, jotka ovat elintärkeitä sen toiminnan tavoitteiden saavuttamiseksi. Usein nämä kohteet ovat sellaisia, joiden suojaamiseen halutaan panostaa turvallisuus- ja riskienhallintatoimenpiteillä. Suojattavia kohteita ovat ihmiset omaisuus, tieto, toiminta, maine ja ympäristöstö. Suojattavia kohteita tulee käsitellä sekä organisatorisesta että riskinäkökulmasta. Organisatorisessa näkökulmassa suojattavia kohteita tarkastellaan suhteessa sen toimintoihin, kun taas riskinäkökulmassa suojattavaa kohdetta tarkastellaan siihen liittyvien riskien perusteella. Leppänen (2006, 61–64).

Nokiassa tuotetietovuotojen ennaltaehkäisytyön keskeiset suojattavat arvot ovat omaisuus, tieto ja maine, koska varhaisen vaiheen tuotetiedon tai fyysisten laitteiden vuotaminen voi luoda vääränlaisia mielikuvia potentiaalisten asiakkaiden keskuudessa, mikä puolestaan voi vaikuttaa yrityksen maineeseen. Yhteistyökumppaneille lainataan usein testilaitteita, prototyyppejä ja ohjelmistoja, jotka ovat Nokian omaisuutta. Julkaisematon tuotetieto taas kuuluu tietokategoriaan suojattavista kohteista puhuttaessa. Tietovuodoilla on monenlaisia seurauksia yrityksen maineeseen, koska vuotanut tieto käynnistää huhuja ympäri maailmaa. Nämä huhut perustuvat yleensä puutteelliseen tietoon, mikä yleensä ruokkii vääränlaisia odotuksia markkinoilla. Kun tuote sitten lopulta julkaistaan, niin markkinat saattavat pettyä siihen, koska huhut ovat luoneet vääränlaisen mielikuvan itse tuotteesta. Tämän vuoksi maine on mukana yhtenä kehittämishankkeen suojattava kohteena.

4.1.2 Tuotetieto

Yrityksellä on aineellista ja aineetonta omaisuutta. ISO 27001 (2005, 2). Tuotetieto on yrityksen omaisuutta, joka voi olla aineellisessa tai aineettomassa muodossa. Tuotetiedolla tarkoitetaan esimerkiksi tuotteen uusia ominaisuuksia, uutta teknologiaa, tuotteen ulkoasua, uudistettua käyttäjäkokemusta tai hintaa. Tämä tieto on yleensä sellaista, mitä sen kilpailijoilla ei ole käytettävissään, mikä puolestaan tuo yritykselle kilpailuetua. Luonnollisesti markkinatkaan eivät ole tietoisia tällaisestä tiedosta, kunnes se julkaistaan virallisesti osana uutta tuotetta. Tuotetiedon ennenaikaisella vuotamisella on monenlaisia seurauksia, joista merkittavimmät ovat tulevan tuotteen saama negatiivinen ja huhuihin pahjautuva maine, osittaisen kilpailuedun menetys, sekä markkinointiviestintäkyvyn osittainen menetys.

4.1.3 Luottamuksellisuus

Luottamuksellisuus on tiedon ominaisuus, jolla korostetaan sen arvoa. Tiedon luottamuksellisuuden varmistamisella tarkoitetaan arvokkaan tiedo-omaisuuden suojaamista. Suojaamisella pyritään estämään sen päätymistä väärin käsiin ja tai joutumista vääriin prosesseihin. ISO 27001 (2005, 2).

4.1.4 Kontrolli

Kontrollit ovat lakiin, johtamiseen, hallinnointiin tai tekniikkaan perustuvia suojausmenetelmiä, joilla pyritään hallitsemaan riskejä. Kontrolleja ovat muun muassa erilaiset turvallisuuskäytännöt, ohjeet, politiikat ja tekniset menetelmät. ISO 17799 (2005, 2).

4.1.5 Ennaltaehkäisy

Ennaltaehkäisevällä toiminnalla pyritään pienentämään riskiä ja estämään ei toivottujen tietoturvallisuustapahtumien syntyminen. Ennaltaehkäisevillä toimenpiteillä pyritään vaikuttamaan tietoturvallisuustapahtumien syntymisen syihin. Vahti (2003, 94).

4.1.6 Tietovuoto

Tietoturvallisuustapahtumalla tarkoitetaan havaittua tietoturvallisuusepäkohtaa, jonka syynä voi olla suojaustoimenpiteen pettäminen tai ohjeen laiminlöynti. Tietoturvallisuushäiriö voi pitää sisällään yhden tai useita tietoturvallisuustapahtumia, jotka aiheuttavat vahinkoa yrityksen liiketoiminnalle. ISO 27001 (2005, 5). Tietovuoto on tietoturvallisuushäiriö. Tietovuodolla tarkoitetaan yrityksen omistaman tiedon päätymistä vääriin käsiin ja sitä kautta vuotamista internettiin tai kilpailijalle. Tietovuodoilla on yleensä negatiiviset seuraukset.

4.1.7 Yrityssalaisuus

Rikoslain mukaan yrityssalaisuudella tarkoitetaan liike- tai ammattisalaisuutta taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedot hänelle. (Rikoslaki luku 30, 11 §).

Yrityssalaisuutta voi olla mikä tahansa yrityksen elinkeinotoiminnan kannalta tärkeä tieto, joka halutaan pitää salassa muilta ja erityisesti kilpailijoilta. Yrityksen toiminnan luonne ratkaisee, mitkä ovat yrityksen yrityssalaisuuksia, jotka se käytännössä pitää ja haluaa pitää salassa. Tieto voi olla teknisiä, kaupallis-taloudellisia tai vaikka yrityksen hallintoon ja organisointiin liittyviä. Yrityssalaisuuksia voivat olla esimerkiksi yrityksen osto- ja myyntihinnat, tarjoukset, katteet, sopimukset, tuotekehityksessä syntyvä materiaali, asiakastiedot jne. Tuotetiedot ovat Nokian yrityssalaisuuksia.

4.1.8 Tietoturvallisuustietoisuus

Siposen (2000, 31-41) mukaan tietoturvallisuustietoisuus on tila, jossa organisaation työntekijät ymmärtävät organisaationsa turvallisuustavoitteen. Tietoturvallisuustietoisuus koostuu kahdesta eri tekijästä. Turvallisuustietoisuudella tulee raamit, joiden varaan se rakentuu. Yhtenä esimerkkinä raameista voidaan pitää lainsäändönnöstä tulevia vaatimuksia yrityksen ja sen työntekijöiden toiminnalle. Raamit pitävät sisällään myös tietoturvallisuuden standardin mukaisuuden, sertifioinnin ja mittaamisen. Toinen keskeinen tietoturvallisuustietoisuuden tekijä on sisältö, joka pitää sisällään ihmisten asenteen,

motivaation ja tiedon. Sisältö on näistä kahdesta tekijästä se, joka ottaa huomioon ihmisen tarpeet ja sen miten ihminen oppii ja omaksuu tietoturvallisuusasioita. Siponen (2000, 31-41).

Von Solms (2000, 615-620) puolestaan kirjoittaa, että tietoturvallisuustietoisuus kuuluu tietoturvallisuuden kolmanteen aaltoon, joka kutsutaan vakiintumisen aalloksi. Kaksi muuta aaltoa ovat tekninen aalto ja tietoturvallisuusjohtamisen aalto. Tekninen aalto pitää sisällään tietotekniikkaan liittyvät tietoturvallisuusasiat ja tietoturvallisuusjohtaminen puolestaan sisältää politiikkojen sekä ohjeistusten luomisen. Tietoturvallisuusvastuuhenkilön nimeäminen on osa tietoturvallisuusjohtamista. Tietoturvallisuuden vakiintumisen aallolla hän tarkoittaa tietoturvallisuuskulttuurin rakentamista siten, että siitä tulee olennainen osa organisaation jokaisen työntekijän normaalia toimintaa. Vakiintumisen aalto on kokonaisuus, jossa on hieman teknisestä aallosta tulevia asioita ja paljon sosio-organisatoorisia asioita. Tietoturvallisuustietoisuuden lisääminen olennainen osa organisaation kulttuurin rakentamista. Von Solms (2000, 615-620).

4.2 Riskienhallinta

Vahti (2003, 35) ohjeistuksen mukaan riskienhallinta on järjestelmällistä toimintaa riskien rajoittamiseksi siten, että ne ovat sopivassa suhteessa riskien rajoittamisen kustannuksiin samlla kun organisaation toiminnalleen asettamat tavoitteet voidaan saavuttaa. Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poitamisesta, alentamisesta tai pitämisestä omalla vastuulla sekä riskienhallinnan organisointi. Vahti (2003, 35). ISO 27005 (2008, 3) standardin mukaan tietoturvallisuuteen liittyviä riskejä hallinnoidaan tietoriskienhallinnalla. Tietoriskillä puolestaan tarkoitetaan tietoon kohdistuvaa tai tiedosta johtuvaa riskiä. Vahti (2003, 49). Tietoriskienhallinnalla on keskeinen rooli, mikäli organisaatio haluaa luoda tietoturvallisuuden johtamisjärjestelmän. Sen tulee olla integroituna organisaation kokonaisvaltaiseen riskienhallintaan. ISO 27005 (2008, 3).

4.3 Turvallisuuskulttuuri

Mäkiloukon (2003, 12) mukaan kulttuuri-käsitteen voi näkökulmasta riippuen esittää lukuisilla eri tavoilla. Viestinnällä on suuri vaikutus kulttuuriin, koska kulttuuria opitaan, ylläpidetään ja siihen vaikutetaan vietinnän avulla. Kulttuuri voidaan nähdä osana yksilön persoonallisuutta. Geert Hofsteden (1993, 21.) mukaan kulttuuri on opittua ja se kumpuaa sosiaalisesta ympäristöstä.

Turvallisuuskulttuurikäsite on peräisin työturvallisuudesta, mutta jos sitä katsotaan kokonaisvaltaisempana ilmiönä, pitää se sisällään muun muassa liikenneturvallisuuden,

tietoturvallisuuden, turvallisuusjohtamisen tai vaikkapa väkivaltaisen käyttäytymisen seuraukset tietynlaisissa sosiaalisissa ryhmissä. Tämän vuoksi turvallisuuskulttuuria tulee tarkastella holistisesti. Henkilön turvallisuusasenteet kuvaavat sitä, kuinka hän suhtautuu tiettyyn riskiin ja miten todennäköisenä tai voimakkaana henkilö kokee riskin seuraukset. Käytännössä katsoen jokaisella on omat turvallisuusaseenteensa, jotka vaikuttavat hänen riskinottokykyynsä. Yleensä vastaamme itse omista riskeistämme, mutta ollessamme jonkin ryhmän jäseniä vastaamme riskeistämme myös kyseisen ryhmän muille jäsenille. Tyypillisesti ryhmän jäsen vertailee omia asenteitaan ryhmän riskikäsityksiin. Jos ryhmän käsitykset ovat yhtenevät jäsenen käsitysten kanssa, on tämän suhteellisen helppo muokata omia käsityksiään ryhmän käsitysten mukaisesti. Mikäli käsitykset eivät ole yhtenäiset, jäsen joko vaihtaa ryhmään tai muuttaa käsityksiään. On tärkeää ymmärtää, että asenteet ovat yksilöllisiä ja riskikäsitykset taas sosiaalisia. Turvallisuuskulttuuriin liittyvät asenteet ovat enemmänkin jonkin yhteisön kollektiivisiä käsityksiä riskeistä. Kollektiiviseen käsitykseen vaikuttavat taas useat eri tekijät, kuten arvot, historia, riskikäsitykset, kultturiset käsitykset riskeistä. Leppänen (2006, 185-186).

Leppäsen (2006, 186) mukaan turvallisuuskulttuuri on keskeinen osa organisaatiokulttuuria. Tämä näkyy siinä, kun analysoidaan jonkin organisaation sosiaalisia ryhmiä, niin voimme tehdä päätelmiä turvallisuusasioista. Esimerkiksi yrityksen eri toiminnoista tulevat ihmiset saattavat nähdä turvallisuuden täysin erilailla. Leppänen (2006, 186). Leppänen (2006, 186-187) esittelee teoksessaan kuusi Edgar Scheinin organisaatiokulttuurille antamaa merkitystä. Ihmisten toimivat säännönmukaisesti keskinäisessä kanssakäymisessä. Tämä näkyy kielessä ja rituaaleissa. Normit puolestaan kehittyvät nousevissa ryhmissä. Organisaatioilla on arvot, joissa näkyvämmät ovat hallitsevimpia. Organisaation toimintaa ohjaa perusfilosofia, joka yleensä vaihtelee organisaatioittain. Organisaatiolla on aina jonkinlaiset pelisäännöt, jotka ovat joko kirjoitetut tai kirjoittamattomat. Organisaation sisällä on aina jonkinlainen tunnelma tai ilmapiiri, joka välittyy ulospäin. Leppänen, (2006, 187).

On yleistä, että työntekijöiden oletukset vaaroista eivät ole yhteviä johdon käsityksen kanssa. Johto saattaa nähdä vaarat tilastona, esimiehet taas osana laajempaa kokonaisuutta ja yksittäinen työntekijä pelkää olevansa se, jonka kohdalla jokin riski toteutuu. Ryhmä puolestaan toimii tavalla, joka edesauttaa sen pääsemistä tavoitteisiinsa. Mikäli turvallisuus on ristiriidassa tavoitteiden kanssa, on mahdollista, että ryhmä toimii omien etujensa mukaisesti ja jättää turvallisuussäännöt huomioimatta. Kaikilla tai vain muutamilla ryhmän jäsenillä saattaa olla olettamuksia turvallisuudesta tai pelkoja, mutta se ei kuitenkaan tarkoita, että ryhmän sisällä olisi yhteinen turvallisuuskulttuuri. On tärkeää tutkia ryhmän toimintaa erilaisissa turvallisuuteen liittyvissä asioissa. Tämä auttaa näkemään kuinka ryhmän jäsenet käyttäytyvät erilaisissa turvallisuuteen liittyvissä tilanteissa. Eri ammattiryhmillä on erilaiset käsitykset turvallisuudesta. Esimerkiksi lakimiehet näkevät turvallisuuden lakien ja

säädösten noudattamisen näkökulmasta, kun taas ekonomit pohtivat asioita riskienhallinta ja nimenomaan hyöty näkökulmasta. Leppänen (2006, 187-189).

Leppänen (2006, 190) kirjoittaa Scheinia mukaillen, että organisaationkulttuuriin tasoja voidaan hahmottaa artefaktien, arvojen ja uskomusten avulla. Artefaktit ovat ihmisten rakentamia ja hallinnoimia kokonaisuuksia, kuten toimitilat tai yrityksen sisäinen viestintä. Auktoriteetit eli ketä uskotaan turvallisuusasioissa, kuuluvat artefakteihin. Arvot ovat yhteisiä moraalisia käsityksiä jostakin tavoiteltavasta. Turvallisuuteen liitettäviä arvoja ovat luotettavuus, varmuus, laatu, rehellisyys ja tuloksellisuus. Uskomukset taas ovat yksilöllisesti vaikuttavia asoita, joita henkilöt pitävät yleensä itsestäänselvyyksinä. Leppänen (2006, 190-193).

Martinsin ja Eloffin (2002, 203-214) mukaan tietoturvallisuuskulttuuri on olettamus hyväksyttävästä tietoturvallisuuskäyttäytymisestä. Hyväksyttävällä tietoturvallisuus-käyttäytymisellä he tarkoittavat tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyttämistä, osana yksilön toimintaa. Tietoturvallisuuskulttuuri pitää sisällään organisaatioon, ryhmiin ja yksilöihin liittyviä tekijöitä, jotka on huomioitava, mikäli kulttuuria halutaan mitata. Martins ja Eloff (2002, 203-214). Dhillonin (1997, 210) mukaan turvallisuuskulttuuri on organisaation käyttäytymistä tiedon ja osaamisen suojaamiseen liittyvissä toiminnoissa. Kuusiston ja Ilvosen (2003, 434) mukaan tietoturvallisuuskultuurin rakentemiseen ja kehittymiseen menee paljon aikaa, koska kyseessä on organisaation työntekijöiden käyttäytymisen muuttamista organisaation tavoitteita tukevaan suuntaan. Keskeinen osa kulttuurin rakentamista on sen raamien ja sisällön määrittely. Raamit luovat perustan organisaation tietoturvallisuustoiminnalle, mutta itse sisältö on se, millä vaikutetaan ihmisiin ja heidän käyttäytymiseensä. Kuusisto ja Ilvonen (2003, 434).

4.4 Työskentely yhteistyökumppaniverkoston kanssa

Yhteistyökumppani on henkilö tai organisaatio, joka tarjoaa tuotteita. Yhteistyökumppani voi olla joko sisäinen tai ulkopuolinen organisaatio. Sisäiset tekevät ja tarjoavat tuotteita oman organisationsa sisällä ja ulkoiset yhteistyökumppanit tarjoavat tuotteita muille organisaatioille. ISO 9001 (2008, 3). Työssäni tulen keskittymään ulkoisiin yhteistyökumppaneihin. Yhteistyökumppanit tuottavat, jakavat ja myyvät tuotteita, sekä sekä antavat palveluita ja julkaisevat tietoja.

4.4.1 Yhteistyökumppaniverkoston hallintaprosessi

Wagnerin (2000, 21) mukaan yhteistyökumppaniverkoston hallintaprosessilla tarkoitetaan toimenpiteitä, joiden avulla ylläpidetään suhteita nykyisten ja potentiaalisten

yhteistyökumppaneiden kanssa. Toimenpiteet pitävät sisällään toiminnan suunnittelua, jalkauttamista, kehittämistoimintaa ja valvontaa. Akamp ja Muller (2012, 2) jakavat prosessin seuraaviin vaiheisiin: yhteistyökumppanin valinta ja arviointi, yhteistyökumppanin toiminnan valvonta, yhteistyökumppanin toiminnan kehittäminen ja yhteistyökumppanin integrointi yrityksen prosesseihin. Akampin ja Mullerin (2012, 2) mukaan yhteistyökumppanin suorituskykyyn voidaan vaikuttaa hallintaprosessin eri vaiheita hyödyntämällä. Yhteistyökumppanin suorituskyvyn parantuminen vaikuttaa puolestaan asiakasyrityksen tyytyväisyyteen.

Yhteistyökumppanin valinta on osa toimitusketjun riskienhallintaa, jolla pyritään sellaisen kumppanin valitsemiseen, joka täyttäisi parhaiten ostajan vaatimukset. Valintaprosessiin vaikuttaa ostajan sisäinen ymmärrys yhteistyökumppanilta edellytettävistä vaatimuksista. Keskeisimmät kumppanin valintakriteerit ovat yleensä laatu, hinta ja toimituskyky eli palvelun tai komponenttien saatavuus. Kumppania valittaessa on tärkeää, että ostaja on tietoinen yhteistyökumppanin kotimaahan liittyvistä riskeistä. Ilman perusteellista riskienarviointia on mahdollista, että jokin riski tunnistamaton riski toteutuu ja aiheuttaa samalla merkittävää vahinkoa ostajayrityksen liiketoiminnalle. Akamp ja Muller (2012, 2-3).

Yhteistyökumppanin toiminnan valvonnalla arvioidaan säännöllisesti yhteistyökumppanin kyvykkyyttä toimia ja toimittaa ostavan vaatimusten ja toiveiden edellyttämällä tavalla. Auditointi on tyypillinen valvontamenetelmä. Valvonnalla pyritään keräämään tietoa mahdollisista epäkohdista ja puutteista yhteistyökumppanin prosesseissa, jotta niihin voidaan reagoida nopeasti, ilman että epäkohdista aiheetuu haittaa ostajan liiketoiminnalle. Käytännössä yhteistyökumppanin valintakriteerit ja toiminnan valvontaan käytettävät kriteerit voivat olla samat. Valvontaan kannattaa panostaa erityisesti silloin, kun yhteistyö on vielä nuorta. Pidemmän aikavälin yhteistyössä liian tiukalla valvonnalla saattaa olla vaikutusta kumppanien valiseen luottamussuhteeseen, koska valvonnan kohde saattaa kokea, ettei heihin luoteta. Akamp ja Muller (2012, 3).

Yhteistyökumppanin toiminnan kehittäminen pitää sisällään kaiken sellaisen toiminnan, jolla ostajayritys pyrkii parantamaan kumppanin suorituskykyä tai heidän toimintansa vaatimustenmukaisuutta. Toiminnan kehittäminen voidaan jakaa suoraan ja epäsuoraan toimintaan. Suoralla kehittämistoiminnalla tarkoitetaan sellaista toimintaa, jossa ostaja yritys käyttää joko henkilö tai muita resursseja yhteistyökumppanin suorituskyvyn parantamiseen. Epäsuorassa toiminnassa ostajan käyttämät resurssit ovat paljon rajatummat. Kehittämisestä saatavat potentiaaliset hyödyt parantavat ostajayrityksen liiketoimintaa. Yhteistyökumppanin kehittämiseen kannattaa erityisesti investoida kehittyvillä markkinoilla, joissa toimivien paikallisten yritysten kyvykkyydet ovat usein sellaisella tasolla, että pienelläkin

kehittämistoiminnalla voidaan saada aikaan merkittävää parannusta. Akamp ja Muller (2012, 3).

Yhteistyökumppanin integroimisella ostajayrityksen prosesseihin tarkoitetaan yritysten välisiä yhteisiä toimintoja. Keskeisenä erona kumppanin toiminnan kehittämiseen on se, että tässä toiminnossa molemmat yritykset investoivat yhtä paljon niiden välisiin yhteisiin toimintoihin. Yhteistoiminta tarkoittaa käytännössä yhteisiä prosesseja, yhteisiä tietojärjestelmiä ja organisaatioiden rajat ylittäviä tiimejä. Akamp ja Muller (2012, 3-4).

Akampin ja Mullerin (2012, 5-7) tutkimuksen mukaan yhteistyökumppanin toiminnan valvonnalla ei ole suoraa vaikutusta kumppanin suorituskykyyn. Tutkimus osoittaa kuitenkin, että yhdistämällä valvonnan ja kumppanin toiminnan kehittämisen, voidaan päästä hyviin tuloksiin, koska valvonnalla saadaan löydettyä kehittämisalueita, joihin voidaan vaikuttaa kehittämiseen investoimalla. Tutkimus osoittaa, että kumppanin valinta ja toiminnan arviointi ovat tärkeitä palasia yhteistyökumppaniverkoston hallintaprosessissa. On tärkeää muistaa, että niiden ei pidä ajatella olevan yksittäisiä palasia, vaan osa kokonaisuutta. Tutkimuksen mukaan yhteistyökumppanin suorituskykyyn voidaan parhaiten vaikuttaa kumppanin toimintaa kehittämällä ja yhteisillä prosesseilla sekä muulla yhteistoiminnalla. Akamp ja Muller (2012, 5-7).

4.4.2 Yhteistyökumppaniverkoston hallinnointitavat

Li, Xie, Teo ja Peng (2010, 333) nostavat tutkimuksessaan esiin kaksi erilaista tapaa hallinnoida yhteistyökumppaneita. Nämä tavat ovat muodollinen ja sosiaalinen. Muodollinen hallinnoitatapa pohjautuu sopimuksiin ja niiden pilkuntarkkaan sisältöön. Käytännössä yhteistyökumppania hallinnoidaan ja ohjataan sopimuksen sisällöllä. Sosiaalinen hallinnointitapa on epämuodollisempi ja se perustuu ihmissuhteisiin. Käytännössä katsoen sosiaalisella hallinnointitavalla tärkeitäkin asioita ja muutoksia voidaan viedä eteenpäin, ilman että niitä on määritelty sopimuksessa. Li ym. (2010, 333-334). Li:n ym. (2010, 334) mukaan muodollinen hallinnointitapa ohjaa yrityksiä tekemään vain sen, mitä sopimuksessa on määritelty. Kovinkaan usein sopimus ei mahdollista omia tulkintoja tai luovuutta jonkin uuden ongelmanratkaisussa. Sosiaalisen hallinnointitavan perustana on luottamus osapuolten välillä. Luottamuksella tarkoitetaan sitä, että osapuolet eivät halua hyödyntää toisessa havaitsemiaan haavoittuvuuksia. Ongelmanratkaisussa puolestaan korostuu yhteistyö eli pyritään ratkaisemaan haastavat ongelmat yhdessä ja luonnollisesti nostamaan esiin haastavatkin asiat. Sosiaalinen hallinnointitapa lisää yleensä yhteistyön joustavuutta ja tehostaa osapuolten välistä kanssakäymistä, koska haastavistakin asioista voidaan puhua avoimesti, mikä mahdollistaa nopeamman ongelmanratkaisun. Li ym. (2010, 335-342).

On tärkeää, että yritykset analysoivat perusteellisesti, että millaisella tavalla he ryhtyvät hallinnoimaan yhteistyökumppaneitaan. Molemmissa tavoissa on hyviä ja huonoja puolia. On tärkeää olla olemassa sopimus, joka määrittää liikesuhteen raamit. Toisaalta liian tiukka sopimus saattaa tehdä toiminnasta muodollista ja jopa tehotonta. On myös mahdollista, että osapuolet eivät halua keskustella haastavista asioista, koska pelkäävät sopimusrikkomusta. Sosiaalinen hallinnointitapa puolestaan lähentää osapuolia ja saa aikaan luottamuksen ilmapiirin. Toisaalta liiallinen luottamus toiseen osapuoleen voi mahdollistaa luottamusaseman väärinkäyttämisen. Hallinnointitapa kannattaa määrittää tilanteen mukaan ja se kannattaa rakentaa siten, että siinä hyödynnetään molempia hallinnointitapoja. Li ym. (2010, 335-342).

4.4.3 Yhteistyökumppaniverkoston tietoturvallisuuden hallinta

Helmsin, Ettkinin ja Morrisin (2000, 10) mukaan yhteistyökumppanit ja niiden toiminta ovat merkittävä uhka yrityksen tieto-omaisuudelle. Helms ym. (2000, 10) nostavat esiin useita menetelmiä, joilla heidän esiin nostamaansa uhkaa voidaan torjua. Yrityksen tulisi pyrkiä toimimaan sellaisten yhteistyökumppaneiden kanssa, jotka eivät toimi liian tiiviissä yhteistyössä yrityksen kilpailijoiden kanssa. Yhteistyökumppaneiden pääsyä tietoon tulisi rajoittaa siten, että ne näkisivät vain yhteistyön kannalta oleellisen tiedon. On tärkeää, että yrityksellä on voimassaolevat sopimukset sen yhteistyökumppaneiden kanssa. Sopimusten tulee sisältää salassapito- ja luottamuksellisuuspykälät. Yhteistyökumppaneiden turvallisuuskyvykkyys tulee auditoida säännöllisesti, Auditoinnin uskotaan syventävän yritysten välistä yhteistyötä. Yrityksen tulee määrittää, ne yksiköt, henkilöt ja roolit, joilla on oikeus kommunikoida yhteistyökumppaneiden kanssa. Helms ym.(2000, 10).

Davisin (2010, 13) mukaan suurilla kansainvälisillä yrityksillä on usein satoja ja jopa muutamia tuhansia yhteistyökumppaneita, joiden kanssa ne joutuvat jakamaan arvokasta tietoa. Yritysten on haasteellista hallinnoida näin laajaa yhteistyökumppaniverkostoa. Erityisen haastellista on tietää, että millä kumppanilla on pääsy minkäkinlaiseen tietoon sekä millaiseen tietoon heidän oikeasti tulisi päästä käsiksi. Tarpeiden ja todellisuuden välissä on usein suuria aukkoja, jotka mahdollistavat turvallisuusepäkohtien synnyn. Monet yritykset panostavat usein auditointeihin, osana yhteistyökumppaniverkoston tietoturvallisuuden hallintaa. Auditointi antaa yhden otoksen yhteistyökumppanin turvallisuustasosta, eikä näin ollen riitä kokonaisvaltaisesti turvaamaan yrityksen etuja. Yritysten tulisi panostaa merkittävimpiin yhteistyökumppaneihin ja toimivan turvallisuusyhteistyön rakentamiseen niiden kanssa. Davis (2010, 13).

ISF:n (2013, 1-11) selvityksen mukaan arvokkaan tiedon jakaminen yhteistyökumppaneiden kanssa on osa nykypäivän liiketoimintaa. Tämä toiminta kasvattaa tietoriskin toteutumisen

todennäköisyyttä. Yhteistyökumppaniverkostoja on vaikea turvata, koska yrityksillä ei ole kunnon näkyvyyttä, miten yhteistyökumppanit hoitavat turvallisuusasioita. Verkostot ovat myös usein niin laajoja, ettei yrityksillä riitä resursseja niiden turvallisuus tason arviointiin ja parantamiseen. Tämän vuoksi monet organisaatiot keskittyvät riskienhallintaa sopimuksiin liittyvillä muodollisilla kontrolleilla ja tässäkin toiminnassa painopiste on suurissa yhteistyökumppaneissa. Tällaisella toimintamallilla saattavat korkeimmat riskitason pienet yhteistyökumppanit jäädä vähemmälle huomiolle, mikä saattaa osaltaan vaikuttaa riskin toteutumiseen. Uutena haasteena ovat yhteistyökumppaneiden alihankkijat, jotka saavat yleensä käsiinsä yrityksen arvokasta tietoa. Näiden hallinta turvallisuusmielessä on äärimmäisen haastavaa, koska ne ovat niin syvällä toimitusketjussa. Mikäli yrityksellä on haasteita hallinnoida turvallisuusasioita yhteistyökumppaninsa kanssa, niin on mahdotonta kuvitella sen pystyvän ulottamaan turvallisuustoimenteensä kumppanin alihankkijoille. ISF (2013, 1-11).

ISF:n (2013, 1-11) yritysten tulisi ensin arvioida yhteistyössä jaettavan tiedon arvo ja suojaustarve, jonka avulla yhteistyökumppanit voitaisiin priorisoida. Tämä auttaisi kohdistamaan turvallisuustoimenpiteet oikeisiin paikkoihin. ISF (2013, 1-11) on luonut prosessin jonka avulla yritys voi ryhtyä hallinnoimaan yhteistyökumppaneihin liittyviä turvallisuusasioita. Ensimmäiseksi yritykseen tulee määritellä yhteistyökumppaneille jalkautettavat turvallisuusvaatimukset. Tämän jälkeen pyritään liiketoimintanäkökulmasta löytämään sopivia kumppaniehdokkaita, joille lähetetään tarjouspyyntö, sisältäen yrityksen turvallisuusvaatimukset. Seuraavassa vaiheessa valitaan ehdokkaista sopivin yhteistyökumppani ja neuvotellaan sopimus. Sopimusneuvotteluissa on tärkeää käydä myös turvallisuusvaatimukset läpi, jotka yhteistyökumppani ymmärtää, mihin se käytännössä sitoutuu. Yhteistyötä käynnistäessä aloitetaan seurantatoimenpiteet, joilla pyritään varmistamaan, että yhteistyökumppanin turvallisuustaso on riittävä. Seurantatoimenpitee tulisi kirjata tietokantaan, jotta voidaan varmistaa toiminnan jatkuva kehittäminen sekä kyvykkyys raportoida kumppanin kyvykkyyden nykytila yrityksen johdolle. Prosessin viimeisenä vaiheena on yhteistyösuhteen hallittu purkaminen. ISF (2013, 3-11).

ISO/IEC 17799:2005 (2005, 14) mukaan on tärkeää arvioida yhteistyöhön liittyvät riskit, ennen kuin yhteistyökumppanille annetaan pääsyoikeutta yrityksen tietoon. Riskiarvioinnissa selvitetään, millaiseen tietoon ja tiedon prosessointitiloihin yhteistyökumppanin tulee saada pääsyoikeus. Osana arviointia selvitetään, miten yhteistyökumppani tulee käsittelemään arvokasta tietoa. Yhteistyössä jaettavan tiedon arvo, luottamuksellisuusaste ja sen liiketoimintakriittisyys tullaan arvioimaan. Arvioinnissa selvitetään kuinka hyvin nykyiset kontrollit pystyvät suojaamaan sellaista arvokasta tietoa, johon tulevalla yhteistyökumppanilla ei tule olemaan pääsyoikeutta. Riskiarvioinnissa selvitetään, ketkä yhteistyökumppanin työntekijät tulevat työnsä puolesta tarvitsemaan pääsyoikeuden yrityksen

tietoon. Keskeisenä osana riskearviointia on tärkeä selvittää yhteistyökumppanin kyvykkyys suojata yrityksen tietoa, käsitellessään sitä eri tavoin. Myös yhteistyökumppanin kyvykkyys reagoida tietoturvallisuusngelmiin ja yhteistyöhön liittyvien mahdollisten lainsäädäntövaatimusten esiintyminen selvitetään osana arviointia. Riskiarvioinnin jälkeen valitaan sellaiset tietoturvallisuuskontrollit, joiden avulla saadaan pienennettyä yhteistyökumppaneihin liittyviä turvallisuusriskejä. Yhteistyökumppanille ei anneta pääsyoikeutta yrityksen tietoon, ennen kuin vaaditut tietoturvallisuuskontrollit on jalkautettu ja yhteistyökumppani on osoittanut ymmärtävänsä heiltä edellytetyt turvallisuustoimenpiteet ja vaatimukset. ISO/IEC 17799:2005 (2005, 14-15). ISO/IEC 17799:2005 (2005, 16-18) standardissa korostetaan, että yhteistyöhön liittyvät turvallisuusasiat tulee kirjoittaa vaatimuksiksi ja liittää osaksi yrityksen ja yhteistyökumppanin välistä sopimusta.

4.4.4 Tietoturvallisuushaasteita pienissä ja keskisuurissa yrityksissä

Useat Nokian yhteistyökumppanit kuuluvat kokoluokaltaan pieniin ja keskisuuriin yritykseen, joten osana teoriakatsausta on hyödyllistä tutustua aiheeseen liittyvään tutkimustietoon. Ebrun, Gizemin, Serpilin ja Nuranin (2010, 361) tutkimuksessa käsitellään tietoturvallisuutta kokonaisuutena, mikä pitää sisällään kaikki tietoturvallisuuden osa-alueet. Nämä osa-alueet olivat samat joita oli käytetty vuonna 2005 tehdyssä Etelä-Afrikkalaisessa pieniin ja keskisuuriin yrityksiin kohdistetussa tietoturvallisuustutkimuksessa. Osa-alueet olivat seuraavat: hallinnollinen tietoturvallisuus, tietoaineistoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, käyttöturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus ja liiketoiminnan jatkuvuus. (Ebru ym. 2010, 361-363) Aikaisemmin samanlaisessa tutkimuksessa käytettyjen kysymysten hyödyntäminen auttaa tutkimuksen tavoitteeseen pääsemiseen, koska vertailukyky muissa maissa tehtyihin tutkimuksiin paranee. Tietoturvallisuus on laaja kokonaisuus, mutta keskittyminen vain johonkin osa-alueeseen ei antaisi kunnollista kuvaa turkkilaisten pienten ja keskisuurten yritysten tietoturvajärjestelyiden nykytilasta. Tutkimukseen osallistuvat yritykset tulivat Bursan kaupungista, jossa myös tutkimusryhmän yliopisto sijaitsee. Kohderyhmän valinnassa ei ole rajattu mitään toimialaa pois, vaan kaikki ovat olleet samassa asemassa. Tutkimuksen tavoitteena ei ole ollut selvittää, että onko tietoturvallisuuskyvykkyydellä ja yrityksen toimialalla jokin yhteys keskenään. (Ebru ym. 2010, 361). Näkisin, että tämä oppi on otettu esimerkkinä olleesta Etelä-Afrikkalaistutkimuksesta ja muista samantyyppistä kansainvälisistä tutkimuksista.

Tutkimuksen taustalla ovat kolme aikaisempaa tutkimusta. Deloitten vuonna 2006 tekemä tietoturvallisuustutkimus antoi alkusysäyksen turkkilaiselle tutkimukselle. Turkissa on tutkittu yritysten tekemien tietotekniikka- ja turvallisuusinvestointien kokonaismäärää vuosina 2005-2006. Tutkimuksessa on havaittu merkittävää kasvua yritysten tietotekniikka-ja

turvallisuusinvestoinneissa.(Ebru ym. 2010, 363). Näkisin, että Ebru ym. ovat tutkimuksellaan halunneet myös selvittää, näkyvätkö investoinnit pienten ja keskisuurten yritysten tietoturvallisuusjärjestelyissä vai ovatko turvallisuusinvestoinnit kohdistuneet suuriin yrityksiin tai muihin turvallisuuden osa-alueisiin. Kolmas vaikuttava tutkimus on Etelä-Afrikassa vuonna 2005 toteutettu tietoturvallisuustutkimus, jonka aineistoa Ebru ym. hyödyntävät tutkimuksessaan. Tutkimustulosten kansainvälisessä vertailussa hyödynnetään Etelä-Afrikkalaista tutkimusta, Ernst & Youngin tietoturvatutkimusta, PricewaterhouseCoopersin tutkimusta ja Ponemon instituutin tutkimusta. (Ebru ym. 2010, 361-365). Ebrun ym. tekemä tutkimus pohjautuu olemassa oleviin vastaaviin tutkimuksiin, joista noin puolet on konsulttiyritysten tekemiä.

Kaikki tutkimukseen osallistuivat yritykset käyttivät internettiä ja sähköpostia, mutta vain puolella yrityksistä oli oma sisäverkko. Laajempi tietotekniikan ja internetin hyödyntäminen, kuten sähköinen kaupankäynti olivat osa vain muutaman yrityksen toimintaa. 85% yrityksistä oli määritellyt tietoturvallisuuteen liittyvät vastuut. 77%:lla yrityksistä oli olemassa tietoturvallisuuspolitiikka ja 70% yrityksissä sen sisältö oli kommunikoitu työntekijöille. Vain 48% kyselyyn osallistuneiden työntekijöistä oli osallistunut tietoturvallisuuskoulutukseen. Tutkimuksessa kävi myös ilmi, että suurin osa yrityksistä ei saanut tai ei osannut hakea riittävää tietoturvallisuuskonsultaatiota yrityksen sisältä tai ulkoa. Mielenkiintoisena seikkana nousi esiin fyysiseenturvallisuuteen panostamisen vähyys. 62% yrityksistä oli tietoinen kansainvälisistä tietoturvallisuusstandardeista, mutta vain harvat hyödynsivät niitä käytännössä. Suurimpana tietoturvallisuusuhkana pidettiin ihmisten huolimattomuutta. 81% tutkimukseen osallistuneista yrityksistä koki, että tietoturvallisuus on tärkeää, ja että siihen tulee panostaa. (Ebru ym. 2010, 363-364).

Turkkilaisen tutkimuksen toisena tavoitteena oli vertailla kyselytutkimuksen tuloksia muiden maiden vastaaviin tutkimuksiin. Tukkilaisten ja etelä-afrikkalaisten yritysten vertailussa Turkki veti pidemmän korren. Turkkilaisissa yrityksissä on panostettu enemmän käytännön tietoturvallisuusjärjestelyihin. Etelä-Afrikassa näkyi selvästi osaavien ihmisten puute. Ernst & Youngin tietoturvallisuustutkimuksen tulokset olivat melkoisen samansuuntaiset turkkilaisen tutkimuksen kanssa. (Ebru ym. 2010, 364) Todennäköisesti tästä johtuen tutkimuksien eroavaisuuksia ei ole tuotu esiin. Ebrun ym. (2010, 364) tutkimuksessa on vertailtu turkkilaisten yritysten tuloksia Iso-Britanniassa toimivien yritysten tuloksiin. Kyseisen vertailun aikana tutkimusryhmä huomasi, että maan taloudellisella tilanteella ja koulutusjärjestelmällä on vaikutusta tutkimuksen tuloksiin. He nostavat esiin, että jatkotutkimuksissa tämä tulee huomioida kysymyksiä määriteltäessä. Vertailussa nähtiin, että Iso-Britanniassa toimivien yritysten tietoturvallisuusjärjestelyt olivat kaikilla mittareilla mitattuna selkeästi edellä turkkilaisia yrityksiä. Tähän vaikuttivat erityisesti maan taloudellinen tilanne ja koulutuksen taso. (Ebru ym. 2010, 364-365)

Ebrun ym. (2010, 365) mukaan pienet ja keskisuuret yritykset elävät siinä uskossa, että tietoturvallisuuspolitiikka ratkaisee kaikki haasteet. Politiikat ovat paikoillaan, mutta ne eivät huomioi tietoturvallisuutta kokonaisuutena. Vastuu on monesti annettu henkilölle, jolla ei ole osaamista selviytyä vastuustaan. Tutkimusryhmä korostaa tietoturvallisuusosaajan rektytoimista tai osaamisen ostamista yrityksen ulkopuolelta. Kansainväliset standardit voisivat antaa lisäarvoa yritysten tietoturvallisuustasojen harmonisoinnissa ja parantamisessa. Johtopäätöksissä korostetaan, että pelkkä tietoturvallisuusjärjestelyiden jalkauttaminen ei riitä, vaan kyvykkyyttä tulee säännöllisesti testata ja seurata erilaisilla menetelmillä (Ebru ym. 2010, 365).

Kuusisto ja Ilvonen (2003, 434) tekivät vastaavanlaisen tutkimuksen Tampereen seudulla, jossa selvitettiin 11 pienen ja keskisuuren yrityksen tietoturvallisuusjärjestelyitä. Tutkimuksessa tietoturvallisuutta mitattiin kolmesta eri näkökulmasta; tekninen, tietoturvallisuusjohtaminen ja tietoturvallisuustietoisuuden lisääminen. Tutkimuksessa kävi ilmi, että pienten ja keskisuurten yritysten tietoturvapanostukset oli pääsääntöisesti suunnattu teknologiaan. Yrityksillä oli olemassa hyvät varmuuskopiointi, virustorjunta ja tietoliikenneturvallisuuskäytännöt. Tietoturvallisuusjohtamisen tasoa tutkiessaan Kuusisto ja Ilvonen (2003, 434-435) havaitsivat, että yritysten välillä alkoi näkymään selkeitä eroja. Vain kolmasosassa yrityksissä oli olemassa tietoturvallisuuspolitiikka, jossa määriteltiin yrityksen johdon tahtotila. Suurimmasta osasta yrityksiä ei myöskään ollut tietoturvallisuusvastaavaa tai turvallisuusvastaavaa, jonka tehtäviin olisi kuulunut yritysten tietoturvallisuustason ylläpitäminen ja kehittäminen. Syinä näille puutteille olivat yritysten pieni koko. Pienissä yrityksissä ei nähty järkeväksi kirjoittaa toimintatapoja ja ohjeita, koska niiden työntekijämäärät olivat niin pieniä. Tietoturvallisuus oli pääsääntöisesti organisoitu niin, että tietojärjestelmistä vastaava henkilö oli vastuussa tietoturvallisuudesta. Tosin suurimmassa osassa yrityksistä kyseinen henkilö hoiti tietoturvallisuutta pelkästään teknisestä näkökulmasta. Kuusisto ja Ilvonen (2003, 434-435).

Kuusiston ja Ilvosen (2003, 436-437) tutkimuksen mukaan tutkimuksen kohteena olleissa pienissä ja keskisuurissa yrityksissä ei panostettu tietoturvallisuustietoisuuden lisäämiseen. Syynä koulutuksen puutteeseen oli jälleen yritysten pieni koko ja työntekijöiden vähyys. Tutkimuksessa kävi kuitenkin ilmi, että yritykset jäjestivät perehdytystä uusille työtekijöilleen, mutta nämä tilaisuudet eivät sisältäneet tietoturvallisuusperehdytystä, koska yrityksillä ei ollut aiheeseen liittyvää politiikkaa tai ohjeistuksia. Kaksi yritystä oli lisännyt tietoturvallisuustietoiskuja osaksi muita yrityksen muita koulutustilaisuuksia. Kuusisto ja Ilvonen (2003, 436-437).

4.5 Yksilön turvallisuuskäyttäytyminen

Porvarin (2012, 135) mukaan yhä merkittävämpi osa nykypäivän turvallisuuden haasteista liittyy inhimillisiin ja organisatorisiin näkökohtiin. Organisatorisiin tekijöihin kuuluvat liiketoiminnnan ja turvallisuuden johtaminen. Inhimilliset näkökohdat pitävät sisällään henkilökunnan osallistumisen merkityksen, turvallisuuden psykologiaa, tietoturvallisuustietoisuutta sekä turvallisuuskäyttäytymistä ja sen parantamista. Porvari (2012, 135). Kraemerin, Carayonin ja Clemmin (2009, 509-520) mukaan inhimillisten ja organisatoristen tekijöiden käsitteiden kehittäminen on alkutekijöissään. Näitä tekijöitä ei ole tutkittu tarpeeksi, jotta voitaisiin selkeästi sanoa, miten ne aiheuttavat haavoittuvuuksia. On kuitenkin olemassa tekijoitä, jotka voivat vaikuttaa haavoittuvuuksiin. Nämä tekijät voidaan luokitella yhdeksään alueeseen: ulkoiset virheet, inhimilliset virheet, johtaminen, tietoturvallisuuden organisaatio, suorituskyvyn sekä voimavarojen hallinta, tietoturvapolitiikka, resurssien hallinta, teknologia ja koulutus. Kraemer ym. (2009, 509-520). Kraemer ym. (2009, 509-520) korostaa, että tietoturvallisuuden haavoittuvuuksien hallintaan tarvitaan monipuolinen, useita osa-alueita sisältävä menetelmä, jonka avulla voidaan parantaa suorituskykyä. Porvarin mukaan (2012, 140-141) osallistamisella on keskeinen rooli työntekijöiden tietoturvallisuuskäyttäytymistä ja tietoisuutta parannettaessa. Osallistamisella tarkoitetaan henkilökunnan mielipiteiden huomioimista tietoturvallisuusohjeita luotaessa ja jalkautettaessa.

4.5.1 Tietoturvallisuuskäyttäytyminen

Tietoturvallisuuskäyttäytymistä on tutkittu melko paljon viime vuosina. Karjalaisen (2011) mukaan työntekijät laiminlyövät organisaation tietoturvallisuuskäytäntöjä. Karjalainen on tutkinut aihetta induktiivisen ja laadullisen tutkimusmenetelmän avulla. Hän korostaa tutkimuksessaan, että merkittävä osa tietoturvallisuudesta on ihmisten toimintaa. Puhakainen (2006) korostaa tutkimuksissaan, että parhaatkin tekniset ratkaisut ovat kierrettävissä ihmisten toimesta. Ihmiset kiertävät ohjeita ja ratkaisuita, joko tahallaan tai tahattomasti. Ihmisen motivaatiolla on keskeisen sija siinä, noudattaako henkilö yhteisesti sovittuja toimintatapoja ja ohjeistuksia. Syitä heikkoon tietoturvallisuustietoisuuden tasoon ovat muun muassa puutteellinen koulutusmateriaali, johdon huono sitoutuminen ja henkilöstön heikko motivointi. Puhakainen (2006).

Porvarin (2012, 152) mukaan tietoturvallisuuspelisääntöjen tuntemus sekä optimaaliset tiedot, taidot ja motivaatio ohjeiden noudattamiseen ovat hyvän tietoturvallisuuden tärkein tekijä. Puhakainen (2006) on rakentanut kolme teoriaa ihmisten tietoturvallisuuskäyttäytymisen muuttamiseksi. Koulutuksen avulla voidaan lisätä henkilön tietoturvallisuustietoisuutta ja samalla vaikuttaa tämän käyttäytymiseen.

Markkinointiviestinnällä tarkoitetaan sitä, että tietoturvallisuusasiat tulee saattaa näkyviksi koko henkilökunnalle. On tärkeää, että ihmiset näkevät millaisia tietoturvavahinkoja oikeasti tapahtuu ja millaisia seurauksia niillä on. Markkinointiviestintää voi harjoittaa erilaisissa tilanteissa ja sitä voi välittää erilaisilla menetelmillä. Tietoturvallisuusviestiä voi liittää osaksi yrityksen yleisiä koulutuksia tai tilaisuuksia. Viestiä voidaan myös jalkauttaa esimerkiksi julisteilla, sähköpostiviesteillä ja artikkeleilla. Esimiehillä on suuri vaikutus ihmisten motivaatioon noudattaa tietoturvallisuusohjeita. On tärkeää, että henkilökunnan tietoturvallisuuskäyttäymistä seurataan esimiesten toimesta. Esimiesten reagoida välittömästi kaikkiin laiminlyönteihin ohjaavalla palautteella. Työntekijöille on tärkeätä saada jatkuvaa palautetta, joka puolestaan auttaa heitä ymmärtämään yrityksen edellyttävän tietoturvallisuustason. Puhakainen (2006).

Porvarin (2012, 159) mukaan yrityksen johdon näkemyksillä ja toiminnalla on suuri merkitys henkilönkunnan tietoturvallisuustietoisuuteen, taitoihin, asenteisiin ja motivaatioon. Inhimilliset ja organisatoriset tekijät vaikuttavat osaltaan haavoittuvuuksiin. Porvari (2012, 159) korostaa, että turvallisuusihmisten ja käyttäjien välillä saattaa olla melkoisia ristiriitoja, joiden taustalla on useita erovaisuuksia. Esimerkkinä nostetaan esiin taito, tietämys ja henkilökohtaiset suhteet. Ihmisten riskikäsityksellä on suuri merkitys sille, miten he käyttäytyvät eri tilanteissa. Porvarin (2012, 159) mukaan yrityksen tietoturvallisuuskulttuuri kehittyy henkilökunnan käyttäymisen johdosta. Tietoturvapelisääntöjen ja käyttäytymisen välinen vuorovaikutus vaikuttaa keskeisesti organisaation tietoturvallisuuskulttuuriin. Osallistavalla vuorovaikutuksella voidaan päästä merkittäviin tietoturvallisuuskulttuuria parantaviin tuloksiin. Porvari (2012, 159).

4.5.2 Yksilöihin liittyviä viestintähaasteita ja rajoituksia

Sussmanin (2008, 332) mukaan viestintärajoituksilla sekä salassapitopykälillä tarkoitetaan sääntöjä, sopimuksia ja toimintatapoja, joiden tarkoituksena on estää arvokkaan tiedon valuminen organisaation ulkopuolelle sen työntekijöiden toimesta. Rajoitusten tarkoituksena on suojata arvokasta tietoa, siten etteivät yrityksen ihmiset, tuotteet, käytännöt, liikesuhteet joudu vaaraan. Osa rajoituksista tulee suoraan paikallisista lainsäädännöistä. Augustinen (1995, 152) mukaan salaisuuksia voidaan pitää, jos tietoa jaetaan vain muutamille luotetuille ihmisille. Näiden henkilöiden tulee allekirjoittaa erillinen salassapitosopimus, jotta he ymmärtäisivät hallussaan olevan tiedon arvon. Augustine (1995, 152) korostaa myös, että tietoa voi pitää salaisena liian kauaa, koska ihmiset pystyvät pitämään salaisuuden vain rajoitetun ajan.

Sussmanin (2008, 333) mukaan jokaisessa organisaatiossa on työntekijöitä, jotka rikkovat sääntöjä ja vuotavat tietoja. Näihin henkilöihin ei voida vaikuttaa rajoituksilla ja politiikoilla,

koska motivaatio ohjaa heitä toimimaan sääntöjen vastaisesti. Pääsääntöisesti kuitenkin sääntöjä rikkovat tyäntekijät ovat vähemmistönä, koska suurin osa ihmisistä haluaa toimia oikein. Suurimmassa osassa tapauksista vuotojen taustalla ovat rehelliset työntekijät, joita ohjaavat järkisyyt ja sosiaalisen vuorovaikutuksen tarpeet. Ihmisillä on tarve luoda yhteys muihin ihmisiin. Tämä yhteys luodaa viestimällä eri tavoilla, kuten puhumalla, kirjoittamalla pikaviestimiin tai jakamalla tietoa sosiaalisessa mediassa. Tietoa ei yleensä vuoda ulos, silloin kuin viestintä pysyy muodollisella tasolla, mutta kun mennään henkilökohtaisemmalle tasolle, niin luottamuksellisen tiedon vuotamisen riski kasvaa. Tämä johtuu siitä, että ihmiset haluavat jakaa arvokkaita asioita läheisiksi kokemiensa ihmisten kanssa. Sussmanin (2008, 333-334) mukaan työntekijöille on erityiseen vaikea olla jakamatta salaisuuksia perheensä ja läheisten ystäviensä kanssa. Sussmanin (2008, 335) mukaan suurin osa nykyisistä tietovuodoista johtuu siitä, että positiivinen sosiaalinen paine ohjaa ihmistä toimimaan sääntöjen vastaisesti.

Sussman (2008, 334) korostaa, että työntekijät eivät pidä käskyistä ja määräyksistä. Työntekijät eivät välttämättä tottele määräyksiä, jos heille ei kommunikoida miksi, jostain asiasta ei saa puhua tai miksi jotain tietoa ei voi jakaa läheisilleen. Määräykset saavat ihmiset kokemaan, ettei yrityksen johto luota heihin ja heidän arvostelukykyynsä. Työntekijät saattavat myös helposti kuvitella, että heidän tekemisiään valvotaan yrityksen johdon toimista. Tällainen vaikuttaa yleensä negatiivisesti työntekijöiden motivaatioon, mikä puolestaan johtaa tietoturvallisuuskäyttäytymisen heikentymiseen. Yrityksen johdon tulisi myös välttää ihmisten pelottelua, salassapitotavoitteita kommunikoidessaan. Sussman (2008, 334).

Ihmisillä on halu ja tarve nostaa itseään esiin, mikä tarkoittaa omista näkökulmista viestimistä ympäröivälle maailmalle. Ihmiset kokevat, että heillä on valtuus jakaa tietoa muille. Tämä puolestaan on usein konfliktissa yrityksen tietoturvallisuusohjeiden kanssa, koska yritys ei luonnollisti halua, että sen arvokasta tietoa tai muita sisäisiä asioita kommunikoidaan esimerkiksi sosiaalisen median välityksellä. Muun muassa Youtuben ja Facebookin menestys johtuu juuri ihmisten tarpeista tuoda itseään ja ajatuksiaan esiin paikassa, josta muut pääsevät sen näkemään. Ihmisten halu päteä löytyy nykyisin usean tietovuodon taustalta. Sussman (2008, 335).

Sussmanin (2008, 335-336) mukaan muuttuneella tavalla tehdä töitä on osaltaan vaikuttanut tietovuotojen määrän kasvuun ja vaikeuttanut turvallisuusviestin kommunikointia. Virtuaalitiimit ja työskentely yhteistyökumppaniverkostoissa on vähentänyt ihmisten lojaliteetia pitää salaisuuksia, koska tiimien jäsenten välille ei ole syntynyt kunnollista sidettä. Syynä tähän on fyysisen läsnäolon määrän väheneminen. Ihmiset kommukoivat virtuaalisesti, mikä osaltaan on hidastanut ja vaikeuttanut luottamussuhteen synnyttämistä.

Tiimien etäjäsenet saattavat myös osaltaan olla tyytymättömiä rooliinsa tiimissä, mikä puolestaa voi johtaa sääntörikkomuksiin. Sussman (2008, 335-336).

4.5.3 Tietoturvallisuustietoisuuden parantaminen

Albrechtsen ja Hovden (2010, 432-435) tutkivat millaisilla keinoilla voisi parantaa työntekijöiden turvallisuustietoisuuden tasoa. Menetelmissä korostettiin vuorovaikutusta asiantuntijoiden ja työntekijöiden välillä. Tietoturvallisuusperehdytys piti sisällään keskusteluita, joissa työntekijät pääsevät esittämään näkemyksiään aiheesta. Perehdytyksen jälkeen suoritettiin arviointia, jossa työntekijät pääsivät yhteisesti pohtimaan opimaansa ja sen vaikutuksia heidän turvallisuuskäyttäytymiseensä. Tutkimus osoittaa, että perinteiset tietoturvallisuustietoisuuden lisäämiskeinot, kuten sähköpostiviestit, julisteet, yleiset koulutukset ja mainoslehtiset eivät tuota merkittävää muutosta ihmisten tietoturvallisuustietoisuuden tasossa. Tutkimuksen mukaan parempiin tuloksiin päästään organisaation sisäisellä ja yhteisöllisellä toiminnalla, jossa työntekijät pääsevät vaikuttamaan turvallisuuteen. Tutkijat nostavat esiin tiiviit tietoturvallisuustyöpajat, jossa yhteisesti käydään läpi ajankohtaista aihetta. He korostavat, että tällaisiä sessioita tulisi järjestää noin kaksi kertaa vuodessa, jotta ihmiset eivät unohda tietoturvalllisuuden merkitystä. Albrechtsen ja Hovden (2010, 435-444).

4.6 Viestintä kansainvälisessä ympäristössä

Kulttuurienvälinen viestintä tarkoittaa kommunikointia eri kulttuureista tulevien ihmisten kesken. Kulttuurienvälisessä viestinnässä ovat keskiössä kulttuurit, ihmisten arvot, uskomukset, tarpeet ja tavat. Gudykunst ja Mody (2002, 179). Kulttuurien välistä viestintää tapahtuu, kun henkilöt eri kulttuureista lähettävät viestejä toisilleen. Viestintäongelmat syntyvät tilanteista, joilloin viestin vastaanottaja ei ymmärrä viestiä oikein. Suuremmat kulttuurierot kasvattavat yleensä väärinymmärryksen todennäköisyyttä ja samalla vähentää viestinnän onnistumisen todennäköisyyttä. Adler (1986, 52–53).

Kansainvälisesti toimivien organisaatioiden on tärkeää osata viestiä tehokkaasti ja monipuolisesti eri kulttuuriesta tuleville sidosryhmille. Sidosryhmiin kuuluvat muun muassa asiakkaat, työntekijät, yhteistyökumppanit ja viranomaiset. Kansainväliseen viestintään liittyy useita haasteita, jotka vaihtelevat sidosryhmittäin. Näitä haasteita ovat vastaanottajien erilaiset kielet, arvot ja monenlaiset eri elämäntavat. Viestinnän vaikeus on suoraan riippuvainen edellä mainittujen tekijöiden määrästä. Ferraro (2005, 47).

Viestinnällä on keskeinen rooli kansainvälisten yritysten toiminnassa. Tällä on suuri vaikutus työntekijöihin, jotka työskentelevät näissä yrityksissä. Työntekijälle ei enää riitä, että osaa

kommunoida ihmisten kanssa, vaan pitää ymmärtää ja huomioida eri osapuolten erilaisuus. Kulttuuriguru (2010). Kultturigurun (2010) mukaan työntekijältä vaaditaan hyvää kielellistä osaamista, kulttuurialueen tuntemista, oikeaa asennetta ja viestintä menetelmien hallitsemista.

4.6.1 Kansainvälisen viestinnän haasteet monikulttuurisessa viestinnässä

Salo-Leen (2003) mukaan toimiminen monikulttuurisessa ympäristössä vaatii paljon työtä, koska asioihin ja niiden viestimiseen tulee paneutua syvällisemmin. Ihmisten toiminnassa näkyy yleensä etnosentrisyys eli omakulttuurikeskeisyys, joka on tyypillinen toimintatapa organisaatioiden sisällä keskuudessa, liiallinen keskittyminen omaan kulttuuriin voi johtaa kuitenkin johtaa konfliktoihin kulttuurien välisessä toiminnassa. Viestinnän tavoitteisiin päästään parhaiten siten, että eri osapuolet ymmärtävät toistensa tavoitteet ja kuinka hyvin he tulkitsevat toistensa viestejä. Viestinnän havainnointi ja tulkinta perustuvat pääosin opittuihin asioihin ja ovat siten kulttuurisidonnaisia. Salo-Lee (2003).

Sanatonta viestintää pidetään suurena haasteena eri kulttuureille. Nonverbaaliviestintä sisältää muun muassa eleet, ilmeet, katsekontaktin, koskettelun sekä fyysisen etäisyyden. Sanattomalla viestinnällä luodaan vaikutelmia, joita viestinnän toiset osapuolet tulkitsevat. Vaikutelmat syntyvät esimerkiksi ihmisten välisistä etäisyyksistä. Sanattoman viestintä näyttää yleensä viestijän oikean suhtautumisen kommunikoitavaan asiaan. Usein henkilö yrittää piilottaa tämän, mutta sanaton viestintä tuo totuuden esiin. Sanallinen ja sanaton viestintä muodostavat yhdessä kokonaisen vuorovaikutusprosessin. Se mitä sanotaan ja miten asia ilmaistaan ovat tavallaan symbioosissa keskenään. Sanaton ja sanallinen viestintä muodostavat yhdessä viestintätyylin. Viestintätyylit vaihtevat kovasti kulttuureittain, mikä asettaa suuren haasteen monikulttuuriselle viestinnälle. Esimerkiksi Aasiassa korostetaan korkeaa viestinnän kontekstia, missä hyödynnetään epäsuoraa viestintää eli pääosassa ovat ilmeet ja eleet. Pohjoismaissa taas käytetään enemmän matalaa kontekstia, mikä näkyy sanallisen viestinnän korostamisena. On kuitenkin tärkeää ymmärtää, että kaikissa kulttuureissa on sekä matalan että korkean viestinnän piirteitä. Salo-Lee (2003).

Kulttuurien välisessä viestinnässä on otettava huomioon useita erilaisia asioita, jotta se toimisi tehokkaasti ilman konflikteja ja epäselvyyksiä. Eri tekijät kuten paikka, aika sekä sosiaalinen ympäristö vaikuttavat merkittävästi viestintään. Kodykunstin ja Modyn (2002, 51). mukaan viestinnän onnistumiseen vaikuttaa keskeisesti se, annetaanko yksilöille mahdollisuus osallistua viestinnän prosessiin sekä sallitaanko oppiminen virheiden kautta. Hofsteden (1993, 329) mukaan työpaikoilla tulee olla mahdollista oppia monikulttuurisen viestinnän taitoja. Taitojen hankkimiseen ja oppimiseen liittyy kolme eri vaihetta. Kaiken perustana on tietoisuus ympärillä tapahtuvista asioista, mikä osaltaan auttaa oman harkintakyvyn

muodostamisessa. Tieto seuraa tiedostamista. Henkilöllä tulee hankkia ja omaksua tietoa eri kulttuureista ja niihin liittyvistä viestinnällisistä asioista. On myös erittäin tärkeää kerätä tietoa viestinnän kohteesta, pystyäkseen luomaan pohjan toimivalle viestinnälle. Tietoisuuden ja tiedon lisäksi tarvitaan taitoja. Taidot perustuvat tiedostamiseen, tietoon ja käytäntöntöihin. Eri käytäntöjen ja tapojen tunnistaminen viestintätilanteissa vaatii taitoa. Hofstede (1993, 329–332).

Munterin (1993) mukaan vaatimuksena tämän päivän kansainväliselle liiketoiminnalle, on hyvien monikulttuuristen viestintätapojen osaaminen ja sujuva hallinta organisaation eri tasoilla. Monikulttuurisessa viestinnässä korostetaan kielen ja erilaisten sanomien ymmärtämistä lähettäjän suunnittelemalla tavalla. Viestinnän monipuolisella osaamisella ja sen korostamisella voidaan luoda toimiva perusta monikulttuuriselle viestinnälle. Tavoitteena toimivalle kulttuurienväliselle viestinnälle on se, että kaikki viestinnän osapuolet ymmärtävät toisiaan ja kaikkien tarpeet otetaan huomioon tilanteesta riippuen. Ferraro (2005, 76). Tehokkaaseen viestintään monikulttuurisessa ympäristössä liittyy paljon erilaisia tekijöitä, jotka vaikuttavat vaikuttavat siihen, miten hyvin viestintä toimii. Näihin tekijöihin kuuluvat itsetietoisuuden rakentaminen, erilaisten näkökulmien erottaminen, kysymysten esittäminen, monimuotoisuuden tunnistaminen sekä stereotypioiden välttäminen. Erilaisuuksien arvostaminen ja kuunteleminen kuuluvat keskeisiin menestystekijöihin. Menestyvä viestintä on sekoitus monia tekijöitä, joiden painoja muutetaan joustavasti erilaisissa viestintä tilanteissa. Practicing Cross-Cultural Communication (2006).

4.7 Yhteenveto teoriakatsauksesta

Tuotetieto on yksi yrityksen suojattavista arvoista ja tietoturvallisuuskontrolleilla pyritään varmistamaan sen luottamuksellisuuden säilyminen. Yhteistyökumppaneiden kanssa työskentelemiseen liittyy arvokkaan tuotetiedon jakaminen osapuolten kesken. Tiedon luottamuksellisuuden turvaamiseksi käytetään sopimuksia, joiden avulla turvallisuusvaatimukset kommunikoidaan muodollisesti yhteistyökumppanille. Vaatimustenmukaisuutta seurataan taas pääosin auditeilla, jossa yhteistyökumppanin turvallisuustaso katselmoidaan. Yhteistyökumppanin hallintaa on olemassa muitakin menetelmiä, kuten yhteistyökumppanin toiminnan kehittäminen ja sen integroiminen lähemmäksi omaa toimintaa. Yhteistyökumppaneiden turvallisuuskulttuurit vaihtelevat kovasti ja ovat todennäköisesti kovin erilaiset verrattuna ostajayrityksen kulttuuriin. Toimiva turvallisuuskulttuuri on erittäin tärkeää, koska se ohjaa työntekijöiden turvallisuuskäyttäytymistä. Yhteistyökumppanin työntekijät käsittelevät työssään julkaisematonta tuotetietoa ja ovat myös pääsääntöisesti niitä, jotka mahdollistavat tietovuodot. Ihmisten on vaikeaa pitää salaisuuksia, koska meillä on sisäsyntyinen luoda siteitä ja kommunikoida muiden ihmisten kanssa. Suhteen syventyessä ihmiset paljastavat

helpommin asioita, jotka kokevat arvokkaiksi. Nykyihmisillä on myös tarve tuoda itseään ja ajatuksiaan esiin. Sosiaalinen media, blogit ja internet-kulttuuri mahdollistavat helpon väylän toteuttaa itseään ja jakaa asioita verkostonsa tai koko internetin kanssa.

On tärkeää, että yrityksillä on keinoja parantaa työntekijöidensä turvallisuustietoisuutta kattamaan nykymaailman uhat. Käytännöllisyys, hyvin perusteltu ja selkeästi esitetty viesti ovat keskeisessä asemassa työntekijöiden turvallisuustietoisuutta parannettaessa. Kansainvälisesti toimivien yritysten on tärkeää huomioida monikulttuurisuus turvallisuusviestintää suunnitellessa ja sitä toteutettaessa. Tuotetietovuotojen ennaltaehkäisytyö yhteistyökumppaniverkostossa koostuu moninaisista turvallisuuteen, kulttuuriin, viestintään ja ihmisen käyttäytymiseen liittyvistä asioista. Tämä tarkoittaa sitä, että ei ole olemassa yhtä menetelmää, teoriaa tai ratkaisua, jonka avulla vuodot voisi lopettaa. Pyrin tutustumani teorian pohjalta löytämään erilaisia tapoja jalkauttaa turvallisuutta keskeisten sidosryhmien keskuudessa ja arvioimaan menetelmien vaikuttavuutta käytännön työssä.

5 Tutkimuksellinen kehittämistyö

Tutkimus ja kehittäminen liittyvät usein yhteen, koska kehittämistyön pohjana käytetään tutkimusta tai tutkimuksellisiä menetelmiä. Tutkimuksellisella kehittämistyöllä voidaan nähdä olevan kaksi ääripäätä, joista toinen on tieteellinen tutkimus ja toinen taas kritiikitön arkiajatteluun perustuva kehittäminen. Itse tutkimuksellinen kehittämistyö on näiden ääripäiden välissä. Tutkimuksellinen kehittämistyö pyrkii ratkaisemaan käytännön ongelmia, uudistamaan käytäntöjä ja luomaan uutta tietoa työelämän käytännöistä. Kehitystyön tueksi kerätään tietoa sekä käytännöstä että teoriasta. Aineiston hankintaan käytetään useita erilaisia menetelmiä ja itse tutkimustyössä korostuu aktiivinen vuorovaikutus eri sidosryhmien kanssa. Tutkimuksellisen kehittämistyössä korostuu vaiheittaisuus ja se, että tuotoksia esitellään eri yleisöille, mikä osaltaan edistää kehitystyötä. Ojasalo, Moilanen ja Ritalahti (2009 17-22).

5.1 Tutkimuksellisen kehittämistyön prosessi

Kehittämistyö on prosessinomaista, jossa edetään vaiheittain. Tämä perustuu sille, että kehittämistyö koostuu selkeistä vaiheista, mikä osaltaan tekee työstä järjestelmällistä. Kehittämistyö lähtee liikkeelle tavoitteiden määrittelemisestä ja hankkeen systemaattisesta suunnittelusta. Kehittämistyö voidaan ajatella olevan muutostyön prosessi, jossa tavoitteiden määrittelyn jälkeen tehdään suunnitelma aikatauluineen. Tämän jälkeen suunnitelma toteutetaan, jota seuraa arviointivaihe, jossa nähdään kuinka hyvin muutostyössä onnistuttiin. Arviointi toimii yleensä pohjana seuraavan muutoshankkeen suunnitelmalle. Ojasalo ym. (2009 22-23).

Tutkimuksellisen kehittämishankkeen lähtökohtana on aina kehittämiskohteen tunnistaminen sekä siihen liittyvien tekijöiden tunnistaminen. Yleensä kehittämishanke liittyy joko liiketoiminnan tai työelämän muuttamiseen. Tavoitteena voi olla esimerkiksi uuden palvelukokonaisuuden luominen tai prosessin kehittäminen. Hanketta suunniteltaessa on tärkeää hankkia ymmärrys sille, mitä odotuksia työyhteisöllä on ja mitä nämä odotukset merkitsevät työyhteisön arjessa. Kehittämiskohteen tunnistamisen jälkeen ryhdytään kasaamaan siihen liittyvää tietoa. Käytännössä tämä tarkoittaa kohteeseen liittyvään teoriaan ja käytäntöihin tutustumista. Tutkijalta edellytetään kriittistä suhtautumista teoriaan ja kykyä tehdä valintoja, jotta löydettäisiin tutkimusta edistävä näkökulma. Näkökulma voidaan nähdä käsitejärjestelmänä, jonka pohjalta tutkismuksellista kehittämistyötä tehdään. Kohteeseen perehtymisen jälkeen määritellään kehittämistehtävä ja rajataan kehittämiskohde. Kohteen rajaamisen jälkeen valitaan tutkimukselliset ja kehittämiseen soveltuvat menetelmät. Menetelmien valinnassa tulisi pyrkiä valitsemaan sellaisia menetelmiä, jotka mahdollistavat vuorovaikutteisen työskentelyn. Seuraavaksi alkaa

käytännön jalkautustyö, jonka aikana toteutetaan suunniteltu muutos. Tämä on koko kehittämishankkeen keskeisin vaihe, joten siihen kannattaa varata suurin osa käytettävästä ajasta ja suurimmat resurssit. Toteuttamisvaiheeseen liittyy myös kehittämisen aikana syntyneen uuden tiedon jakaminen eri sidosryhmille, jotta muutkin voivat hyödyntää arvokasta tietoa. Viimeisessä vaiheessa kehittämistyön tulokset arvioidaan. On tärkeää ymmärtää, että tutkijan tulee tehdä kriittistä arviointia kehittämishankkeen eri vaiheissa, jotta varmistetaan kyky reagoida kohdeympäristössä tapahtuviin mahdollisiin muutoksiin. Ojasalo ym. (2009, 23-26).

5.2 Tutkimusmenetelmiä

Tässä osiossa tutustutaan erilaisiin tutkimusmenetelmiin, minkä pohjalta valitaan toimintaympäristöön ja työskentelytapaan soveltuvin tutkimusmenetelmä.

5.2.1 Kehittämistutkimus

Jorma Kanasen (2012, 19) mukaan kehittämistutkimuksessa yhdistyvät kehittäminen ja tutkimus syklisessä prosessissa. Organisaatiot kehittävät ja parantavat toimintaansa säännöllisesti. Tätä toimintaa kutsutaan kehittämistyöksi. Kehittämistutkimuksen taustalla on yleensä muutostarve, jonka seurauksena syntyy tuotos. Taustalla on aina tavoitteellinen suunta parempaan. Kehittämistutkimus itsessään ei ole oma tutkimusmenetemänsä, vaan joukko eri menetelmiä, joita hyödynnetään tilanteen mukaan. Kehittämistutkimus on enemmänkin monimenetelmäinen tutkimusote, jossa yhdistyvät kvalitatiiviset ja kvantitatiiviset tutkimusmenetelmät. Kehittämistutkimuksen taustalla on aina teoria tai useita teorioita, joihin kehittämisessä nojataan. Tämän lisäksi mukana täytyy kulkeä tutkimuksellinen ote, jotta voidaan puhua tutkimuksesta. Kehittämistutkimus on lähellä organisaation kehittämistyötä, jonka avulla parannetaan esimerkiksi yrityksen prosesseja, tuotteita, palveluita ja asiantiloja. Edellä mainitut kehittämiskohteet ovat muutenkin asioita, joiden kehittämiseen yritykset ja organisaatiot panostavat. Tutkimuksellisuus tähän saadaan kytkettyä, tekemällä kehittämistyötä tiedettä. Tämä tapahtuu tieteellisiä menetelmiä hyödyntämällä, kehittämistyön dokumentoinnilla ja sillä, että osana kehittämistukimusta tuotetaan uutta tietoa. (Kananen 2012, 19-21).

Kehittämisestä varten tulee olla valittuna tutkimuksen kohde. Tämä voi olla esimerkiksi prosessi, toiminto, asiantila tai tuote. Kohde voi käytännössä olla, mitä vaan, kunhan siihen voidaan vaikuttaa. Kehittämistutkimuksen keskeiset haasteet liittyvät kohteen määrittelyyn ja rajaamiseen. Nämä samat ongelmat ovat tyypillisiä muillekin tutkimusmenetelmille. Käytännössä kehittämiskohteessa tulisi olla ongelma, joka pyritään ratkaisemaan ja samalla muuttamaan kohdetta. Ongelman ja kehittämiskohteiden lisäksi on olemassa toimenpiteitä,

interventioita, joilla pyritään saamaan aikaiseksi muutos. Interventioiden valintaan liittyy paljon haasteita, kuten mitkä ovat oikeita keinoja muutoksen aikaansaamiseksi ja miten muutokset onnistutaan kohdistaan oikeaan kohteeseen? Kehittämistutkimus vaatii tutkijalta paljon osaamista, koska prosessin sisäiset mekanismit ja tekijöiden väliset syy-seuraussuhteet on tunnettava, koska muuten on mahdotonta vaikuttaa oikealla tavalla. Ilman aiheen ymmärrystä on myös vaikeaa valita oikeita interventioita. (Kananen 2012, 21).

Muutokseen ja kehittämiseen liittyvät myös muutoksen mittaaminen ja mittaamiseen käytettävät mittarit tai vähintään muutoksen vaikuttavuuden arviointi. Mittareilla on tarkoitus mitata´muutosta ja on tärkeää, että ne ovat valideja eli tarkoituksenmukaisia. Kehittämiskohteet vaihtelevat kovasti, joten mittarit tulee rakentaa sellaisiksi, että niillä voidaan mitata juuri kyseessä olevan kohdeympäristön muutosta. Kananen (2012, 22-23). Kanasen (2012, 23) mukaan muutos kohteessa tai sen kehittyminen voidaan asettaa tavoitteen muotoon. Tavoitteen on aina oltava mitattavissa, jotta sen saavuttavuus voidaan todentaa. Tavoitteen määrittelemättä jättäminen tarkoittaa sitä, että saavutettua muutosta ei välttä voida todentaa. Kehittämistutkimuksen tavoitteen tulee täyttää seuraavat yleiset vaatimukset: 1) mitattavuus, 2) yksiselitteisyys, 3) hyväksyttävyys, 4) keskeisyys, 5) kattavuus, 6) realistisuus, 7) ristiriidattomuus ja 8) vaikutettavuus. Kananen (2012, 23).

5.2.2 Kvalitatiivinen tutkimus

Hirsjärven, Remeksen ja Sajavaaran (160-161, 1998) mukaan kvalitatiivinen tutkimus eli laadullinen tutkimus keskittyy todellisen elämän kuvaamiseen. Tutkimuksessa on tärkeää huomioida, ettei sen kohdetta voi pilkkoa osiin, koska aihe saattaa pitää sisällään useita tapahtumia ja niiden moninaisia suhteita. Tämän johdosta laadullinen tutkimus pyrkii tutkimaan aihetta kokonaisuutena. Kvalitatiivisen tutkimuksen tekijä ei yleensä pysty olemaan täysin objektiivinen, koska tutkijan omat arvot vaikuttavat hänen tulkintoihinsa. Kvalitatiivisessa tutkimuksessa saadaan tuloksiksi yleensä johonkin aikaan ja paikkaan liittyviä ehdollisia selityksiä. Tästä johtuen laadullisessa tutkimuksessa on tavoitteena löytää tai paljasta tosiasioita. Kvalitatiivinen tutkimus ei pyri suoranaisesti todentamaan jo olemassa olevia asioita, joita pidetään totuusväittäminä. Hirsjärvi ym. (1998, 161)

Kokonaisvaltainen tiedon hankinta, joka kootaan todellisissa tilanteissa, on ominaista laadulliselle tutkimukselle. Tutkimusta tehdessä ihmisellä on keskeinen rooli tiedon kerääjänä. Tyypillisesti tutkija luottaa enemmän omiin havaintoihinsa ja keskusteluihin tutkittaviensa kanssa, kuin mittausvälineisiin. Tätä perustellään sillä, että ihminen on tarpeeksi joustava sopeutuakseen muuttuviin tilanteisiin. Tästä huolimatta tutkijoilla on tapana hyödyntää lomakkeita ja testejä. Kvalitatiivista tutkimusta tehdessään tutkija pyrkii

paljastamaan odottamattomia seikkoja, minkä vuoksi tutkimuksen perustana ei ole teorian tai hypoteesien testaaminen, vaan tutkimusaineiston monimuotoinen ja syvällinen analysointi. Kvalitatiivisessa tutkimuksessa suositaan metodeja, joissa tutkittavien henkilöiden näkökulmat tulevat hyvin esille. Esimerkkejä aineistonkeruumenetelmistä ovat teemahaastattelu, osallistuva havainnointi, ryhmähaastattelut ja erilaisten aineistojen diskursiiviset analyysit. Laadullisen tutkimuksen kohdejoukko valitaan tyypillisesti tarkoituksenmukaisesti, ei sattumanvaraisesti. Laadullinen tutkimus etenee yleensä joustavasti ja suunnitelmia muutetaan tarpeen mukaan. Laadullisen tutkimuksen keskeisenä piirteenä voidaan pitää sitä, että kaikkia tapauksia käsitellään ainutlaatuisina ja tutkitaan sen mukaisesti. Hirsjärvi ym.(1998, 165).

5.2.3 Kvantitatiivinen tutkimus

Kvantitatiivinen eli määrällinen tutkimus vaatii, että tutkimuksen perustana on teorioita ja malleja. Se edellyttää ilmiön ymmärtämistä siten, että siihen vaikuttavat sisäiset ja ulkoiset muuttujat tunnetaan. Ilman muuttujien ymmärtämistä ei voida laskea mitään, koska ei tiedetä, mitä pitäisi laskea. Määrällisen tutkimuksen taustalla on lähes aina toinen tutkimus, jonka teoriaa hyödynnetään uudessa tutkimuksessa. Kvantitatiivisessä tutkimuksessa ilmiötä lähestytään ensin yleisestä näkökulmasta, minkä jälkeen mennään syvemmälle eli yksityiseen. Määrällisessä tutkimuksessa tutkimuskysymykset ovat selvillä, koska ne johdetaan jo todetuista ilmiöistä ja olemassa olevista teorioista. Kananen (2012, 31-32).

Kvantitatiivisessa tutkimuksessa on keskeistä lähteä liikkeelle olemassa olevista johtopäätöksistä, joiden pohjalla on aiempia teorioita. Keskeisessä roolissa ovat olettamuksien eli hypoteesien esittäminen, joiden perusteella tutkija rakentaa esimerkiksi strukturoidun kyselyn. Määrillisessä tutkimuksessa korostuu vahvasti käsitteiden määrittely, koska sen avulla tutkija voi osoittaa tutkimuksen pohjautuvan aiempiin teorioihin. Määrillisessä tutkimuksessa on tärkeää määritellä koejärjestelyiden ja aineiston keruun suunnitelmat, jotta saadaan kerättyä numeerista tutkimusaineistoa. Koehenkilöihin valintaan on oleellista panostaa, jotta saadaan valideja tuloksia. Kvantitatiivisen tutkimuksen aineisto esitetään aina taulukkomuodossa, jotta sitä voidaan käsitellä tilastollisilla menetelmillä. Johtopäätösten ja päätelmien teko perustuu tilastolliseen analyysiin, jossa tuloksia esitellään esimerkiksi prosenttitaulukoiden avulla. Hirsjärvi ym. (1998, 137).

5.2.4 Case-tutkimus

Case-tutkimuksella tarkoitetaan tapaustutkimusta, jossa yleensä tutkitaan, joko yhtä tai useita tapauksia. Tapaustutkimusmenetelmää käytetään usein psykologiassa ja liiketaloustieteessä. Tutkittava tapaus voi olla jokin suuri yksikkö esimerkiksi yritys tai sitten

jopa vain yksi henkilö, joita tarkastellaan omassa ympäristössään. Case-tutkimusta voidaan pitää lähestymistapana, jossa on sekä laadullisen, että määrällisen tutkimuksen piirteitä. Tutkimusaineistona käytetään erilaisia dokumentteja, arkistoja, haastatteluita ja havaintoja. Käytössä lähteiden määrä on erittäin suuri, lähinnä kaikki aineisto, joka tapaukseen liittyy. Mikäli tapaustutkimuksen tarkoituksena on kehittää tutkimuskohdetta, niin silloin se muuttuu kehittämistutkimukseksi. Case tutkimusta ei koskaan tehdä vain yhden tietolähteen varassa, koska laadukkaisiin tutkimustuloksiin vaaditaan evidenssiä, jota ei ole mahdollista saada kattavasti vain yhdestä lähteestä. Haasteellisinta case-tutkimuksessa on itse tapauksen valinta, koska jos kohteeksi on valittu yritys, niin miten sitä voidaan esimerkiksi haastatella tai havainnoida. Kananen (2012, 34-35).

Tapaustutkimuksessa valitaan yleensä yksi tapaus, jossa pyritään pääsemään syvälle. Case-tutkimuksen tulkinnan voi rakentaa, joko teorialähtöisesti tai aineistolähtöisesti. Teorialähtöisessä asetelmassa lähdetään liikkeelle ammattialan teorioista, joista sitten rakennetaan hypoteesejä. Tämän jälkeen näitä testataan tapauksella. Aineistolähtöisessä asetelmassa lähdetään liikkeelle siitä, että tutkija perehtyy materiaaliin ja katsoo millaisen teorian aineistosta voi rakentaa. Aineistolähtöisessä asetelmassa ei käytetä ennakkohypoteeseja. Tapaustutkimuksen luotettavuutta arvioidaan siihen liittyvän dokumentaation riittävyyden ja tarkkuuden perusteella. Case-tutkimuksen aikana itse tutkija pyrkii olemaan täysin ulkopuolinen havainnoija, joka ei millään tavoin osallistu tutkittavan ilmiön toimintaan, eikä omalta osaltaan pyri saamaan aikaiseksi minkäänlaista muutosta tai kehitystä. Mikäli tutkija osallistuu tapaustutkimukseen ja alkaa kehittämään kohdeympäristöä, niin tutkimus muuttuu joko toimintatutkimukseksi tai kehittämistutkimukseksi. Kananen (2012, 36-37).

5.2.5 Toimintatutkimus

Ojasalon ym. (2009, 58) mukaan toimintatutkimus on osallistavaa tutkimusta, jolla pyritään yhdessä ratkaisemaan käytännön ongelmia ja saamaan aikaan muutoksia. Tämän vuoksi toimintatutkimus sopii hyvin kehittämistyön lähestymistavaksi. Toimintatutkimuksella etsitään ratkaisuja käytännön ongelmiin, jotka voivat olla teknisiä, sosiaalisia, eettisiä ja ammatillisia. Tutkimuksen tavoitteena on ratkaista esimerkiksi yrityksen prosessiin liittyvä ongelma ja samanaikaisesti luoda uutta tietoa ilmiöstä. Toimintatutkimuksessa ollaan kiinnostuneita siitä, miten asioiden tulisi olla, eikä vaan siitä, miten ne ovat. Asioita tai epäkohtia ei vain nosteta esiin, vaan tavoitteena on nykytilan muuttaminen. Yleisiä tutkimuksen ja kehittämisen kohteita ovat organisaation toimintatavat ja toimintatilanne. Toimintatutkimuksen tyypillisiä piirteitä ovat ongelmakeskeisyys ja tutkijan aktiivinen rooli. Toimintatutkimuksessa on tärkeää se, että tutkittavat ymmärretään tietoisiksi toimijoiksi, joilla on aktiivinen rooli. Ojasalo ym. (2009, 58).

Toimintatutkimus on osallistava menetelmä, joka tarjoaa tutkijalle ja kehittäjälle monenlaisia etuja, koska yhteisesti kehitetty toimintamalli on monesti parempi, kuin ulkoa tulevat ja yleiseen teoriaan perustuvat mallit. Tämä johtuu siitä, että kehittettävän ympäristön tai yhteisön jäsenet tuntevat toimintaympäristönsä haasteet paremmin kuin muut. On kuitenkin tärkeää, että kohteena oleva yhteisö on valmis muutoksiin. Tutkija taas tuo ryhmään teoreettisen osaamisen tutkittavasta ilmiöstä ja oman ulkopuolisen näkökulmansa. Tutkijan tuoma lisäarvo auttaa yleensä ongelman ratkaisemisessa, tosin on tärkeää ymmärtää, että toimintatutkimuksen aikana tehtävä muutos voi toteutua tai olla toteutumatta. Vaikka muutos ei aina tapahtuisikaan, niin silti toimintatutkimus tuottaa yleensä uutta tietoa toimintaympäristön asenteista, valtarakenteista ja työkulttuureista. Tutkijan on tärkeää muistaa, että toimintatutkimus on onnistunut, vaikka muutosta ei saataisikaan aikaan, kunhan se vaan tuottaa uutta ja hyödyllistä tietoa. Toimintatutkimuksen keskeisimpänä haasteena on se, että tutkimus´kohde on tilanteeseen sidottu, jolloin aikaisempia tuloksia on erittäin vaikea hyödyntää. Tämän ymmärtää hyvin, jos tutkimuksen kohteena on yritys ja meillä tutkimustuloksia muista eri maissa toimivista vastaavanlaisista yrityksistä, eivät tulokset ole täysin hyödynnettävissä, koska yritysten kulttuurit saattavat vaihdella kovasti. Eräänä toimintatutkimuksen sudenkuoppana voidaan pitää, tavoitteiden ja menetelmien liian kevyttä määrittelyä. Usein myös kohteen lähtötilannetta eli nykytilaa ei analysoida tarpeeksi syvällisesti, mikä saattaa johtaa epärealistisiin odotuksiin. Ojasalo ym. (2009, 59).

Toimintatukimus soveltuu täydellisesti tutkimukselliseen kehittämistyöhön. Tutkimuksen kohde voi käytännössä olla mikä tahansa ihmiselämään liittyvä ilmiö. Toimintatutkimus soveltuu erinomaisesti sosiaalisten, työkäytänteiden ja työmenetelmien kehittämistyöhön. Sen pyrkimyksenä uuden ymmärtäminen ja kehittäminen ja näiden kuvaaminen kirjallisesti. Toimintatutkimus saattaa parantaa kohdeympäristön sisäistä kommunikaatiota ja sitä kautta ratkaista uudenlaisia ongelmia, jotka ovat aikaisemmin mahdollisesti jääneet piiloon. Tutkimus ei paneudu pelkästään siihen, miten asiat ovat, enemmänkin siihen, miten asioiden tulisi kohdeympäristössä olla. Toimintatutkimuksella pyritään ensisijaisesti nykytilan muuttamiseen käytönnön osallistavan toiminnan ja teoreettisen tutkimuksen vuorovaikutuksella. Ojasalo ym. (2009, 59-60).

Toimintatutkimus nähdään yleensä laadullisena eli kvalitatiivisena menetelmänä, mutta sen aikana voidaan hyödyntää myös kvantitatiivisiä menetelmiä. Tutkimusmenetelmiä pohdittaessa on tärkeää miettiä, miten tutkimustoteutetaan. Mikäli kyseessä on osallistava tutkimus ja kehittäminen, niin silloin menetelmienkin tulee olla laadullisia. Toimintatutkimuksen aikana voidaan kerätä aineistoa useilla erilaisilla menetelmillä. Näitä menetelmiä ovat muun muassa kyselyt, ryhmäkeskustelut, haastattelut ja havainnointi. Näistä

menetelmistä havainnointia pidetään usein parhaimpana aineistonkeruutapana. Näiden lisäksi tutkimusaineistona voidaan hyödyntää asiakirjoja ja erilaista kirjallista aineistoa. Yleisenä esimerkkinä kirjallisesta aineistosta voidaan pitää päiväkirjoja, joihin kohdeympäristön henkilöt kuvaavat erilaisia tapahtumia ja ilmiöitä. Toimintatutkimuksessa hyödynnetään paljon toimijoiden välisiä keskusteluita, joissa käydään läpi kyseistä kehittämisvaihetta. Tutkija dokumentoi keskustelun ja se toimii perustana kehittämisprosessin seuraavalle vaiheelle. Ojasalo ym. (2009, 61-62).

Toimintatutkimus voidaan nähdä prosessina, jossa edetään spiraalimaisesti. Toiminta etenee siis sykleissä, joiden eri vaiheet toistuvat uudelleen. Käytännössä ensiksi valitaan päämäärät tai määritellään kehittämisongelma tai –ongelmat, sekä asetetaan työn tavoitteet. Määrittelyn jälkeen tutustutaan teoriaan, jotta nähdään onko kyseisestä ilmiöstä aikaisempaa tutkimusaineistoa. Teoriaan tutustumisen jälkeen aihetta voidaan vielä täsmentää ja tavoitteita muokata selkeämmiksi. Itse kehittämistyö aloitetaan kokeilemalla ja tutkimalla, millaisilla käytännön toimenpiteillä voidaan päästä tavoitteeseen. Tämän jälkeen analysoidaan aineistoa ja arvioidaan jalkautettuja toimenpiteitä, sekä niistä saatuja tuloksia. Edellä mainituista asioista tehdään johtopäätöksiä, jotka konkretisoituvat muutoksina ja uusina käytännön kokeiluina. Usein johtopäätökset johtavat myös tavoitteiden muuttamiseen. Toimintatutkimuksen tutkimusprosessi koostuu siis suunnittelusta, toteutuksesta, havainnoinnista ja toiminnan arvioinnista. Näitä vaiheita toistetaan useita kertoja, koska yleensä yksi kerta ei välttämättä johda muutokseen tai uuden tiedon syntymiseen. Tutkijan on varautua siihen, että toimintatutkimus vie usein paljon aikaa, koska kyseessä tutkimuksellinen toiminnan kehittämisprosessi. Ojasalo ym. (2009, 60-61).

Kehittämistutkimuksen ja toimintatutkimuksen välillä on erittäin pieni eroavaisuus. Molemmat pyrkivät jonkin kohdeympäristön muuttamiseen tai parantamiseen. Käytännössä ero tulee siitä, että toimintatutkimuksessa itse tutkija on mukana kohdeympäristön toiminnassa. Tämä tarkoittaa sitä, että toiminta ja tutkimus toteutuvat samanaikaisesti. Toimintatutkimuksen kohteena ovat enemmänkin inhimilliset tekijät, kun taas kehittämistutkimus paneutuu enemmänkin ei-sosiaalisiin ilmiöihin, kuten tuotteisiin, palveluihin, prosesseihin ja toimintoihin. Kehittämistutkimus myöskään edellytä tutkijalta toimintatutkimuksen mukaista läsnäoloa. Kananen (2012, 41-42).

5.2.6 Tutkimusmenetelmän valinta

Toimintatutkimus on työhöni parhaiten soveltuva tutkimusmenetelmä, koska kyseessä on pitkäkestoinen kehittämishanke, jolla pyritään pysyvään muutokseen eli yhteistyökumppaniverkostosta tulevien tuotetietovuotojen vähentämiseen ja uusien ennaltaehkäisymenetelmien luomiseen. Toimintatutkimuksen valintaa tukee myös se, että

kyseessä on erittäin käytännönläheinen hanke, josta ei ole olemassa suoria tutkimustuloksia. Kolmantena perusteluna tutkimusmenetelmän valinnalle on se, että tutkimuksen aihe on osa päivittäistä työtäni, joten joudun väkisinkin osallistumaan aktiivisesti toimintatutkimuksen kaikkiin vaiheisiin. Toimintatutkimus on menetelmänä sellainen, että se sulautuu vaivattomasti osaksi yksikkömme kehittämistoimintaa, mikä puolestaan tukee tavoitteisiin pääsemistä. Tässä hankkeessa on ollut erittäin tärkeää löytää menetelmä, joka ei lisää ylimääräisiä kerroksia päivittäiseen toimintaan, koska meillä ei ole resursseja haaskattavaksi siihen, että tutkija tutkii sivusta muiden toimintaa ja lähettelee kyselylomakkeita täytettäväksi. Suuri osa toimintatutkimuksen aikana jalkauttavista menetelmistä ovat sellaisia, joita on käytetty Nokian sisällä ja niistä saatu palaute on ollut positiivista. Emme ole kuitenkaan aikaisimmin käyttäneet mitään varsinaista tutkimusmenetelmää toimenpiteiden jalkauttamiseen ja vaikutusten arvioitiin pitkäaikaisissa kehittämishankkeissa. Koen, että toimintatutkimusmenetelmää hyödyntämällä ja sitä testaamalla, voimme löytää jotain uutta, josta voi olla hyötyä vastaanvanlaisissa hankkeissa.

5.3 Toimintatutkimuksen tekemistä tukevia menetelmiä

Tässä osiossa tutustutaan toimintatutkimuksen tekemistä tukeviin tiedonkeruu ja kehittämismenetelmiin. Menetelmiin tutustumisen jälkeen valitaan niistä sellaiset, joista on hyötyä itse toimintatutkimuksen tekemiselle Nokian globaalissa työympäristössä.

5.3.1 Haastattelu

Haastattelu on yleisesti kätetty tiedonkeruumenetelmä, molemmissa sekä tutkimustyössä että kehittämishankkeissa. Haastattelu on hyvä menetelmä, koska sen avulla saadaan nopeasti kerättyä paljon syvällistä tietoa kohdeympäristöstä. Haastattelun avulla saadaan korostettua yksilöllisiä eli subjektiivisiä asioita, joita haastateltava yleensä tuo esiin. Erilaisia ihmisiä haastattelemalla saadaan usein esiin uudenlaisia näkökulmia jo tunnettuun ilmiöön. Haastettelulla pyritään yleensä jonkin asian syventämiseen tai sitten paremman selvyyden luomiseen. Haastattelumenetelmiä on useita, tosin niiden suurimmat erot liittyvät strukturointiasteeseen eli miten suljetuiksi kysymykset on muotoiltu, vai käytetäänkö avoimia kysymyksiä ja annetaan haastettelijalle mahdollisuus joustaa tilanteen mukaan. Ojasalo ym. (2009, 95-96).

Haastatteluun käytetty aika vaihtelee kovasti. Sen kesto voi olla mitä vaan, muutamista minuuteista tunteihin. Haastattelu on vuorovaikutusta, jossa haastattelijalla on suuri rooli haastateltavan mielenkiinnon ylläpitämisessä. On suositeltavaa nauhoittaa haastattelut, koska tämä mahdollistaa haastateltavan syvällisemmän tarkkailun. Tutkijan on tärkeää varata aikaa myös haastatteluiden jälkeen, koska tässä vaiheessa on tärkeää tehdä muistiinpanot,

jotteivat haastattelun aikana tehdyt havainnot pääse unohtumaan. Haastatteluiden oikeaoppiminen suorittaminen on vaativaa, joten on tärkeää perehtyä siihen syvällisesti. Ojasalo ym. (2009, 96).

5.3.2 Havainnointi

Havainnoinnin avulla saadaan selville tietoa siitä, miten ihmiset käyttäytyvät ja toimivat luonnollisessa toimintaympäristössään. Tutkimuksellisella havainnoinnilla tarkoitetaan jonkin kohteen systemaattista tarkkailua ja havaintoaineiston dokumentointia. Aineistoa voidaan kerätä sekä keinotekoisessa testiympäristössä että luonnollisessa toimintaympäristössä. Havainnointia voidaan käyttää itsenäisesti tai esimerkiksi haastattelun ohessa. Havainnoinnin keskeisenä hyötynä on se, että päästään luonnolliseen ympäristöön katsomaan, että toimivatko ihmiset kuvaamallaan tavalla. Havainnointi sopii erittäin hyvin kehittämistehtäviin, joiden kohteena on ihmisen toiminta ja vuorovaikutustilanteet. Vaikeasti ennakoitavat ja nopeasti muuttuvat tilanteet ovat sellaisia, joiden nykytilan arviointiin havainnointi on oivasti soveltuva menetelmä. Havainnointitilanteet tulee suunnitella hyvin etukäteen, koska ennakkovalmistelut pitävät sisällään useita toimintoja. On tärkeää pohtia, että tapahtuuko havainnointi läpinäkyvästi vai suoritetaanko se kohteelta salassa. Havainnointi vaatii usein luvan pyytämistä, havainnoinin kohteelta. Havainnoinnin tulokset on tärkeää kirjata muistiin järjestelmällisesti. Apuvälineiden, kuten videokameroiden jne. Käyttäminen on suotavaa, koska ihmisen havainnointikyvyt ovat rajalliset. Tallennusvälineiden käyttämättä jättäminen saattaa merkitä jonkin oleellisen ilmiön jäämistä pois tutkimusaineistosta, koska tutkija ei ole sitä kyennyt rekisteröimään. Havainnointi saattaa häiritä kohdetta ja mikä taas osaltaan saattaa muuttaa kohteen normaalia toimintaa. Tämä nähdään yleisesti havainnoinnin heikkona puolena. Ojasalo ym. (2009, 103-105).

5.3.3 Kysely

Kyselytutkimus on yleisesti käytetty määrällisen tutkimuksen menetelmä, koska sen avulla voidaan kerätä laaja tutkimusaineisto. Kyselyt tuottavat usein paljon numeerista aineistoa, jota sitten puolestaan analysoidaan tilastollisesti. Tiedonkäsittelyyn käytetään yleisesti Microsoftin excel-ohjelmistoa. Kyselyn heikkouksina pidetään sen pinnallisuutta ja sitä, että ei voida olla täysin varmoja, kuinka tosissaan vastaajat ovat kyselyyn vastanneet. Kyselyitä voidaan lähettää postitse, tehdä puhelimessa tai kasvokkain sekä rakentaa internetissä vastattavia lomakkeita. Kyselytutkimus soveltuu erinomaisesti erilaisten aiheiden ja ilmiöiden tutkimiseen. Kyselyä suunniteltaessa ja rakennettaessa on tärkeää, että tutkijalla on olemassa paljon aikaisempaa tietoa tutkittavasta ilmiöstä, koska ilman tietoa on vaikeaa rakentaa kunnollista kyselylomaketta. Ojasalo ym. (2009, 108-109).

5.3.4 Dokumenttianalyysi

Dokumenttianalyysillä tarkoitetaan menetelmää, arvoidaan ja tehdään päätelmiä kirjalliseen muotoon tehdystä aineistosta. Analyysin kohteina voivat olla muun muassa haastattelumuistiot, www-sivut, artikkelit, palaverimuistiot, raportit. Menetelmän avulla pyritään luomaan selkeä ja kirjallinen kuvaus tutkittavasta kohteesta. Dokumenttianalyysin vahvuutena pidetään sen herkkyyttä asiayhteydelle eli sille miten tutkimuksen kohteena oleva ilmiö esiintyy luonnollisessa ympäristössään. Menetelmällä voidaan menestyksekkäästi analysoida sellaistakin kirjallista aineistoa, jota ei ole tarkoitettu tutkimusta varten. Yhtenä esimerkkinä voidaan markkinointiesitteitä ja www-sivuja. Dokumenttianalyysi voidaan jakaa kahteen eri analyysitapaan. Sisällön analyysillä tarkoitetaan, sitä että tutkija pyrkii kuvaamaan dokumenttien sisältöä sanallisesti. Tällä pyritään tekstin merkityksien tunnistamiseen. Sisällön erittelyllä puolestaan tarkoitetaan dokumenttien analysointia, jossa määrällisesti dokumenttien sisältöjä. Dokumenttianalyysissä aineisto hajotetaan osiin, käsitteellistetään ja kasataan uusitulla tavalla loogiseksi kokonaisuudeksi. Ojasalo ym. (2009. 121-122).

5.3.5 Ennakointi

Ennakoinnilla pyritään tarkastelemaan systemaattisesti ja pitkäjänteisesti jonkin aihealueen tulevaisuutta sekä yritetään tunnistamaan tutkimus- ja kehittämisalueita, joista on mahdollista saada suuri taloudellinen, organisatorinen ja yhteiskunnallinen hyöty. Ennakoinnissa on mahdollisuus käyttää lukuisia eri aineistonkeruumenetelmiä, koska sen avulla pyritään selvittämään mahdollista tulevaisuutta. Ennakointi on ominaisuuksiltaan arvosidonnaista, mikä tarkoittaa sitä, että tutkimuksiin otetaan erilaisia rooleja asiantuntijoista, päättäjiin ja edunvalvojiin. Yksi yleisistä tulevaisuuden analysointimenetelmistä on skenaariotyöskentely. Skenaarioilla tarkoitetaan ajallisesti toisiaan seuraavien ja perusteltavissa olevien vaihtoehtoisten tulevaisuuskuvien sarjaa. Skenaariota voidaan pitää myös tarinana tai kertomuksena, jolla pyritään halutun tulevaisuuden saavuttamiseen. Skenaariossa kuvataan aina keskeiset toimijat, toiminnot, päätöksentekoprosessi sekä päätöksiin liittyvien seurausten tapahtumaketju, joka johtaa tästä hetkestä haluttuun tulevaisuuteen. Skenaariomenetelmä on hyvä tapa herättää laajankin joukon kiinnostus eri tulevaisuuksia kohtaan, koska sen avulla voidaan tuoda esiin uutta ja tuoretta aineistoa. Skenaariomenetelmässä analysoidaan nykyhetkeäm megatrendejä, heikkojasignaaleita ja muita virtauksia. Ojasalo ym. (2009, 131-132).

Skenaariotyö jaetaan kuuten vaiheeseen. Työn ensimmäisessä vaiheessa selvitetään kohdeympäristön nykytila, SWOT-analyysiä hyödyntämällä. SWOT-analyysissä kuvaataan kohteen vahvuudet, heikkoudet, uhat ja mahdollisuudet. Tämän jälkeen arvioidaan käytössä

olevat resurssit ja organisaation arvot, pelot, toiveet ja tavoitteet. Edellä mainittuun analyysiin liitetään myös megatrendit, heikot signaalit ja niiden vaikutukset. Sitten ryhdytään rakentamaan skenaarioita, joita tulisi olla vähintään kolme. Skenaarioiden pohjalta rakennetaan organisaatiolle tulevaisuuden visio. Viimeisessä vaiheessa luodaan strategia, jossa lopullisesti päätetään ne toimenpiteet joilla visio voidaan saavuttaa. Skenaariotyön lisäksi on olemassa myös Delfoi-menetelmä ja tulevaisuusverstaat, joilla voidaan tutkia tulevaisuutta. Ojasalo ym. (2009, 133-137).

5.3.6 Yhteisöllisiä ideointimenetelmiä

Uuden kehittämiseen tarvitaan luovuutta, koska ilman sitä ei synny innovaatioita. Luovuus voidaan nähdä kykynä ja rohkeutena katsoa ja arvioida asioita, kuten yrityksen toimintatapoja uudella tavalla. Uusien näkökulmien tuottamista varten on olemassa useita erilaisia työkaluja. Työkaulujakin keskeisemmässä roolissa on avoin ja positiivinen ilmapiiri, jota ilman luovuus ei yleensä pääse esille. Uuden keksimisessä auttaa se, että on olemassa sopiva ryhmä, joka yhdessä ratkoo ongelmia ja pyrkii tuomaan esiin uusia näkökulmia. Innovaatiot syntyvät pitkäjänteisen ja kärsivällisen prosessin kautta. Välillä uusia ideoita ryöpsahtelee ja välillä voi olla pitkiäkin aikana niin, että mitään ei synny. On tärkeää, että luovan ongelmanratkaisun prosessissa ideointi ja arviointi pidetään erillilään, koska liian varhainen idean arviointi voi helposti tyrehdyttää innovaation jalostamisen, ja jopa estää sen puhkeamisen kukkaan. Ojasalo ym. (2009, 143).

Luova ongelmanratkaisu on prosessi, joka pitää sisällään ongelman tai parannusmahdollisuuksien löytämisen ja siihen liittyvien asioiden tunnistamisen. Tämän jälkeen asetetaan tavoite ja määritetään visio, jonne halutaan päästä. Kun on ensin määritetty minne halutaan päästä, niin sen jälkeen pohditaan lähestymistapoja ja ideoidaan uusia näkökulmia. Tämän jälkeen ideat arvioidaan ja valitaan niistä parhaimmat, jotka soveltuvat pöydällä olevan ongelman ratkaisemiseksi. Priorisoinnin jälkeen on tärkeää hankkia hyväksyntä ratkaisujen jalkauttamiselle, jonka jälkeen ratkaisu toteutetaan suunnitelman mukaisesti. Ojasalo ym. (2009, 144).

5.3.7 Prosessianalyysi

Prosessianalyysi on menetelmä, jonka avulla voidaan tutkia ja kehittää prosesseja. Analyysin aikana voidaan selvittää eri osapuolien roolit prosessissa, mitkä ovat prosessin kriittiset vaiheet sekä missä ja miksi mahdollisia ongelmia ilmenee. Näiden tietojen pohjalta pyritään löytämään ja ideoimaan ratkaisuja löydettyihin ongelmiin. Menetelmää käytettäessä luodaan prosessikaavio, joka havainnollistaa prosessin vaiheet, niissä ilmenevät ongelmat ja niihin ratkaisemiseen soveltuvat ideat. Ojasalo ym. (2009, 158-159).

5.3.8 Benchmarking

Benchmarking perustuu sille, että ollaan kiinnostuneita siitä, miten toiset yritykset toimivat ja menestyvät. Yleensä benchmarkingin kohteena on menestyvä yritys tai organisaatio, jolta sitten muut pyrkivät benchmarkingin kautta oppimaan uusia hyviä käytäntöjä. Benchmarkingia voidaan tehdä joko organisaation sisäisten tai ulkoisten toimijoiden kanssa. Benchmarking vaatii aina perusteellisen pohjatyön, jossa pyritään erityisesti tunnistamaan ja rajaamaan kehittämistä kaipaava kohde. Ilman kunnollista pohjatyötä ei välttämättä päästä haluttuihin kehittämistavoitteisiin. Kohteen määrittelyn jälkeen etsitään sopiva vertailukumppani tai useita vertailukumppaneita, joilta yritys voi oppia. Tämän jälkeen kerätään aineistoa ja järjestetään yritysvierailuita, joiden aikana voidaan havainnoida isäntäyritysten käytäntöjä. On tärkeää, että benchmarkia tekevä yritys osaa tunnistaa ne asiat, jotka ovat sovellettavissa omassa organisaatiossa, sillä yleensä kaikkia hyvää ei pysty omaan organisaatioonsa jalkauttamaan. Benchmarking on hyvä menetelmä oman organisaation kilpailukyvyn kehittämiseen. Ojasalo ym. (2009, 163-164).

5.3.9 Kehittämismenetelmien valinta

Tuotetietovuotojen ennaltaehkäiseminen yhteistyökumppaniverkostossa on sen verran käytännönläheinen aihe, joten valitsen kehittämismenetelmiksi sellaisia menetelmiä, joita muutenkin hyödynnämme organisaatiossamme. Tulen eniten hyödyntämään luovaa ongelmanratkaisua, jonka avulla pyrimme löytämään uusia ja toimivampia tapoja vaikuttaa keskeisten sidosryhmien toimintaan. Tämän toiminnan tulisi osaltaan vähentää tuotetietovuotoja. Toisena keskeisenä menetelmänä käytetään prosessianalyysiä, jonka avulla pyritään löytämään kehityskohteita hankintaprosessista ja siihen liittyvistä turvallisuusaktiviteeteista. Tulen myös hyödyntämään haastetteluita, havainnointia ja dokumenttianalyysia, mutta en yhtä syvällisellä tavalla kuin tieteellisessä tutkimuksessa. Työni on vuorovaikutteista ja olen jatkuvasti tekemisissä eri sidosryhmien kanssa, joka mahdollistaa minulle haastettelutyyppisen keskustelun käymisen aina kun näen sille tarvetta. Havainnointia hyödynnetään siinä, että katsotaan käytännössä, miten ihmiset toimivat hankintaprosessissa. Dokumenttianalyysiä hyödynnän olemassa olevien ohjeiden ja muiden aineistojen analysoimiseksi, jotta näen, onko niiden sisältö riittävä tavoitteeseen pääsemiseksi.

6 Tutkimuksen suorittaminen

6.1 Tavoite ja tutkimuskysymys

Toimintatutkimuksen ja ohessa tehtävän kehittämishankkeen tavoitteena on löytää ja kehittää kohdeympäristöön sopivimmat tuotetietovuotojen ennaltaehkäisymenetelmät. Tutkimuksessa huomiodaan kansainvälinen toimintaympäristö ja arvioidaan menetelmien toimivuutta käytännössä. Työssä keskitytään löytämään yksinkertaisia, edullisia ja tehokkaita menetelmiä, joilla saadaan vähennettyä tuotetietovuotoja yhteistyökumppaniverkostossa. Mittarina käytetään vuosien 2011 ja 2012 vuototilastoja. Tarkoituksena ei ole tehdä nopeata ja kevyttä hanketta, vaan syvällistä ja pitkäkestoista kehitystyötä, jossa luodaan pohja uudelle turvallisuuskulttuurille ja kestäville rakenteille. Uudistettu turvallisuuskulttuuri ja kestävät rakenteet mahdollistavat tuotetietovuotojen määrän merkittävän vähenemisen tulevina vuosina, koska hankkeessa kehitettävät menetelmät ja toimenpiteet tulevat osaksi normaalia turvallisuustoimintaa yhteistyökumppaniverkostossa.

Hankkeen tavoite on äärimmäisen haastava, koska verkosto on todella laaja pitäen sisällään tuhansia eri kokoisia yrityksiä, jotka toimivat lukuisilla liiketoiminta-alueilla ja tulevat eri kulttuureista ympäri maailmaa. Pystyäkseen vähentämään tuotetietovuotoja tulee kehittämistoiminpiteet jalkauttaa kaikkialle, missä on toimintaan liittyviä sisäisiä ja ulkoisia sidosryhmiä, koska jonkin yhteistyökumppanin tai sidosryhmän väliin jättäminen lisää vuotoriskin todennäisyyttä. Onnistumista tullaan mitataan sillä, onnistutaanko vuotoja ennaltaehkäisemään niistä ympäristöissä joihin turvallisuusmenetelmiä jalkautetaan. Vuosien 2011 ja 2012 kokonaisvuototilastot auttavat osaltaan näkemään onko vuotojen trendi laskeva vai nouseva, mutta onnistumista ei niiden avulla voida täysin arvioida, koska kaikkien vuotojen syitä ei saada selville, mikä saattaa vääristää tilastoja. Tavoitteena on myös luoda uutta tietoa tuotetietovuotojen ennaltaehkäisystä kansainvälisessä yhteistyökumppaniverkostossa.

Tutkimuskysymys: Millaisilla menetelmillä voidaan ennaltaehkäistä tuotetietovuotoja Nokian kansainvälisessä yhteistyökumppaniverkostossa?

6.2 Aiheen rajaus

Tuotetietovuotojen ennaltaehkäisytyöhön liittyy useita erilaisia sidosryhmiä. Luonnollisesti yhteistyökumppanit ovat näistä keskeisin, koska Nokia antaa arvokasta tuotetietoa heidän haltuunsa. Hankkeeseen sisältyvät vain ne yhteistyökumppanit, jotka käsittelevät julkaisematonta tuotetietoa. Yhteistyökumppanien käyttämät alihankkijat sisältyvät hankkeeseen, mikäli myös ne käsittevät Nokian julkaisematonta tuotetietoa. Tosin Nokia ei

suoranaisesti jalkauta menetelmiä niin syvälle verkostossa, vaan vastuu tästä on yhteistyökumppanilla. Toki samat menetelmät soveltuvat näihin tapauksiin. Sisäisistä sidosryhmistä hankkeeseen sisältyvät Nokian hankintayksikkö, joka rakentaa sopimuksellisen perustan yhteistyölle ja huolehtii kumppanin kyvykkyyksien arvioinnista ja kehittämisestä. Nokian liiketoimintayksiköt puolestaan työskentelevät ja jakavat tietoa yhteistyökumppaneiden kanssa, joten ovat myös yksi hankkeeseen kuuluvista sidosryhmistä. Liiketoimintayksiköiden ihmiset voivat helposti huonolla turvallisuuskäyttäytymisellään ohjata yhteistyökumppaneiden työntekijöitä olla noudattamatta ohjeita. Hankkeeseen sisältyy paljon eri sidosryhmiä ympäri maailmaa, joita ei voi rajata pois, koska heidän tekemisensä on niin keskeisesti kytketty yhteen. Yhden sidosryhmän laiminlyönnillä voi olla merkittävä vaikutus muihin ryhmiin ja siihen miten hyvin ne käsittelevät tuotetietoa.

Hankkeessa pyritään löytämään sellaisia turvallisuustoimenpiteitä, joilla voidaan vaikuttaa ihmisten turvallisuuskäyttäytymiseen. Menetelmillä pyritään suojaamaan julkaisemattoman tuotetiedon luottamuksellisuutta yhteistyökumppanin työntekijöiden toimesta. Tarkoituksena on etsiä yleisesti tunnettuja tietoturvallisuuskontrolleja, joita voidaan menestyksekkäästi hyödyntää tuotetietovuotojen ennaltaehkäisytyössä. Osaa kontrolleista tullaan soveltamaan kohdeympäristöön paremmin soveltuviksi. Suurin osa tietoturvallisuuskontrolleista rajataan hankkeen ulkopuolelle, koska aiheena on pelkästään julkaimattoman tuotetiedon suojaaminen.

6.3 Toimintatutkimuksen kulku

Työ aloitettiin tammikuussa 2012, jolloin analysoitiin sen hetkinen tilanne yhteistyökumppaniverkossa tapahtuneiden tuotetietovuotojen osalta. Samalla aloitettiin kohteen tai paremminkin sanottuna toimintaympäristön nykytila-analyysi, jota on osaltaan täydennetty koko hankkeen ajan, koska uutta tietoa syntyy jatkuvasti. Tammi- ja helmikuussa tutustuin olemassa oleviin tietoturvallisuuskäytäntöihin ja menetelmiin, joita voisin hyödyntää ennaltaehkäisytyössä. Samalla valitsin ensimmäiset jalkautusmenetelmät, joita hyödynnettiin maaliskuun ja elokuun välisenä aikana. Tuona aikana tein myös kehitystyötä ja räätälöin muutamia uusia menetelmiä ennaltaehkäisytyöhön. Syyskuussa analysoitiin hyödynnettävien menetelmien toimivuutta ja tehtiin hieman muutoksia olemassaoleviin menetelmiin. Tämän jälkeen jalkautusta jatkettiin pienten muutosten kera helmikuun 2013 loppuun asti. Maaliskuussa menetelmien toimivuus arvioitiin uudestaan ja valittiin ne menetelmät, joita tullaan hyödyntämään jatkossa tuotetietovuotojen ennaltaehkäisytyössä Nokian yhteistyökumppaniverkostossa. Opinnäytetyön loppuraportti on kasattu huhtikuussa 2013.

Kuvio 3: Toimintatutkimuksen kulku.

6.3.1 Käytännön toteuttamisesta

Laajaan globaaliin kehittämishankkeeseen liittyy useita riskejä, koska sen läpiviemiseen tarvitaan yli yksikkörajojen tehtävää yhteistyötä sekä sisäisten että ulkoisten sidosryhmien kanssa. Mikäli osa sidosryhmistä ei sitoutu hankkeen läpivientiin, niin se saattaa hidastaa hanketta tai jopa kokonaan estää turvallisuustoimenpideiden jalkauttamisen. Hankkeessa olevat henkilöresurssit ovat myös rajalliset ja ne joudutaan jakamaan muiden käynnissä olevien hankkeiden kesken. Kehittämishankkeen aikataulu on kunnianhimoinen, mikä tarkoittaa sitä, että siinä pysyminen vaatii nykytila-analyysistä suoritumista aikataulun mukaisesti. Nykytila-analyysin viivästyminen siirtää jalkauttamisen aloittamista, mikä osaltaa estää hankkeen valmistumisen vuoden loppuun mennessä.

Kehittämishankkeessa tullaan käyttämään täysin uusia turvallisuustoimenpiteitä, joita on onnistuneesti testattu muutamien sidosryhmien kanssa vuoden 2011 aikana. Osa jalkautettavista toimenpiteistä ovat taas täysin uusia. Niitä ei ole käytetty toimintaympäristössämme aikaisemmin. Tämä tarkoittaa sitä, että ei ole täyttä varmuutta niiden toimivuudesta ja siitä miten hyvin sidosryhmät ottavat ne vastaan. Tätä voidaan pitää pienenä epävarmuustekijänä, joka voi vaikuttaa hankkeeseen posiitivisesti tai negatiivisesti. Hankkeen kansainvälisyys tuo mukanaan lisää epävarmuustekijöitä, joilla voi olla vaikutusta hankkeen aikatauluun ja onnistumiseen. Voiko toimenpiteet jalkauttaa samalla tavalla maasta ja kulttuurista riippumatta, vai pitääkö esimerkiksi Kiinassa hoitaa jalkautus eri tavalla? On myös mahdollista, ettei jokin ennalta määritelty turvallisuustoimenpide tuo muutosta, koska

kyseisestä kulttuurista tulevat ihmiset eivät esimerkiksi ymmärrä luottamuksellisuuden käsitettä. Riskinä voidaan pitää myös kehittämishankkeen projektiryhmän liiketoimintaympäristön vaihtelevaa tuntemista. Mikäli ei tunne toimintaympäristöä hyvin, niin saataa jalkauttaa turvallisuustoimenpiteitä, jotka hidastavat ja muuten haittaavat liiketoimintaa merkittävästi, minkä seurauksena menetää jonkin sidosryhmän tuen.

6.3.2 Hankkeen riskienhallinta

Hankkeen alussa tullaan panostamaan sidosryhmäkommunikaatioon ja siinä erityisesti avoimuuteen ja läpinäkyvyyteen. Sidosryhmille tullaan avoimesti kertomaan nykyiset haasteet tuotetietovuotojen osalta ja kertomaan miksi niiden ennaltaehkäisy on tärkeää ja miten se hyödyttää Nokian liiketoimintaa. Avoimen viestinnän lisäksi jalkautettavia turvallisuustoimenpiteitä ei saa olla paljon ja niiden tulee olla selkeitä ja helposti hyödynnettäviä. Edellä mainituilla toimenpiteillä voidaan saada sidosryhmät paremmin sitoutettua tukemaan ennaltaehkäisytyötä. Nokian sisällä olemme avoimuudella ja läpinäkyvyydellä saaneet aikaan hyviä tuloksia. Resursseihin liittyviä riskejä voidaan hallita myös sidosryhmiä sitouttamalla, koska niistä voidaan saada vapaaehtoisia henkilöitä, jotka oman toimensa ohella auttavat nykytila-analyysiin tarvittavan tiedon keräämisessä ja turvallisuustoimenpiteiden jalkauttamisessa. Aikataulussa pysymiseen tarvitaan kurinalaisuutta, seurantapalavereita ja riittävien resurssien saatavuutta.

Valittujen turvallisuustoimenpiteiden käytettävyyteen ja oikeellisuuteen voidaan vaikuttaa pilotoimalla niitä ennen laajaa käyttöönottoa. Pilotoinnissa aikaisemmin testaamattomia toimenpiteitä testataan rajatussa ympäristössä, minkä jälkeen analysoidaan tulokset ja tehdään johtopäätökset toimenpiteen käytöstä hankkeen jalkautusvaiheessa. Pilotoinnista huolimatta kaikkia epävarmuustekijöitä ei voida poistaa, koska hankkeen aikataulu ei mahdollista laajaa pilotointia. Aikataulun salliessa voidaan hakea vahvistusta teoriasta tai kysellä kokemuksia muista yrityksistä. Globaalisuuteen ja turvallisuustoimenpiteiden jalkauttamiseen eri kulttuureihin liittyviin riskeihin tullaan vaikuttamaan siten, että turvallisuusyksikön sisältä kasattavaan projektiryhmään otetaan henkilöitä eri maanosista. Paikalliset henkilöt tuntevat parhaiten kyseisen kohdeympäristön kulttuurit ja niiden erityispiirteet. Tämä tullaan huomioimaan jalkauttamissuunnitelmassa, mikä osaltaa auttaa toimenpiteiden menestyksekästä käytäntöön viemistä. Projektiryhmän tueksi otetaan liiketoimintaosaajia eri liiketoiminta-alueilta, joiden kanssa tullaan katselmoimaan toimintaympäristökohtaiset turvallisuustoiminpiteet ja arvioimaan niiden liiketoimintalähtöisyys. Liiketoimintaosaajat auttavat myös projektiryhmään eri liiketoimintaalueiden ymmärtämisessä.

7 Nykytila-analyysi kohteesta

Nykytila-analyysin sisältö on kerätty Nokian Yritysturvallisuusyksikön toimesta yrityksen sisäisistä lähteistä ja sen tarkoituksena on ollut paikallistaa kehitysalueita. Aineiston keräämiseen on allekirjoittaneen lisäksi osallistunut useita saman organisaation työntekijöitä eri puolilta maailmaa. Nämä tiedot on kerätty osana konsernitason tietovuotojen ennaltaehkäisytyötä. Aineistonkeruumenetelminä on käytetty prosessianalyysiä, havainnointia ja haastatteluita. On kuitenkin tärkeää huomioida, että kyseisiä menetelmiä ei ole käytetty tieteellisen tutkimuksen näkökulmasta vaan osana organisaation normaalia kehittämistoimintaa.

7.1 Analyysi yhteistyökumppaniverkostossa toteutuneistä tuotetietovuodoista

Tuotetietovuotojen syitä on tutkittu jo useita vuosia, mutta tarkkoja tilastoja on pidetty vasta vuodesta 2010. Käytän vuosien 2011, 2012 sekä vuoden 2013 tammi-ja helmikuun tilastoja osana toimintatutkimukseen liittyvää kohteen nykytila-analyysiä. Tulen kuvaamaan muutamia vuotoja, jotta lukija saa käsityksen, miten niitä käytännössä tapahtuu. Tämän lisäksi olen seurannut yhteistyökumppaneiden osuutta kaikista vuodoista, koska tämä on yksi keskeisistä mittareista ennaltaehkäisevien menetelmien toimivuutta arvioitaessa. On tärkeää ymmärtää, että yhteistyökumppaneiden osuus vuodoista saattaa olla suurempi, kuin esitetty luku, koska kaikkien tuotetietovuotojen taustoja ei onnistuta selvittämään. Vuotoprosentti kertoo kuitenkin kehityksen suunnan eli ovatko yhteistyökumppaniverkostosta tulevien vuotojen määrä laskemassa vai kasvamassa.

7.1.1 Vuotojen syitä vuonna 2011

Vuonna 2011 15% tuotetietovuodoista aiheutui yhteistyökumppaneiden toimesta. Suurimmassa osassa tapauksessa vuosi ulos markkinointimateriaalia, kuten kuvia ja julistevedoksia. Tapausten taustoilta löytyi vuodoille altistavaa käyttäytymistä, jossa markkinointitoimistossa työskentelevät ihmiset laittoivat materiaalia internettiin tai käyttivät suojaamattomia tapoja siirtää tietoa. Eräässäkin tapauksessa henkilö oli tehnyt omat kotisivut ja päätti testata niiden toimivuutta julkaisemattomalla tuotekuvalla. Tyypillisesti kuvan päätyessä internettiin, bloggerit löytävät sen nopeasti, minkä jälkeen vuoto leviää nopeasti ympäri maailmaa. Myös sopimusvalmistajamme luona tapahtui muutamia vuotoja, jotka liittyivät paikallisiin tullausprosesseihin ja prototyyppinen lähettämiseen paikasta toiseen. Ensimmäisessä tapauksessa yhteistyökumppani oli ulkoistanut tullausjärjestelyt pienelle yritykselle, jonka työntekijä onnistui kuvaamaan laitteen ja laittamalla kuvan internettiin. Toisessa tapauksessa vuoto tapahtui prosessin myöhemmässä vaiheessa, jolloin laitteet olivat poistumassa valmistusmaasta. Kaikille näille näille tapauksille on yhteistä se, että kyseiset

yhteistyökumppanit ja heidän turvallisuusjärjestelynsä oli auditoitu Nokian toimesta. Tämän lisäksi salassapitosopimukset ja muut vaatimukset olivat sopimuksissa. Nämä toimenpiteet eivät kuitenkaan estäneet vuotoja, koska ne eivät keskittyneet tarpeeksi siihen, miten yhteistyökumppaneiden työntekijät käsittelevät julkaisematonta tuotetietoa. Sopimusvalmistajan vuototapaukset osoittivat, että pelkän tehtaan auditointi ei riitä, vaan pitää arvioida kaikki prosessit, joissa julkaisematonta tuotetietoa kulkee. On myös tärkeää pohtia, miten voi vaikuttaa yhteistyökumppaneiden työntekijöiden turvallisuuskäyttäytymiseen, niin etteivät he tekisi tyhmiä virheitä.

7.1.2 Vuotojen syitä vuonna 2012

Vuonna 2012 11% tuotetietovuodoista aiheutui yhteistyökumppaneiden toimesta. Yhteistyökumppaneiden työntekijät vuosivat ulos tuotekuvia, tuotevideoita sekä kuvia prototyypeistä ja komponenteista. Eräässä tapauksessa erittäin luottamuksellinen video oli ladattu cargocollective nimiseen verkkopalveluun, jossa luovat yritykset ja luovalla alalla työskentelevät ihmiset esittelevät tuotoksiaan. Toisessa tapauksessa yhteistyökumppanin työntekijä oli käyttänyt palvelua, josta saa ladattua ammatillisesti kiinnostavaa tietoa, mutta palvelu vaati hänen tallentavan sinne vastineen, jota muut käyttäjät voivat hyödyntää. Tämä työntekijä päätti sitten tallentaa vastineeksi luottamuksellista tuotekehitystietoa.

Syksyllä 2012 havaitsimme Kiinassa vuotoepidemian, jonka seurauksena tapahtui useita vakavia tuotetietovuotoja. Suurimmassa osassa tapauksissa taustalta löytyi vuotajien henkilökohtainen halu kertoa työstään Nokian tulevien tuotteiden kanssa. Osittain taustalla oli myös sosiaalisen verkoston paine, joka houkutti henkilöitä paljastamaan luottamuksellista tietoa. Yksi tapaus oli hieman poikkeuksellinen, koska siinä henkilö oli suuttunut tuoteohjelman lopettamispäätöksestä. Hän oli niin ylpeä tuotteesta, jonka parissa oli työskennellyt, joten hän halusi levittää kuvia internettiin. Henkilö oli tunteiden vallassa, eikä ajatellut loogisesti tekojensa seurauksia. Näiden Kiinassa tapahtuiden vuotojen motiivina oli pääsääntöisesti siis halu päteä internetissä. Tarkempi analyysi osoitti myös puutteita yritysten turvallisuusperehdytyksessä ja fyysisen turvallisuuden käytännöissä. Perehdytysmateriaalit eivät pitäneet sisällään muun muassa, miten toimia turvallisesti sosiaalisessa mediassa. Havaitsimme myös, että pääsyä Nokian projektialueelle ei oltu rajoitettu tarpeeksi tehokkaasti, eikä kuvauskieltoa oltu laitettu käytäntöön riittävän hyvin.

Yksi näistä tapauksista oli omalla tavallaan poikkeuksellinen, koska Nokia oli muutamaa kuukautta ennen vuotoa käynyt pitämässä turvallisuuskoulutuksen kyseisen yhteistyökumppanin työntekijöille. Vuoto tapahtui koulutuksesta huolimatta, mikä osaltaan osoittaa, että internetkulttuuri ja henkilön halu päteä internetissä on monesti vahvempi kuin

turvallisuusviesti. Suurin osa vuonna 2012 tapahtuneista vuodoista, johtuivat ihmisten halusta nostaa itseään esiin internetissä tai heidän tekemistään virheistään.

7.1.3 Muita vuotoja mahdollistavia turvallisuustapahtumia vuosilta 2011-2012

Vuosina 2011 ja 2012 tapahtui paljon turvallisuustapahtumia ja läheltä piti tilanteita, jotka osaltaan mahdollistavat tuotetietovuodot. Nämä tapahtumat eivät aiheuttaneet tietovuotoja, mutta ilman oikeaa reagointia tai huonommalla tuurilla vuotoja olisi saattanut tapahtua paljon enemmän. Nämä tapaukset ovat oivallisia tapoja arvioida turvallisuusjärjestelyiden nykytilaa, koska niiden taustalta löytyy samoja epäkohtia kuin vuototapauksissa.

Meille raportoitiin useita prototyyppivarkauksia, joissa laitteita oli varastettu yhteistyökumppanien toimipisteista ja prototyyppilähetyksistä. Taustana näissä tapauksissa olivat puutteelliset toimitilaturvallisuusjärjestelyt ja vajaavaiset tiedot prototyyppien lähettämiseen liittyvistä asioista. Saimme tietoa useista tapauksista, jossa luottamuksellista tietoa lähetettiin osapuolten välillä ilman riittävää suojausta. Yhteistyökumppanit käyttivät usein suojaamattomia FTP-palvelimia sekä ilmaisia, internetistä löytyviä tiedonsiirto ja tallennuspalveluita, joiden turvallisuustaso ei ole yrityksen edellyttämien standardien mukainen. Tämän lisäksi meillä oli tapauksia, jossa yhteistyökumppanien työntekijät eivät noudattaneet prototyyppien käsittelyohjeita, vaan veivät laitteita pois tuotekehitysalueelta. Yhteistyökumppanien tiloissa järjestämämme auditit ja kumppanien tekevät itsearvioinnit osoittivat meille, että monilla yrityksillä oli vakavia puutteita heidän turvallisuusjärjestelyissään. Keskeiset puutteet olivat heikko turvallisuustietoisuudentaso ja se, että turvallisuusjärjestelyitä ei oltu integroitu osaksi liiketoimintaa.

7.1.4 Johtopäätökset

Vuototilastot osoittavat, että suurin osa vuodoista johtuu ihmisistä. Taustalla on tietämättömyyttä, halua päteä internetissä ja ohjeiden tahallista noudattamatta jättämistä. Vuototilastojen analyysi kertoo sen, että tuotetietovuotoja ei voi ennaltaehkäistä yhdellä menetelmällä tai pelkästään salassapitosopimuksilla ja turvallisuusvaatimuksilla. Auditointikaan ei ole tarpeeksi tehokas menetelmä, jos se ei arvioi kaikkia oleellisia prosesseja ja ihmisten turvallisuuskäyttäytymistä. Ennaltaehkäisevien menetelmien tulee ensisijaisesti keskittyä ihmisiin ja olla sellaisia, joilla voidaan vaikuttaa heidän käyttäytymiseensä. Sopimusvaatimukset ja turvallisuuskyvykkyyden auditoinnin luovat perustan, jonka lisäksi tulee kehittää muita ihmisiin ja kriittisiin prosesseihin vaikuttavia kontrolleja.

7.2 Turvallisuuskulttuuriin liittyviä kehittämisalueita

7.2.1 Turvallisuuskulttuuri Nokian sisällä

Nokian turvallisuuskulttuurin perustana on luottamus työntekijöihin ja usko siihen, että he tekevät oikeanlaisia turvallisuutta ja liiketoimintaa edistäviä päätöksiä. Luottamus mahdollistaa sen, että työntekijöillä on pääsyoikeus varsin laajaan määrään arvokasta ja julkaisematonta tuotetietoa. Turvallisuuskulttuurissa korostuu vastuullisuus, joka tarkoittaa vastuunottamista omista päätöksistä ja niiden seurauksista. Nokialla ei ole ollut tapana väkisin työntää turvallisuustietoisuutta työntekijöilleen, koska on luotettu siihen, että fiksut ihmiset huomioivat tarvittavat turvallisuusasiat työssään. Nokian turvallisuuskulttuurissa korostuvat sekä suomalainen ja osin Skandinaavinen yrityskulttuuri että globaali yrityskulttuuri. Ne näkyvät erityisesti luottamuksen korostamisessa ja pehmeämmässä, skandinaavisessa tavassa jalkauttaa turvallisuutta, mikä perustuu siihen, että yksilö huolehtii vastuualueistaan varsin itsenäisesti, ilman sen suurempaa valvontaa. Osana kulttuuria on ollut myös se, että virheistä ei rangaista, vaan niistä opitaan.

Useilla matkapuhelinliiketoiminnassa toimivalla yrityksellä on täysin erilainen turvallisuuskulttuuri. Eniten tähän vaikuttaa yrityksen kotimaa, vaikka kyseessä olisikin globaalisti toimiva yritys. Apple on loistava esimerkki täysin päinvastaisesta turvallisuuskulttuurista verrattuna Nokiaan. Apple ei luota työntekijöihinsä, mikä näkyy siinä, että ihmisillä on pääsy vain erittäin rajattuun määrään tietoa. Esimerkiksi älypuhelimen antennisuunnittelija ei tiedä, millaiseen laitteeseen antennia suunnittelee. Ihmiset työskentelevät siiloissa, peläten tekevänsä virheen turvallisuusasioissa, mikä tarkoittaa välitöntä irtisanomista vahingonkorvauksineen. Toisaalta Applen turvallisuuskulttuuri on toiminut hyvin ja onnistunut pitämään tuotetietovuodot kurissa.

Nokialla on taas ollut suuria vaikeuksia vuotojen kurissa pitämisessä, mutta viime aikoina olemme onnistuneet jalkauttamaan uudenlaista turvallisuuskulttuuria, jossa yrityksen johto on avoimesti kertonut työntekijöille olemassa olevista haasteista ja siitä, että vuodot aiheuttavat suurta vahinkoa liiketoiminnallemme. Tämä on ollut askel positiivisempaan suuntaan, koska yrityksen työntekijät kuuntelevat johdon esittämiä asioita ja usein myös muokkaavat toimintaansa toiveiden mukaisesti. Johdon esimerkki on aivan välttämätöntä kulttuurin jalkauttamisessa.

7.2.2 Globaalin yrityskulttuurin haasteita turvallisuudelle

Yrityksen johdon tehtävänä on määrittää turvallisuuden tavoiteet, jotka yleensä kirjataan yrityksen turvallisuuspolitiikaksi. Politiikka sisältää yrityksen johdon toivoman

turvallisuuskulttuurin ja kertoo yleisellä tasolla, että miten sinne päästään. Politiikassa kuvataan myös eri roolien vastuut ja jossain tapauksissa, mitä turvallisuuden laiminlyömisestä seuraa. On tärkeää ymmärtää, että politiikka antaa raamit turvallisuudelle, mutta ei kerro käytännössä, miten jokin toimenpide tehdään turvallisesti. Tätä tarkoitusta varten yrityksillä on turvallisuusohjeet, joiden tarkoituksena on kertoa työntekijöille millaista turvallisuustasoa yrityksen johto edellyttää eri toiminnoissa. Politiikka ja ohjeet jalkautetaan tyypillisesti osana uuden työntekijän turvallisuusperehdytystä. Tämän jälkeen turvallisuusviestiä toistetaan vaihtelevasti.

Turvallisuuspolitiikka ja ohjeistukset luodaan yleensä yrityksen pääkonttorissa, joka monesti sijaitsee sen kotimaassa. Tämä tarkoittaa sitä, että perusta yrityksen turvallisuustoiminnalle tulee sen kotimaan turvallisuuskulttuurista. Tämä tuo mukanaan mielenkiintoisen haaasteen globaaleille yrityksille, kuten Nokialle. Turvallisuuspolitiikka ja ohjeet perustuvat suomalaiseen turvallisuuskulttuurin, jossa voidaan pääsääntöisesti luottaa siihen, että ihmiset hoitavat vastuunsa ja tekevät, kuten on sovittu. Kaiken lisäksi turvallisuusviesti voidaan kommunikoida pehmeällä tavalla, eikä seuraamuksia painottamalla. Merkittävänä haasteena ovat globaalin yrityksen useat erilaiset toimintamaat, joiden paikalliset kulttuurit vaihtelevat suunnattomasti. Maailmassa on paljon maita, joissa ei voi luottaa siihen, että ihmiset noudattavat turvallisuusohjeita. Tämän johtuu monesti siitä, että ihmiset ovat tottuneet erilaiseen erilaiseen turvallisuusviestintään, osaltaan muodollisen turvallisuusviestin ja näkyvien kontrollien, esimerkiksi vartijoiden ja kameroiden muodossa. On hyvä huomioida, että esimerkiksi Suomessa on turha käyttää todella tiukkoja turvallisuusohjeita ja ylläpitää erittäin tiukkoja turvallisuuskontrolleita. Ihmiset kokevat, että turvallisuus on ylikorostettua suhteessa käytännön uhkiin ja lopettavat turvallisuusviestin kuuntelemisen.

Maailmassa on useita maita, joissa turvallisuusriskit liityvät pääosin ihmisiin liittyviin vaara-ja uhkatilanteisiin. Kyseisissä maissa, kuten esimerkiksi Meksikossa ei pystytä toimimaan globaalien turvallisuusohjeiden mukaisesti, mikäli niissä ei ole huomioitu maahan liittyviä turvallisuusriskejä. Tämä näkyy myös siinä, että Meksikossa on vaikeata saada ihmisiä ymmärtämään tietoturvallisuuden merkitystä, koska he eivät koe sitä yhtä tärkeäksi kuin henkilöturvallisuus. Luottamuksen käsite vaihtelee myös maittain. Suomessa voi hyvin luottaa siihen, että yrityksen uusi tuote pysyy piilossa, kun taas esimerkiksi Kiinassa on ihmisten mielestä oikein kertoa uudesta tuotteesta verkostolleen. Globaalissa yrityksessä toimiessa on tärkeää ymmärtää, että on erittäin vaikeaa rakentaa globaalia turvallisuuskulttuuria, koska ihmisillä on oma ymmärrys turvallisuudesta sekä siitä, mikä on oikein ja mikä väärin. Jos turvallisuuskulttuurin jalkauttaminen on haastavaa omassa globaalissa yrityksessä, niin kuinka haastavaa on levittää toivomaansa turvallisuuskulttuuria yhteistyökumppaniverkostolle ympäri maailmaa?

Kuvio 4: Useita erilaisia turvallisuuskulttuureita.

7.2.3 Turvallisuuskulttuuri yhteistyökumppaneiden kanssa toimittaessa

Kuten edellä mainittiin, niin Nokian turvallisuuskulttuuri perustuu siihen, että luotetaan fiksujen ihmisten huolehtivan turvallisuuteen liittyvistä vastuistaan. Luottamuksen osoituksena työntekijät allekirjoittavat salassapitosopimuksen, joka osaltaan sitoo heitä säilyttämään luottamuksellisuuden. Käytännössähän saman turvallisuuskulttuurin tulisi päteä, kun työskennellään yhteistyökumppaneiden kanssa. Kun vaadittavat sopimukset ovat voimassa, niin yhteistyökumppaniin voidaan luottaa ja heille voidaan jakaa hankkeeseen liittyvää luottamuksellista tai salaista tuotetietoa. Valitettavasti asia ei ole yleensä näin yksinkertaista. Ihmiset ajattelevat usein, että oman yrityksen työntekijöihin voidaan luottaa, mutta yhteistyökumppanin työntekijöihin taas ei, vaikka luottamus ja avoimuus olisivatkin keskeisiä tekijöitä yrityksen kulttuurissa. Näkisin, että taustalla on usein ennakkoluuloja ja yleistä epäluuloa eri kulttuureista tulevia yrityksiä ja ihmisiä kohtaan. Todella usein kuulee lausahduksia, että eihän siellä Kiinassa mikään pysy salassa tai että Venäjän mafia pyörittää kaikkea liiketoimintaa Venäjällä. Me turvallisuusyksikössä korostamme, että kumppaneihimme voi luottaa huolimatta siitä, mistä maasta he ovat kotoisin. Pyrimme myös avoimesti näyttämään ihmisille vuototilastoja, joista näkyy, että vuotoja tapahtuu myös omien työntekijöidemme toimesta ja että kaikki vuototapaukset eivät tapahdu Kiinassa, vaan niitä tapahtuu Suomessakin. Pyrimme avoimuudella pääsemään eroon kulttuureihin liitettävistä stereotypioista.

Yleensä yhteistyökumppanit eivät ole tasa-arvoisessa asemassa suhteessa heidän asiakasyritykseensä. Nokiassakin on usein ajateltu, että me seisomme jalustalla ja meillä on oikeus vaatia kaikenlaisia asioita kumppanieltamme. Toimivaa yhteistyötä on vaikeaa rakentaa, jos toinen osapuoli pitää itseään jalustalla ja pyrkii vain yksisuuntaiseen kommunikaatioon. Onneksi tällainen epäterve toimintakulttuuri on häviämässä. Suurimpana syynä tähän ovat liiketoiminnan haasteet, vähentyneen älypuhelinmyynnin muodossa. Kun liiketoiminta on pienempää, niin ei voi enää seisoa korkeammalla kuin muut, koska neuvotteluasetelmat ja riippuvuussuhteet ovat merkittävästi muuttuneet. Myös turvallisuusihmiset ovat pyrkineet luomaan turvallisuuskulttuuria muodollisesti eli pelkästään vaatimuksia kommunikoiden. Keskeisenä ajurina oli se, että mikäli haluat tehdä Nokian kanssa yhteistyötä, niin Nokian turvallisuusvaatimukset tulee olla paikoillaan, huolimatta sisällöstä ja sen soveltuvuudesta kohdeympäristöön.

Eroavaisuudet sisäisessä turvallisuuskulttuurissa ja tavassa tehdä yhteystyötä kumppanien kanssa ovat varsin mielenkiintoisia. Sisäisiin työntekijöihin luotetaan ja uskotaan heidän toimivan vastuullisesti sekä noudattavan vapaaehtoisesti turvallisuusohjeita. Yhteistyökumppaneihin taas ei luoteta, eikä uskota heidän kykenevän luomaan itsenäisesti riittävää turvallisuustasoa, mikä näkyy suurina vaatimusmäärinä. Nämä eroavaisuudet kulttuureissa korostuvat silloin, kun tarkastellaan vuototapausten seurauksia ja minkälaisia mahdollisia rangaistuksia niistä on seurannut. Mikäli olet sisäinen työntekijä ja laitat esimerkiksi julkaisemattoman tuotekuvan sosiaaliseen mediaan, niin saatat selvitä varoituksella. Mikäli yhteistyökumppanin työntekijä tekee saman rikkeen, niin seuraksena on yleensä ollut irtisanominen ja mahdolliset vahingonkorvaukset.

Mikäli halutaan oikeasti muuttaa maailmaa, niin yllä kuvattuja eroja ei saisi olla, koska ne ruokkivat eriarvoisuutta saman tiedon kanssa työskentelevien sisäisten ja ulkoisten sidosryhmien välillä. Henkilökohtaisesti olen lähtenyt tekemään muutosta Nokian sisällä, minkä tarkoituksena on luoda uudenlainen avoimempi ja luottamukseen perustuva turvallisuuskulttuuri Nokian ja yhteistyökumppaneiden välille. Keskeistä siinä on ollut avoin keskustelu ikävistäkin asioista ja sitä kautta yhteisten tavoitteiden asettaminen. Toistaiseksi alku on ollut lupaava ja toimintatapa on toiminut useissa liiketoimintaympäristöissä.

7.2.4 Johtopäätökset

On tärkeää, että ostajayritys laittaa panostaa oman sisäisen turvallisuuskulttuurinsa kehittämiseen, koska epäselvyys sisäisessä kulttuurissa vaikuttaa omien työntekijöiden turvallisuuskäyttäytymiseen. Yrityksen heikko turvallisuuskulttuuri heijastuu sen yhteistyökumppaneihin ja voi osaltaan edistää vääränlaisia ja turvattomia toimintamalleja.

On tärkeää ymmärtää, että yhteistyökumppanit tulevat erilaisista kulttuureista ja että yrityksen ja kumppanin turvallisuuskulttuureissa saattaa olla suuria eroja. Yhteistyökumppaneille tulisi viestiä selkeästi mitä yritys heiltä edellyttää, mikä tarkoittaa myös elämistä omien ohjeiden ja vaatimusten mukaisesti. Turvallisuustavoitteeseen pääsy vesittyy helposti, jos yhteistyökumppani huomaa, että yrityksen sanat ja käytännön toimet eroavat toisistaan. Tuotetietovuotojen ennaltaehkäisytyö on oiva mahdollisuus rakentaa yhteistä turvallisuuskulttuuria Nokian ja sen toimittajien välille. Molemmilla yrityksillä olisi yhteinen tavoite ja osittain yhtenevät turvallisuuskäytännöt siihen pääsemiseksi. Tämä takoittaisi käytännössä sitä, että molemmat ymmärtäisivät, että vuototapauksen toteutuessa, ei syytettäisi yritystä, mikäli tapaus olisi yksittäisen työntekijän tahallinen tai tahaton teko, koska parhaillakaan käytännöillä ei voida estää kaikkia vuotoja.

7.3 Sisäisiin sidosryhmiin liittyviä kehittämisalueita

Sisäisiä sidosryhmiä ovat kaikki ne Nokian liiketoimintayksiköt, joissa käsitellään julkaisematonta tuotetietoa ja työskentelevät yhteistyökumppaneiden kanssa. Näiden liiketoimintayksiköiden ne henkilöt, jotka työskentelevät yhteistyökumppaneiden kanssa, sisällytetään tämän sidosryhmään. Merkittävin sisäinen sidosryhmä on Nokian hankintayksikkö, joka vastaa hankinnoista ja yhteistyökumppanisuhteista. Hankinnoilla tarkoitetaan muunmuassa ohjelmistokehityksen alihankintaa, komponenttivalmistusta ja markkinoinnin alihankintaan. Muita merkittäviä sisäisiä sidosryhmiä ovat lakiyksikkö, joka vastaa sopimusmalleista, ja IT-yksikkö, jonka vastuulla on tietojärjestelmäyhteydet Nokian ja sen toimittajien välillä. Hankintayksikkö vastaa sopimusten tekemisestä ja monissa tapauksissa yhteistyökumppanisuhteen ylläpitämisestä. Liiketoimintayksiköt taas työskentevät kumppanien kanssa ja päättävät siitä millaista tuotetietoa kanssa jaetaan. Turvallisuusyksikön tehtävänä on tukea edellä mainittuja sidosryhmiä, mikä tapahtuu muun muassa sopimusvaatimuksia luomalla, konsultoimalla ja yhteistyökumppaneita auditoimalla.

Sisäiset sidosryhmät ovat pääosin edellyttäneet, että sopimusasiat Nokian ja yhteistyökumppanin välillä ovat kunnossa. Käytännössä salassapitosopimuksen olemassa olo on usein koettu riittäväksi tavaksi suojata tuotetietoa. Turvallisuusvaatimukset, niiden vieminen sopimukseen ja yhteistyökumppanin turvallisuustason tarkastaminen eli auditointi ovat olleet usein osa toimintaa. Kuitenkin toiminnasta on puuttunut järjestelmällisyys, mikä tarkoittaa sitä, että joissakin tapauksissa turvallisuusvaatimukset ovat sopimuksissa ja yhteistyökumppanin turvallisuustaso on auditoitu, kun taas toisissa tapauksissa tätä ei ole tehty. On jopa tapauksia, joissa edes salassapitosopimusta ei ole tehty toimittajan kanssa. Tämä kertoo siitä, että työntekijöiden keskuudessa on turvallisuustietoisuuden puutetta ja joissakin tapauksissa jopa välinpitämättömyyttä. Niissä tapauksissa, joissa turvallisuusvaatimukset on saatu sopimukseen ja yhteistyökumppanin turvallisuustason on

auditoitu, ilo on usein jäänyt lyhytaikaiseksi. Yhteistyökumppani on rakentanut turvallisuustasonsa asiakkaan vaatimalla tavalla, mutta tasoa ei ole ylläpidetty tai kehitetty riskienhallinnan keinoin. Tämä on johtunut siitä, että yhteistyökumppani ei ole kokenut asiaa tärkeäksi, koska asiakas ei ole korostanut asiaa sopimuksen tekemisen jälkeen. On myös paljon tapauksia, joissa turvallisuusyhteistyö on ollut toimivalla tasolla, mikä osaltaan on pienentänyt vuotoriskiä ja vähentänyt turvallisuusepäkohtia. Turvallisuusyksikölle on raportoitu tapauksista, joissa Nokian liiketoimintayksikön työntekijä on kehottanut toimittajan työntekijää olemaan noudattamatta esimerkiksi prototyyppien käsittelyohjeita. Tämäkin havainto kertoo siitä, että turvallisuuskulttuuri ei ole ollut oikealla tasolla.

Turvallisuusyksikkökin on viime vuosina tyytynyt osaansa toimia turvallisuusvaatimusten ylläpitäjänä ja yhteistyökumppaneiden turvallisuustason tarkastajana. Auditoinnit ovat pohjautuneet sopimusvaatimuksiin ja pääsiassa keskittyneet fyysisen ympäristön, kuten kumppanin toimiston turvallisuustason katselmointiin. Yhteistyökumppaniverkoston turvallisuustyössä on usein puuttunut liiketoiminnan ja siihen liittyvien arvokkaiden tuotetietojen ymmärtäminen, mikä on johtanut epäoleellisiin vaatimuksiin ja väärin kohdistettuihin turvallisuusauditointeihin. Viime vuosien havaintojen perusteella voidaan todeta, että tuotetietovuotoja yhteistyökumppaniverkostossa ei voida ennaltaehkäistä pelkästään perinteisellä muodollisella ja sopimusvaatimuksiin perustuvalla jalkauttamistavalla sekä yhteistyökumppanien turvallisuustason auditoinneilla. Hyvin käytettynä ne luovat tarvittavan perustan, mutta eivät sellaisenaan riitä pienentämään riskejä nykyisessä globaalissa ja nopeasti muuttuvassa maailmassa.

7.3.1 Havaintoja tietovuotojen ennaltaehkäisytyöstä yhteistyökumppaniverkostossa

Tässä kappaleessa esitettävät asiat pohjautuvat vuosina 2010-2012 tehtyihin havaintoihin. Tuotetietovuotojen määrä yhteistyökumppaniverkostossa on kasvanut viime vuosina. Syinä tähän ovat olleet turvallisuustietoisuuden puute, laajentunut internetin ja sosiaalisen median käyttö toimittajien työntekijöiden keskuudessa, huolimattomuus, puutteet turvallisuusjärjestelyissä, tahallinen vuotaminen henkilökohtaisessa hyötymistarkoituksessa, sekä turvattomien prosessien ja työkalujen käyttö. Taustalla on ollut julkaisemattoman tuotetiedon kysyntä teknologiabloggereiden keskuudessa sekä erittäin aktiivinen kirjoittelu ja huhujen levittely internetissä. Yritysvakoilun merkitystä varhaisen vaiheen tuotetiedon häviämisessä ei voida jättää huomioimatta, mutta sen olemassa olosta ei useinkaan jää jälkiä, vaikka sitä esiintyykin.

Yhteistyökumppaniverkoston turvallisuuden ylläpitämiseen käytetyt toimenpiteet ovat olleet pääsääntöisesti sopimusvaatimuksia ja niiden noudattamisen seuraamista toimittajia auditoimalla. Tosin havaintojen perusteella voidaan todeta, että edellä mainitut toimenpiteet

eivät ole olleet käytössä kaikkien kumppaneiden kanssa ympäri maailmaa. Toimenpiteet ovat pitäneet sisällään salassapito- ja tuotelainasopimukset, turvallisuusvaatimusten liittämisen sopimuksiin ja yhteistyökumppanin turvallisuusauditoinnin. Turvallisuutta on siis hoidettu tavalla, jossa vahvempi osapuoli määrittää tason, joka ei ole neuvoteltavissa, koska se on määritelty sopimuksessa. Yhteistyökumppanit ovat siis jalkauttaneet turvallisuutta, koska se on ollut asiakkaan tahto. Usein tämän tyyppinen toimintatapa ei johda hyviin tuloksiin, koska ihmiset ja yritykset eivät yleensä sitoudu pakottamalla ja oikeasti ymmärtämättä, miksi jonkin asian tekeminen on tärkeää.

Sopimusvaatimuksiin pohjautuvalla jalkauttamistavalla voidaan esimerkiksi turvata jokin fyysinen ympäristö, mutta niillä on vaikeaa turvata prosesseja. Sopimusvaatimukset ovat yleensä melko yleisellä tasolla, eivätkä ne siten ota käytännön tasolla kantaa, miten toimittajan työntekijän tulee käsitellä arvokasta tietotietoa ja miksi näin tulee tehdä. Sopimusvaatimukset ohjaavat yhteistyökumppanit jalkauttamaan yhdellä tavalla, oikeasti ajattelematta, että voisi olla järkevämpiäkin toiminpiteitä turvata tuotetietoa heidän toimintaympäristössään. Toisin sanoen sopimusvaatimukset saattavat ohjata yhteistyökumppanit jättämään riskit arvoimatta ja kulkemaan tekemään vain asiakkaan toivomalla tavalla. Riskien arvioinnin puute saattaa helposti johtaa siihen, että ei huomata toimintakentän riskien muuttuneen ja sitä, että sopimuksessa oleva edellytettävä turvallisuustaso ei olekaan enää riittävä. Sopimusvaatimukset päivitetään usein jälkijunassa, eikä pelkästään niitä seuraamalla päästä useinkaan optimaaliseen lopputulokseen. Maailma on muuttunut nopeasti, mutta Nokian toimintatapa turvallisuuden jalkauttamisessa yhteistyökumppaniverkostossa ei, mikä taas on johtanut tuotetietovuotojen määrän kasvuun.

7.3.2 Turvallisuusviestin jalkauttaminen yhteistyökumppaniverkostossa

Turvallisuusviesti on pääsääntöisesti jalkautettu muodollisesti salassapitosopimuksella ja yleisillä vaatimuksilla. Käytännössä katsoen yhteistyökumppanille on kommunikoitu, että edellytämme, että suojaatte arvokasta tietoamme asianmukaisella tavalla. Tämän lisäksi edellytämme, että turvallisuustasonne on riittävällä tasolla. On ollut täysin yhteistyökumppanista kiinni, että miten hyvin he ovat viestin ymmärtäneet ja millaisia vaikutuksia sillä on ollut. Viesti ei ole yleensä koskaan saavuttanut niitä yhteistyökumppanien työntekijöitä, jotka käsittelevät arvokasta tietoa päivittäin, yhteistyökumppanin alihankkijoista puhumattakaan. Viesti on siis ollut todella yleisellä tasolla, eikä se ole yleensä saavuttanut oikeaa kohderyhmää. Toki joitain poikkeuksiakin on ollut. Mikäli kumppanilla on ollut toimiva turvallisuuskulttuuri ja sen henkilökunnan turvallisuustietoisuutta on kehitty jatkuvasti.

7.3.3 Hankintaprosessi

Vahinkoriskien arviointi ei ole ollut osana hankintaprosessia. Ei ole riittävällä tavalla arvioitu, että millaista arvokasta tuotetietoa yhteistyökumppanille tullaan antamaan, jotta he voivat tuottaa Nokialle lisäarvoa. Ei ole myöskään selvitetty riittävällä tavalla, että ketkä osapuolet työn oikeasti tekevät eli käyttääkö kumppani omia alihankkijoitaan työn tekemiseen. Riittävän riskitietoisuuden puute on tarkoittanut sitä, että turvallisuusvaatimukset ovat puuttuneet osasta yhteistyösopimuksista, eikä oikeastaan mitään ennaltaehkäiseviä toimenpiteitä ole tehty. Riskitietoisuuden puute on tarkoittanut myös sitä, että Nokian edustaja ei ole osannut kertoa yhteistyökumppanille, että se tulee saamaan käsiinsä erittäin arvokasta tietoa ja että sitä tulee käsitellä huolellisesti. Yhteistyökumppani on saattanut saada sellaisen käsityksen, että tärkeintä on toimittaa tuotos ajallaan, eikä niin hirveästi haittaa, jos tietoa lipsahtaa ulkopuolisille. Tietovuotojen ennaltaehkäisyyn liittyvät asiat eivät ole olleet kriteereinä kumppaneita valittaessa, koska asia ei ole noussut esiin sisäisissä riskiarvioinneissa.

7.3.4 Liiketoimintayksiköiden työskentely yhteistyökumppaneiden kanssa

Liiketoimintayksiköiden tavat työskennellä ja jakaa tietoa yhteistyökumppaneiden kanssa ovat vaihdelleet kovasti. Toimintatavat ovat vaihdelleet henkilöittäin, mutta on ollut myös paljon liiketoimintakohtaisia eroja. Tuotekehityksessä työskentelevät ihmiset ovat olleet hieman valveutuneempia kuin markkinoinnissa työskentelevät ihmiset. Tässä näkyy selkeästi liiketoimintakohtaiset kulttuurierot. Tämä näkynyt muun muassa siinä, että markkinointi-ihmiset ovat yleensä antaneet yhteistyökumppaneille vapaat kädet sille, miten luottamuksellista tietoa lähetetään paikasta toiseen. On ennemminkin käytetty kumppanin tietojärjestelmiä tai kumppanin suosimia ilmaisia ja internet-pohjaisia tiedonjakamismenetelmiä. Olemme havainneet myös tapauksia, että liiketoimintayksiköt ovat tehneet yhteistyötä kumppanin kanssa, ilman kunnollisen sopimuksen olemassaoloa. Tämä on tarkoittanut sitä, että tiedon suojaamiseen liittyviä asioitakaan ei ole käyty läpi kumppanin kanssa.

7.3.5 Johtopäätökset

Nokian toiminta on perustunut muodollisille kontrolleille, jotka käytännössä jalkautettu sopimusten ja vaatimusten muodossa. Tämän jälkeen yhteistyökumppanin turvallisuuskyvykkyys on auditoitu, minkä jälkeen turvallisuus tai tietovuotojen ennaltaehkäisyasiat eivät ole olleet agendalla, kun osapuolet ovat olleet tekemisissä keskenään. Luonnollisesti poikkeavia toimintatapojakin on ollut, mutta pääosin toiminta on

ollut kuvaamallani tasolla. Hankintaprosessiin ei ole liitetty vahinkoriskien arviointi, mikä on tarkoittanut, että Nokian sisällä ei ole ollut riittävää ymmärrystä yhteistyöhön liittyvistä riskeistä, mikä on osaltaan näkynyt suojaustoimenpiteiden riittämättömyytenä. Auditointeja on tehty, mutta ne on toteutettu varsin yleisellä tasolla, eikä yhteistyökumppanin prosesseja on katselmoitu riittävällä tavalla. Turvallisuusviestintäkin on toteutettu muodollisella tavalla salassapitosopimuksiin ja yleisiin turvallisuusvaatimuksiin tukeutumalla. Viestin sävykin on vaihdellut todella tiukasta olemattomaan eli yhtenäisyys on puuttunut. Viestistä ovat yleensä puuttuneet vastaukset keskeisiin ihmistä motivoiviin kysymyksiin eli mitä tämä tarkoittaa, miksi tämä on tärkeää ja miten minun tulee toimia käytännössä.

Hankintayksikön ja muiden sisäisten sidosryhmien turvallisuustietoisuuden taso ei ole riittävällä tasolla. On ollut paljon yksittäisiä ihmisiä, joiden osaaminen on ollut riittävällä tasolla, mutta keskimäärin tietoisuus on ollut heikkoa. Tämä on näkynyt turvallisuustoimenpiteiden laiminlyönteitä tai puutteellisina toteutuksia. Ei ole myöskään ymmärretty omaa roolia ja vastuita turvallisuusasioissa.

7.4 Yhteistyökumppanit

Yhteistyökumppanit tulevat lukuisilta liiketoiminta-alueilta, joista suurimmat ovat markkinointi, ohjelmisto- ja sovelluskehitys, komponenttien kehittäminen ja valmistus, testaus, käyttöliittymäsuunnittelu, sopimusvalmistus ja käyttöohjeiden luominen. Nämä yritykset tulevat lukuisista maista, joista merkittävimmät ovat Kiina, Intia, Iso-Britannia, Yhdysvallat, Suomi ja Taiwan. Edellä mainittujen lisäksi yhteistyökumppaneita sijaitsee kymmenissä maissa, mikä tarkoittaa toimimista lukuisien eri kansallisuuksien ja kulttuurien parissa.

Yhteistyökumppaneiden koko ja toiminta-alueet vaihtelevat laidasta laitaan. On pieniä ja paikallisia, vain muutamia henkilöitä työllistäviä yrityksiä ja suuria globaalisti toimivia yrityksiä, joilla on kymmeniä tuhansia työntekijöitä. Näiden yritysten turvallisuuskulttuuri, osaaminen ja siihen käytettävissä olevat resurssit vaihtelevat suuresti. Yleensä suurilla yrityksillä on oma turvallisuusorganisaationsa ja riittävästi resursseja käytettävissä turvallisuuden jalkauttamiseen ja asiakasvaatimusten käytännön toteuttamiseen, kun taas pienemmillä yrityksiltä puuttuvat resurssit ja riittävä turvallisuusasioiden osaaminen. Tuotetietovuotojen ennaltaehkäisy yhteistyökumppaniverkostossa ei ole kuitenkaan resurssikysymys. Sitoutumisaste on paljon tärkeämpää. Suuret yritykset eivät läheskään aina sitoudu kunnolla asiakkaan vaatimuksiin ja toiveisiin, koska yhden vahinkoriskin toteutuminen ei vaikuta merkittävästi heidän liiketoimintaansa. Tämän lisäksi he tietävät, että asiakas ei pysty irtautumaan heistä kovinkaan nopeasti. Pienillä yrityksellä taas sitoutumisen aste on yleensä suurempi, koska heidän liiketoimintansa on riippuvaisempi suuresta asiakkaasta kuin

suuren yrityksen. Pienten yritysten osalta osaamisen ja resurssien puute saattaa taas estää heitä toteuttamasta asiakkaiden toiveita turvallisuuden suhteen. Osa yhteistyökumppaneista saattaa myös jättää kertomatta totuuden heidän turvallisuuskyvykkyydestään tai jonkin epäkohdan toteutumisesta, koska pelkäävät liiketoimintamahdollisuuden menettämistä.

Yhteistyökumppaneille tekemämme auditoinnit ovat osoittaneet, että useilla yrityksillä on puutteita niiden turvallisuuskyvykkyyksissä. Useiden yhteistyökumppaneiden työntekijät eivät osaa käsitellä julkaisematonta tuotetietoa asianmukaisella tavalla, mikä on näkynyt turvattomina tapana siirtää tietoa paikasta toiseen. Syynä tähän on usein yhteistyökumppanin heikko panostus turvallisuustietoisuuden lisäämiseen. Olemme havainneet puutteita prototyyppien säilytys ja inventaariokäytännöissä. Käytännössä tämä on tarkoittanut sitä, että laitteita ei ole säilytetty niille tarkoitetulla suojatulla alueella. Inventaario ei ollut läheskään aina ajantasalla, eikä vastuuhenkilö ole tiennyt laitteiden olinpaikkaa. Toimitilaturvallisuusjärjestelyissäkin on löydetty haavoittuvuuksia, mikä on tarkoittanut käytännössä sitä, että Nokian projektialueelle on päässyt henkilöitä, joilla ei ole oikeutta eikä tarvetta oleskella siellä. Yhtenä syynä näille puutteille on ollut Nokia tapa olla ylläpitämättä säännöllistä turvallisuuskeskustelua yhteistyökumppanin kanssa. Keskustelun puute on osaltaan vaikuttanut kumppanin motivaatioon ylläpitää ja kehittää riittävää turvallisuuskyvykkyyttä.

7.4.1 Johtopäätökset

Yhteistyökumppanit tulevat eri maista ympäri maailmaa ja heidän taustoillaan on erilaista liiketoimintaa komponenttivalmistuksesta tuotepakkausten valmistukseen. Yhteistyökumppaneiden turvallisuuskyvykkyys ja motivaatio toimia Nokian toivomalla tavalla vaihtelevat kovasti. Keskeisenä puutteena yhteistyökumppaneiden turvallisuuskyvykkyyksissä on turvallisuustietoisuuden heikko taso, mikä puolestaan näkyy vuototilastoissa ihmisten tekeminä virheinä ja huolimattomuutena. Olemme havainneet myös usein, että yhteistyökumppanin turvallisuusohjeistukset ja koulutusmateriaalit ovat todella yleisellä tasolla, eivätkä sisällä tämän päivän keskeisiä turvallisuusasioita, kuten sosiaaliseen mediaan ja internetin käyttöön liittyvät pelisäännöt. Tuotetietovuotojen ennaltaehkäisytyössä tulee panostaa yhteistyökumppaneiden turvallisuustietoisuuden kehittämiseen ja hyvien ennaltaehkäisykeinojen kommunikoimiseen.

7.5 Tuotetietovuotojen ennaltaehkäisyyn liittyviä kulttuurisia ja viestinnällisiä haasteita globaalissa yhteistyökumppaniverkostossa

Tämän osion ei tarvitsisi olla osa opinnäytetyötäni, koska täydellinen teoreettinen perusta puuttuu. Aineisto on osa yritykselle tehtyä nykytila-analyysiä ja siten osa tätä työtä.

Allaolevat kappaleet perustuvat pelkästään allekirjoittaneen tekemiin käytännön havaintoihin työskennellessäni Nokian yhteistyökumppaniverkoston kanssa.

Nokia tekee yhteistyötä useilta eri liiketoiminta-alueilta tulevien kumppanien kanssa. Turvallisuusviestinnässä on tärkeää huomioida, että turvallisuuden merkitys vaihtelee eri liiketoiminta-alueiden välillä. Tämän asian sisäistäminen on yhtä tärkeää, kuin eri maiden kulttuurien ymmärtäminen. Tehtaissa ja valmistusteollisuudessa turvallisuus ymmärretään osana tuotantoprosessia, joka osaltaa varmistaa toiminnan häiriöttömyyttä. Tuotekehitystä tekevissä yrityksissä ymmärretään yleensä luottamuksellisuuden merkitys, koska niissä luodaan asioita, joita maailma ei ole vielä nähnyt. Luovilla aloilla, kuten muotoilupuolella ja markkinoinnissa ei kovinkaan hyvin ymmärretä turvallisuuden merkitystä, koska molempien tavoitteena on näyttää aikaansaannoksensa mahdollisimman monille ihmisille. Muutenkaan luovilla aloilla ei yleensä pidetä rajoitteista, koska niiden koetaan haittaavan toimintaa ja estävän innovaatioita.

Lakimiestenkin näkökulma on tärkeää ymmärtää, koska he ovat vahvasti mukana kaikessa toiminnassa. Lakimiehet näkevät turvallisuuden lainsäändäntövaatimusten ja sopimusvaatimusten näkökulmasta. Kunhan toimintamme on vaatimusten mukaista, niin asia on kunnossa. Eroavaisuudet liiketoiminta-alueiden turvallisuusajattelussa asettavat suuria haasteita tuotetietovuotojen ennaltaehkäisytyölle, koska yhdenlainen turvallisuusviesti ei vältämättä toimi yhtä hyvin kaikilla liiketoiminta-alueilla. Ajatellaampa vaikka, että laitetaan lakimies ensin luomaan ja sitten jalkauttamaan viestin jollekin luovan alan yritykselle. Viesti sisältäisi turvallisuusohjeen ja viittauksen lakiin, sekä listan sanktioista joita ohjeen noudattamatta jättämisestä seuraisi. Toimisiko tällainen viesti luovan alan yrityksen kanssa? Todennäköisesti tulokset eivät olisi kovinkaan hyviä, koska viestin sisältö ja oloasu eivät välttämättä toimisi kohdeympäristössä. Liiketoimintakulttuurin tuntemus on erittäin tärkeää turvallisuutta jalkautettaessa.

Jokainen ihminen on erilainen ja jokaisella on omanlaisensa käsitys mikä on oikein ja mikä väärin. Ihmiset kokevat samat asiat eri tavalla. Tämä tulee huomioida turvallisuutta kommunikoitaessa. Osa ihmisistä oppii lukemalla, osa oppii kuuntelemalla ja osa taas kuvia katsomalla. On tärkeää ymmärtää, että globaalin yhteistyökumppaniverkostomme lukuisten yritysten työntekijät ovat yksilöitä, joilla on erilaiset tarpeensa ja käsityksensä turvallisuudesta. On myös turha kuvitella, että kaikki ihmiset muuttavat toimintaansa hyvin kommunikoidun turvallisuusohjeen mukaisesti. Suurin osa ihmisistä haluaa toimia oikein ja noudattaa turvallisuusohjetta. Osa ihmisistä taas saattaa laiminlyödä ohjeen, jos tietää että kiinnijäämisen riski on pieni. Tällaista käytöstä kuvataan usein lauseella, että tilaisuus tekee varkaan. Sitten on ihmisiä, jotka ovat syystä tai toisesta vihaisia työnantajalleen ja haluavat tämän vuoksi tehdä vahingollisia tekoja. Tällaiset epälojaalit toimet nousevat esiin

esimerkiksi yritysten irtisanoessa paljon ihmisiä. Kaksi muuta ihmiskategoriaa ovat rikolliset ja henkilöt jotka elävät sosiaalisten normien ulkopuolella. Rikolliset pyrkivät yleensä kaikin keinoin kiertämään turvallisuusohjeet ja sosiaalisten normien ulkopuolella elävät ihmiset tekevät asiat omalla tavalla, mistään ohjeista riippumatta. On hyödyllistä tiedostaa erilaisten käyttäytymismallien olemassaolo, koska sen avulla ymmärtää, että yhdellä menetelmällä ei voida jalkauttaa turvallisuutta ympäristössä, joka pitää sisällään eri motiiveilla ja taustoilla olevia ihmisiä.

Ihmisillä on yrityksissä erilaisia rooleja ja vastuualueita. Tietty rooli saattaa tuoda mukanaan tietynlaisen tavan suhtautua turvallisuuteen. Johtajilla ei ole yleensä halua mennä yksityiskohtaisiin ja käytännön tason turvallisuusasioihin. Heitä sattaa kiinnostaa lähinnä se, että asiat tulevat tehdyksi, ilman että heitä vaivataan asialla. Yleensä yhteistyökumppaniyrityksen johto haluaa, että heidän turvallisuustoimenpiteensä ovat Nokian vaatimusten mukaiset ja että heidän liiketoimintansa on mahdollisemman häiriötöntä. Työntekijät taas odottavat johdon kommunikoivan heille turvallisuudelle asetetut tavoitteet. Tämän lisäksi työntekijöille on kerrottava, mitä heiltä käytännössä edellytetään, ja miten toimimalla he pääsevät tavoitteeseen. Tavoitteeseen pääsemisen jälkeen he odottavat yleensä jonkinlaista palkintoa.

Työntekijätasolle on tyypillistä, että tehdään vain välttämätön, mutta ei mitään ylimääräistä. Toisaalta hyvällä motivoinnilla voidaan vaikuttaa tähän asenteeseen. Viestintää suunniteltaessa ei aina huomioida erilaisia rooleja ja heidän tarpeitaan. Turvallisuusviestissä tulisi aina korostaa, miksi on tärkeää toimia tietyllä tavalla ja miten yksilön tulee toimia päästäkseen tavoitteeseen. Toimittajien kanssa työskenneltäessä ei yleensä panosteta siihen, että huolehdittaisiin siitä, että toivottu turvallisuusviesti jalkautetaan lattiatasolle asti. Mikäli hyvä aikomus jää vain johdon pöydälle, ei viestin sisältö konkretisoidu käytännön toiminnaksi, eikä osaltaan edistä turvallisuustavoitteeseen pääsemisessä.

Kielellä on suuri merkitys turvallisuusviestin onnistuneeseen jalkauttamiseen. Globaalissa ympäristössä käytetään englantia, joka on myös Nokian sisäinen kieli. Englannin kieltä käytetään pääasiallisesti yhteistyökumppaneiden kanssa työskennellessä. Kumppaneille tarkoitetut ohjeistukset ja koulutusmateriaalit on kirjoitettu englanniksi. Keskeisimpänä kielellisenä haasteena näen sen, että suurin osa turvallisuusohjeiden kohderyhmän ihmisistä eivät ole syntyperäisiä englanninkielen puhujia. Tämä tarkoittaa sitä, että kaikki lukijat eivät välttämättä ymmärrä ohjeiden sisältöä. Kohderyhmässä on myös henkilöitä, jotka eivät puhu ollenkaan englantia. Usein ohjeen luojakaan ei ole natiivi englannin puhuja, mikä saattaa näkyä viestin sisällön köyhyytenä.

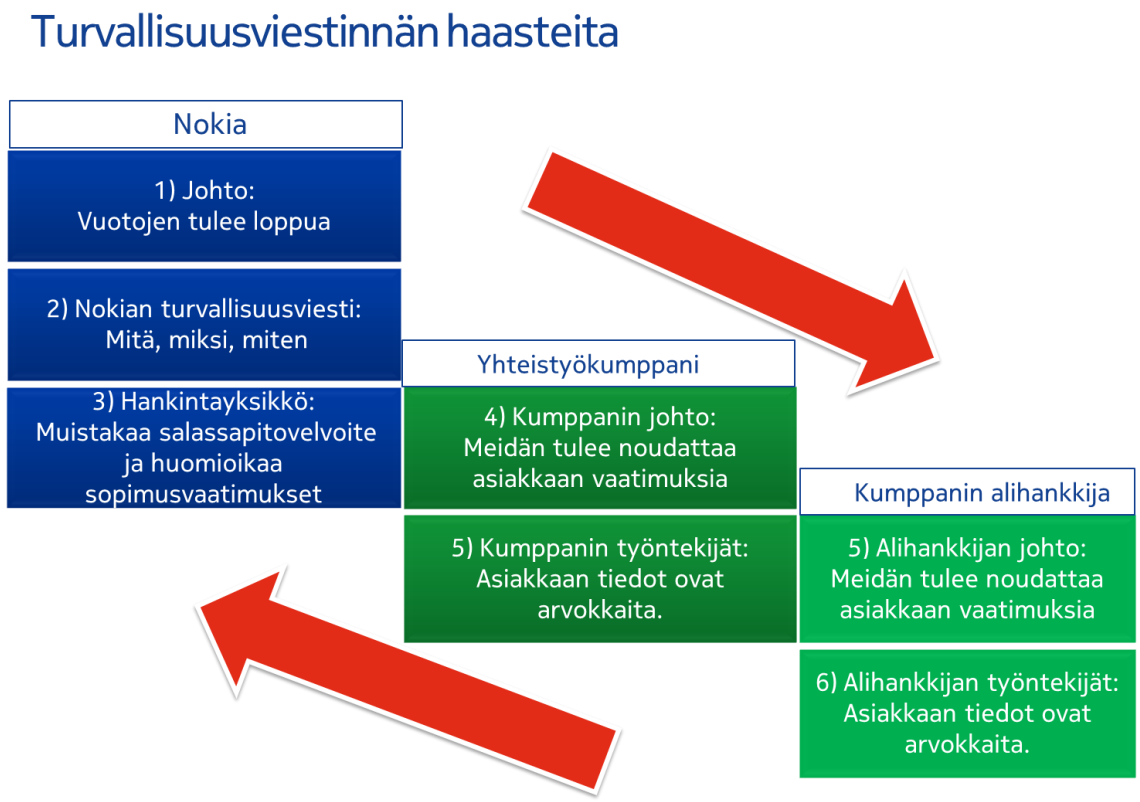
Turvallisuusalalla on omia ammattitermejä, joita me turvallisuusihmiset tapaamme käyttää erilaisissa ohjeistuksissa, jotka on tarkoitettu muille kuin turvallisuusasiantuntijoille. Ammattitermit saattavat vaikeuttaa viestin ymmärtämistä. Yritysten sisällä saattaa olla käytössä firman sisäisiä kieliä, jotka sisältävät suuria määriä lyhenteitä, joita ulkopuolisen on mahdotonta ymmärtää. Turvallisuusviesti on usein osana sopimusta, esimerkiksi vaatimusten muodossa. Tämä teksti on yleensä lakimiesten kirjoittamaa kankeaa, lakitekstin tyyppistä kirjoitusta, josta muiden ammattiryhmien on vaikea ottaa selkoa. Aikaisemmin turvallisuusviestimme jalkautettiin pääosin sopimustekstimuodossa, mutta se ei tuottanut riittävää tulosta. Syynä tähän oli viestin kompleksisuus ja jalkauttamismenetelmä, joka ei koskaan vienyt sitä lattiatasolle, jossa Nokian arvokkaita tuotetietoja käsiteltiin.

Viestiminen tapahtuu usein virtuaalisesti puhelimella tai virtuaalikokousten ja koulutusten muodossa. Tämä asettaa suuria haasteita viestinnälle, koska näissä tapauksissa viestintä perustuu puhutulle kielelle ja mahdollista esitystä varten tehdyille kalvoille. Tekniset ongelmat ja heikko äänenlaatu saattavat osaltaan heikentää viestin läpimenoa. Kehonkieltäkään ei pystytä hyödyntämään riittävästi. Nämä haasteet tarkoittavat käytännössä sitä, että ellei viesti ole todella yksinkertainen, niin ei voi edellyttää sen menevän läpi.

Globaalissa yhteistyökumppaniverkossa on lukuisia eri kerroksia, joiden läpi turvallisuusviestin tulee uida. Turvallisuusyksikön haasteena on varmistaa yhtenäisen viestin läpimeno oikeisiin paikkoihin ja osaltaan viestin ymmärtämisen varmistaminen. Seuraava esimerkki kuvaa tätä haastetta. Turvallisuusviesti lähtee yrityksen johdosta, joka tässä tapauksessa sanoo, että tuotetietovuotojen on loputtava. Tämä viesti tulee turvallisuusyksikköön, jossa viestiin lisätään, miksi vuotojen ennaltaehkäisy on tärkeää ja mitä toimittajan työntekijän tulee käsitellä Nokian tuotetietoa. Tämän jälkeen viesti menee hankintayksikköön ja lakiosastolle, jotka muuttavat viestin sopimustekstiksi. Nyt viestin sisällön mukaan yhteistyökumppanin tulee suojata Nokian tuotetietoa. Tämän jälkeen alkavat neuvottelut, joissa viesti kommunikoidaan kumppanin johdolle. Yhteistyökumppaniyrityksen johdon suusta tuleva viesti kertoo, että Nokia vaatii meitä suojaamaan tieto-omaisuuttaan. Tämän jälkeen viesti kommunikoidaan niille työntekijöille, jotka tulevat työskentelemään Nokian projektissa. Heille viesti kertoo, että asiakastiedon suojaaminen on tärkeää. Useissa tapauksissa ketjuun voidaan liittää vielä yhteistyökumppanin käyttämät alihankkijat ja heidän mahdolliset alihankkijansa, joilla saattaa olla pääsyoikeus projektissa käsiteltävään Nokian arvokkaaseen tuotetietoon. Ketjun kaukaisimmassa päädyssä viesti saattaa olla jo heikentynyt ja jopa menettänyt merkityksensä.

On äärimmäisen haastavaa pystyä viemään tärkeä viesti useiden kerrosten läpi kaikkiin niihin paikkoihin, joissa tietoa tarvitaan. Mikäli tähän ei pystytä, niin ei välttämättä saada aikaa toivottua vaikutusta ja muutosta asenteisiin. Mielestäni tämän viestinnällisen haasteen

ratkaisemisellä on keskeinen rooli tuotetietovuotojen ennaltaehkäisytyössä yhteistyökumppaniverkostossa.



Kuvio 5: Viestinnän jalkauttamisen haasteita yhteistyökumppaniverkossa

Turvallisuusviestin läpimenon esteenä on useita potentiaalisia häiriötekijöitä. Osa näistä tekijöistä ovat kulttuurisidonnaisia ja osa liittyy ihmisten perustarpeisiin. Kiinalaisissa yrityksissä on ollut paljon haasteita työolosuhteiden kanssa ja ihmiset ovat esimerkiksi kapinoineet Foxconnin tehtailla. Jos työntekijät eivät ole tyytyväisiä työnantajaansa ja kapinoivat pihalla, niin on aivan turha olettaa, että he omaksuisivat uusia turvallisuuskäytäntöjä. Ihmisen perustarpeet tulee olla tyydytettyinä ennen kuin turvallisuusviestiä kannattaa lähteä viemään yhteistyökumppanin työntekijöille. Kulttuurisidonnaisina häiriötekijöinä voidaan pitää sellaisia asioita, jotka mahdollisesti loukkaavat paikallista kulttuuria. On paljon maita, joissa miesten edellytetään toimivan viestinviejinä. Monesti nainen saattaisi olla parempi asiantuntija viestin kommunikoimisesssa, mutta jossain maissa hänen esiintymisensä saattaisi aiheuttaa häiriön, ja siten estää viestin läpimenon.

Kuva 1: Foxconnin kiinalaiset työntekijät protestoivat huonoja työoloja vastaan (Cristi Li, 2013).

Internet on tuonut mukanaan paljon hyviä asioita, kuten pääsyn suureen määrään tietoa ympäri maailmaa ja mahdollisuuden viestiä ulkomaisten ihmisten kanssa. Internet on kulttuurina varsin nuori, joten sen käyttöä ohjaavat pelisäännötkään eivät ole täysin kypsiä. Länsimaissa ollaan pisimmällä internetin käytön pelisäännöissä ja niiden jalkauttamisessa. Tämä näkyy hyvin vuototilastoissa. Maat, joissa internetin käyttö on vielä varsin uusi asia, tapahtuu paljon tietovuotoja toimittajien työntekijöiden toimesta. Nämä vuodot johtuvat pääosin siitä, että ihmiset eivät ymmärrä tekevänsä väärin, koska heille ei ole kommunikoitu internetin ja sosiaalisen median käytön pelisääntöjä. Taustalla on myös verkoston antama paine, joka ohjaa ihmisiä tekemään väärin. Internetkulttuuri on todella suuri haaste tuotetietovuotojen ennaltaehkäisytyölle, koska internetin kautta vuotaminen on helppoa, eikä taitavia vuotajia voi saada kiinni.

7.5.1 Johtopäätökset

Turvallisuusviestin vieminen kansainväliseen ja monikulttuuriseen yhteistyökumppaniverkostoon ei ole helppoa, koska viestijän tulee ymmärtään viestinnän kohteen kulttuuria, pystyäkseen saamaan viestinsä muuttamaan ihmisten käyttäytymistä ja toimintaansa. Viestintää suunniteltaessa on tärkeää analysoida kohdeympäristön monet eri viestintään vaikuttavat tekijät, ennen itse viestinnän jalkauttamista. On myös tärkeää huomioida, ovatko kohteen ihmiset valmiita vastaanottamaan viestin ja mikä on oikea viestintätapa, jotta viesti menee oikeille henkilöille. Yrityksen sisällä on tärkeää sopia, että kuka toimii viestijänä ja että viestin sisältö on yhtenäinen. On tärkeää, että viestinnän aikana

mahdollistetaan vuorovaikutus, koska muuten turvallisuusviesti saattaa kuulostaa muodollisilta vaatimuksilta ja pakolta toimia jollain tietyllä tavalla. On selvää, että liian muodollisella viestillä ei pystytä nostamaan ihmisten motivaatiota toimia turvallisella tavalla. Turvallisuusohjeiden sisältöä mietittäessä on tärkeää huomioida kohdeympäristön liiketoiminta-alue ja räätälöidä sisältö heille sopivaksi. Tämä saa viestinnän kohteen ymmärtämään, että viestijä ymmärtää hänen työtään ja näin viesti otetaan yleensä paremmin vastaan. Olemme saanut tuosta menetelmästä hyviä kokemuksia Nokian sisäisessä turvallisuusviestinnässä.

8 Tutustuminen erilaisiin tiedonsuojaamiskeinoihin ja jalkauttamismenetelmiin.

Tässä osiossa pyritään löytämään teoriasta ja käytännöstä tuotetietovuotojen ennaltaehkäisyyn soveltuvia kontrolleja ja menetelmiä. Teoriapohjana on muutavia soveltuvia tieteellisiä julkaisuita ja kaksi kansainvälisesti tunnettua tietoturvallisuusstandardia. Käytännön menetelmistä esiin nostetaan Nokian käytössä olevia menetelmiä.

8.1 ISF:n The standard of good practice ja ISO 17999

ISF (2012, 48-59) korostaa, että yrityksellä tulee olla ohjelma, jonka tavoitteena on ylläpitää ja kehittää henkilökunnan sekä keskeisimpien sidosryhmien turvallisuustietoisuutta. Turvallisuustietoisuutta voidaan lisätä useilla eri keinoilla, kuten ohjeistuksilla ja koulutuksella. On tärkeää, että turvallisuusviestintä räätälöidään kohdeyleisön mukaan. Turvallisuusviestin tulee vähintään sisältää, että mitä tietoa tulee suojata, miksi ja miten se tulee eri kohdeympäristöissä tehdä. Ohjelman tehokkuutta tulee seurata kohdeorganisaation omilla mittareilla, jotta nähdään, saadaanko sillä aikaan riittävää muutosta. ISF (2012, 48-59). ISO 17799 (2005, 26) pitää sisällään turvallisuustietoisuuden lisäämiseen liittyviä toimenpiteitä, mutta ne on kuvattu paljon suppeammin, kuin ISF:n standard of good practicessa.

ISF:n (2012, 61-67) mukaan yrityksen on luokiteltava tieto-omaisuutensa. Luokittelu auttaa ihmisiä ymmärtämään sen arvon, ja samalla lisäämään huolellisuutta, kun he käsittelevät todella arvokasta tietoa. Fyysisen omaisuuden, kuten prototyyppien seurantaa varten kannattaa rakentaa seurantatyökalu, josta nähdään omaisuuden liikkeet. Järjestelmä parantaa tiedon jäljitettävyyttä ja ihmisten vastuullisuutta. ISO 17799 (2005, 19-21) pitää sisällään samanlaiset kontrollit, jotka luovat perustan tuotevuotojen ennaltaehkäisytyölle.

ISF (2012, 61-67). ISF:n (2012, 165-174) mukaan yrityksillä tulee olla kyky reagoida erilaisiin turvallisuustapahtumiin, kuten tietovuotoihin. Hyvä reagointikyky auttaa pienentämään liiketoiminnalla aiheutuvan vahingon suuruutta sekä voi auttaa jatkossa ennaltaehkäisemään samantyyppiset tapahtumat. Työntekijöille on rakennettava raportointijärjestelmä, joka tekee tapahtumista raportoinnin helpoksi ja samalla nopeuttaa niihin reagoimista sekä kuntoonlaittamista. ISO 17799 (2005, 90-93) korostaa turvallisuustapahtumista oppimista.

ISF (2012, 165-174). ISF:n mukaan (2012, 243-245) yritysten tulee rajoittaa ihmisten pääsyä tiloihin, joissa käsitellään arvokasta tietoa. Pääsyoikeus tulee sallia vain niille henkilöille, jotka työskentelevät alueella. ISO 17799 (2005, 29-31) pitää sisällään useita erilaisia fyysisen turvallisuuden kontrolleja, joiden avulla voidaan varmistaa, ettei ulkopuoliset ihmiset pääse tiloihin, joissa käsitellään arvokasta tietoa.

8.2 Tietovuotojen ennaltaehkäisykeinoja Kiinassa

Pagnattaro (2012,1) on tutkinut kuinka yritykset voivat suojata osaamistaan ja yrityssalaisuuksia toimiessaan Kiinassa. Samat turvallisuustoimenpiteet ovat sovellettavissa muissakin liiketoimintaympäristöissä ja kulttuureissa. Pagnattaro (2012, 7) korostaa, että yrityksellä tulee olla olemassa tietoturvallisuuspolitiikka ja ohjeistus, joka määrittää kuinka arvokasta tietoa tulee käsitellä. Politiikka ja ohjeistus tulee säännöllisesti kommunikoida kaikille työntekijöille ja viestin perille meno tulee varmistaa seurannan avulla. Yrityksen tulee pitää kirjaa niistä työntekijöistä, joille on myönnetty pääsyoikeus luottamukselliseen tietoon, koska Kiinan oikeislaitos saattaa vaatia näitä tietoja todistusaineistoksi riitatilanteissa. On Tärkeää, että työntekijöille kommunikoidaan selkeästi, että kuka omistaa liiketoimintaan liittyvän tiedon, jotta he ymmärtävät, että työssä syntyneidne keksintöjen ensisijainen omistusoikeus kuuluu yritykselle. Yrityksen tulee huolehtia luottamuksellisen tiedon suojaamisesta fyysisillä ja loogisilla pääsynrajoituksilla. Käytännössä tämä tarkoittaa, että vain projektissa työskentelevät ihmiset pääsevät käsiksi arvokkaaseen tietoon. Tämän lisäksi työntekijöille on kerrottava, että arvokasta tietoa ei saada viedä pois pääsynrajoitetuista paikoista. Pääsynrajoitetuissa työtiloissa, tuotantolinjoilla ja tuotekehityslaboratorioissa tulee olla kuvauskielto ja mielellään kielto käyttää laitteita, jotka mahdollistavat kuvien ottamisen tai videon nauhoittamisen. Yrityksen esimiehet tulee kouluttaa siten, että he osaavat valvoa ja motivoida työntekijöitään toimimaan ohjeiden mukaisesti. Yrityksellä on hyvä olla olemassa käytäntöjä, joilla varmistetaan, että henkilön siirtyessä pois projektista, hänen hallussaan oleva tieto ja pääsyoikeudet tietoon tullaan poistamaan välittömästi. Samat käytännöt pätevät irtosanomis ja irtisanoutumistilanteissa. Pagnattaro (2012, 7).

Pagnattaro (2012, 7-8) esittelee julkaisussaan useita sopimuksellisia ja muodollisia kontrolleita tietovuotojen ennaltaehkäisemiseksi. Työntekijöiden tulee allekirjoittaa salassapitosopimus, jossa määritellään selkeästi, millaista tietoa sopimus koskee ja mitä työntekijältä edellelytetään. Työsopimuksessa tulisi puolestaa olla pykäliä, joissa työntekijät sitoutuvat siihen, että eivät saa ryhtyä kilpailemaan yrityksen kanssa. Tyypillisesti nämä pykälät ovat maksimissaan voimassa kaksi vuotta. On suositeltavaa liittää työsopimukseen pykälä, jossa työntekijä velvoitetaan ilmoittamaan etukäteen yrityksen johdolle, mikäli aikoo loikata kilpailevan yrityksen palvelukseen. Pagnattaro (2012, 7-8). Pagnattaro (2012, 8) suosittelee, että yritykset järjestäisivät seurannan, jossa seurattaisiin millaista työtä ja kenen palveluksessa sen entiset työntekijät tekevät. Seurannan avulla olisi mahdollista havaita mahdolliset salassapitosopimus rikkeet.

8.3 Yksilöiden viestintään liittyviä ja tietovuotoja ennaltaehkäiseviä keinoja

Sussmanin (2008, 336) mukaan yrityksen tuleen luoda sellainen kulttuuri, jossa ihmiset ymmärtävät miksi arvokasta tietoa tulee suojata. Tämä tarkoittaa asioiden kommunikoimista siten, että kaikki ymmärtävät suojaustavoitteen ja mihin sillä pyritään. Asiasta viestiminen tulee toteuttaa sellaisella tavalla, joka ei loukkaa työntekijöiden tunteita tai saa heitä kokemaan, että yrityksen johto eim luota heihin. Kulttuurin luomisessa on tärkeää, että kaikille on samat säännöt ja, että säännöt kommunikoidaan kaikille sidosryhmille liikesuhteen tai työsuhteen alkaessa. Turvallisuusviestiä kommunikoitaessa on tärkeää synnyttää kahdensuuntaista vuorovaikutusta, joka vähintään mahdollistaa aiheeseen liittyvien kysymysten esittämisen. Viestin kommunikoimiseen kannattaa käyttää erilaisia menetelmiä ja se tulisi toistaa säännöllisin väliajoin, jotta työntekijät ja sidosryhmät näkevät asian tärkeyden. Yritysten ei tulisi suosia menetelmiä, jossa jonkin asian tekeminen kielletään tai estetään täysin. Esimerkiksi Facebookin käyttörajoitukset työpaikalla eivät estä ihmisiä vuotamasta tietoa ulos. Yritysten tulee olla äärimmäisen tarkkana sen suhteen, että eivät leimaa kaikkia tietoa salaiseksi, koska sellainen vesittää suojaamisviestin. Sussman (2008, 336-337).

8.4 Tiedon suojaaminen kumppanuuksissa

Norman (2001, 51) on tutkinut kuinka yritys voi suojata tieto-omaisuuttaan työskennellessään yhteistyökumppaneiden kanssa. Yhteistyötä aloittavien yritysten tulee ymmärtää, että kumppaneille valuu paljon enemmän arvokasta tietoa, kuin yritys haluaisi. On tärkeää, että yritykset ymmärtävät tämän riskin ja ovat valmiit sen hyväksymään. Suojausmenetelmät jaetaan kolmeen eri kategoriaan: henkilöstöön, sopimuksiin ja prosesseihin. Henkilöstöön liittyvät menetelmät pitävät sisällään johdon sitoutumista, toiminnan sisäistä organisointia ja henkilökunnan kouluttamista. Sopimuskontrolleihin liittyvät yhteistyösuhteen sekä jaettavan tiedon määrittely, salassapitosopimukset ja turvallisuusvaatimukset. Sopimuskontrollit pitävät myös sisällään sopimusrikkomuspykälät sanktioineen. Keskeisimpiä prosessikontrolleita ovat muun muassa portinvartioiden määrittäminen. Nämä henkilöt varmistavat, että vain tarvittavilla henkilöillä on pääsyoikeus arvokkaaseen tietoon. Prosessikontrolleihin kuuluvat myös loogiset ja fyysiset pääsyoikeusprosessit. Norman (2001, 52-55).

Norman (2001, 55-56) nostaa tutkimuksessaan esiin kaksi merkittävää tieto-omaisuutta suojaavaa menetelmää, joita yhdistää ihmisesten turvalllisuustietoisuuden lisääminen. Ihmisten tulee olla tietoisia, että miksi tietoa tulee suojata ja mitkä tiedot liittyvät suojauksen piiriin. Norman (2001, 57) korostaa, että patentit ovat erittäin hyvä suojauskeino lääketeollisuudessa, koska lääkkeiden valmistukseen on äärimmäisen vaikeaa löytää vaihtoehtoisia kaavoja. Hän nostaa esiin, että elektroniikkateollisuudessa on taas helpompi

kiertää patentteja, joten yritysten ei tulisi ajatella, että pelkästään patentit suojaavat heidän liiketoimintaansa. Normanin (2001, 57) mukaan salassapitosopimukset ja sopimuskontrollit olivat heikoimpia menetelmiä tieto-omaisuuden suojaamiseksi, koska ne antoivat ihmisille vääränlaisen mielikuvan. Ihmiset kuvittelivat, että sopimus tarkoitti sitä, että kumppanin kanssa voidaan jakaa kaikkea tietoa, koska hehän olivat allekirjoittaneet salassapitosopimuksen. Tutkimuksessa kävi myös ilmi, että koulutuksen ja sopimuskontrollien yhdistämisellä päästiin usein hyviin lopputuloksiin, koska tämä auttoi ihmisiä ymmärtä mitä tietoa ja miten sitä voitiin jakaa kumppanien kanssa. Norman (2001, 57-59).

8.5 Nokian käytössä olevia tuotetietovuotoja ennaltaehkäiseviä menetelmiä toimittaessa yhteistyökumppaniverkoston kanssa

Yhteistyökumppanirajapinnassa käytettävät kontrollit voidaan jakaa muodollisiin ja sosiaalisiin kontrolleihin.

8.5.1 Muodolliset kontrollit

Nokian ja yhteistyökumppanin välillä on yleensä olemassa salassapitosopimus, tuotelainasopimus ja ohjelmistojen lisenssiointisopimus, jotka sisältävät turvallisuuteen liittyviä pykäliä. Näiden lisäksi on olemassa paljon erilaisia liiketoimintaan ja prosesseihin liittyviä vaatimuksia, joiden osana on turvallisuusvaatimusliite. Nämä vaatimukset sisältävät erilaisia yritysturvallisuuteen liittyviä kontrolleita. Tuotetietovuotojen ennaltaehkäisyyn liittyvät vaatimukset on sisällytetty yleisiin turvallisuusvaatimuksiin. Näihin vaatimuksiin edellyttävät kumppanin arvioivan ne prosessinsa, joissa liikkuu julkaisematonta tuotetietoa ja jalkauttamaan sopivat kontrollit prosessien suojaamiseksi ja ihmisten tietoisuuden parantamiseksi. Edellä mainittujen lisäksi vaatimukset painottavat prototyyppien käsittelyn organisointia ja turvallisia tapoja siirtää luottamuksellista tietoa. Vaatimustenmukaisuutta arvoidaan kaksi vaiheisella auditointiprosessilla, jonka ensimmäisessä vaiheessa kumppani arvioi oman turvallisuuskyvykkyytensä ja toisessa vaiheessa järjestetään tilojen ja prosessien auditti kumppanin toimitiloissa. Käytännössä auditointitoiminta on viime vuosina keskittynyt ensimmäiseen eli itsearviontivaiheeseen, koska yhteistyökumppaneita on ollut liikaa suhteessa olemassa oleviin auditointi resursseihin, eivätkä auditit itsessään ole saaneet vuotoja vähenemään.

Nokia suorittaa taustojen selvitykset niille yhteistyökumppanien työntekijöille, jotka tulevat työskentelemään Nokian toimipisteissä. Taustaselvitykset tehdään niissä maissa, joissa paikallinen lainsäädäntö mahdollistaa sen. Nokialla on käytössään useita tietojärjestelmiä, jotka ovat tarkoitettu Nokian ja yhteistyökumppanien väliseen tiedon ja tieto-omaisuuden siirtämiseen ja tallentamiseen. Tällaisia järjestelmiä on tuotekehityksen sekä suunnittelu ja

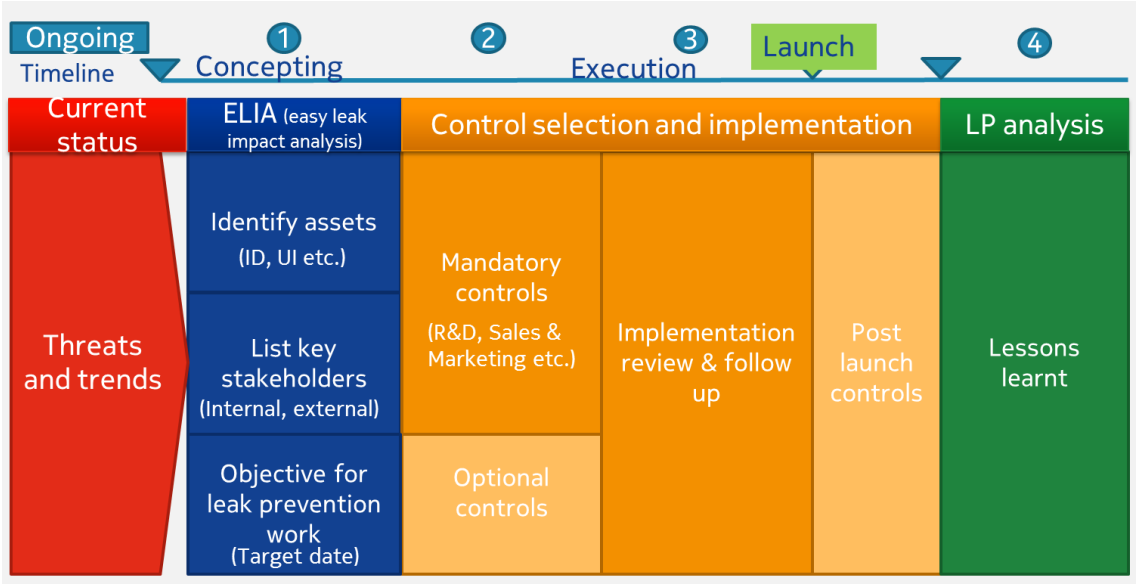
markkinointitoimistojen käytössä. Nokia on luonut oman prototyyppien seurantatietokannan, jolle on luotu internet-pohjainen käyttöliittymä, jotta kaikki yhteistyökumppanit voivat käyttää sitä sujuvasti. Seurantatietokannalla pyritään parantamaan prototyyppien käyttäjien vastuullisuutta sekä prototyyppien jäljitettävyyttä. Yhteistyökumppaneilta vaaditaan jokaisen prototyypin rekisteröimistä kantaan. Käyttöliittymä löytyy osoitteesta proto.nokia.com ja se sisältää myös prototyyppien käsittelyyn liittyvät turvallisuusohjeet.

8.5.2 Sosiaaliset kontrollit

Turvallisuusorganisaatio on muutaman viime vuoden aikana lähtenyt jalkauttamaan uudenlaista lähestymistapaa yhteistyökumppaneihin, joka perustuu kahdensuuntaiseen vuorovaikutukseen. Olemme pyrkineet rakentamaan turvallisuusyhteistyötä merkittävimpien yhteistyökumppaneiden kanssa. Tämä työ aloitettiin muutamien kumppanien kanssa jo vuonna 2011. Osana yhteistyötä me pidimme tietoiskuja kumppanin asiakkuusvastaaville henkilöille ja heidän turvallisuusvastuuhenkilöilleen. Tietoiskuissa käytiin läpi tietovuotojen ennaltaehkäisyyn liittyviä keskeisiä asioita ja sovimme että kumppanit ryhtyvät tekemään samanlaisia turvallisuustoimenpiteitä omissa organisaatioissaan. Osana keskustelua kerroimme yhteistyökumppaneille mitä vaikutuksia vuodoilla on meidän liiketoiminnallemme ja mitä toivomme heidän tekevät. Koimme, että avoimuus vaikeistakin asioista auttoi rakentamaan luottamusta osapuolten välille ja osaltaan paransi kumppanin sitoutumisastetta. Yhteistyötä rakennettiin vain muutaman yrityksen kanssa, mutta tulokset olivat positiivisia, jos niitä peilataan turvallisuustapahtumien ja vuotojen vähenemiseen kyseisessä yhteistyökumppaniyrityksissä.

8.6 Sisäisesti käytettyjä tuotetietovuotoja ennaltaehkäiseviä kontrolleja

Nokialla on olemassa systemaattinen toimintatapa, jonka avulla pyritään ennaltaehkäisemään tuotetietovuotojen syntyminen. Työn tavoitteena on estää vuodot ennen tuotteen julkistusta. Tuotetietovuotojen ennaltaehkäisytyön perusteesit ovat vastuullisuus, jäljitettävyys ja kontrolloitavuus. Vastuullisuudella tarkoitetaan sitä, että ihmiset toimisivat vastuullisesti käsitellessään julkaisematonta tuotetietoa. Jäljetettävyydellä pyritään suurentamaan kiinnijäämisen riskin todennäköisyyttä, mikä osaltaan vaikuttaa ihmisten tapaan käsitellä arvokasta tietoa ja muuta omaisuutta. Kontrolloitavuuden avulla pyritään jalkauttamaan liiketoimintatavoitteita tukevia kontrolleja, jotka mahdollistavat oikeiden roolien oikea aikaisen pääsyn julkaisemattomaan tuotetietoon. Tuotetietovuotojen ennaltaehkäisyohjelma jakaantuu muutamaan keskeiseen vaiheeseen, jotka ovat easy leak impact analyysi, kontrollien valinta, kontrollien jalkauttaminen, seuranta ja loppuanalyysin tekeminen. Toimintaympäristöön liittyviä uhkia ja riskejä seurataan jatkuvasti.



Kuvio 6: Nokian toimintamalli tuotetietovuotojen ennaltaehkäisyyn.

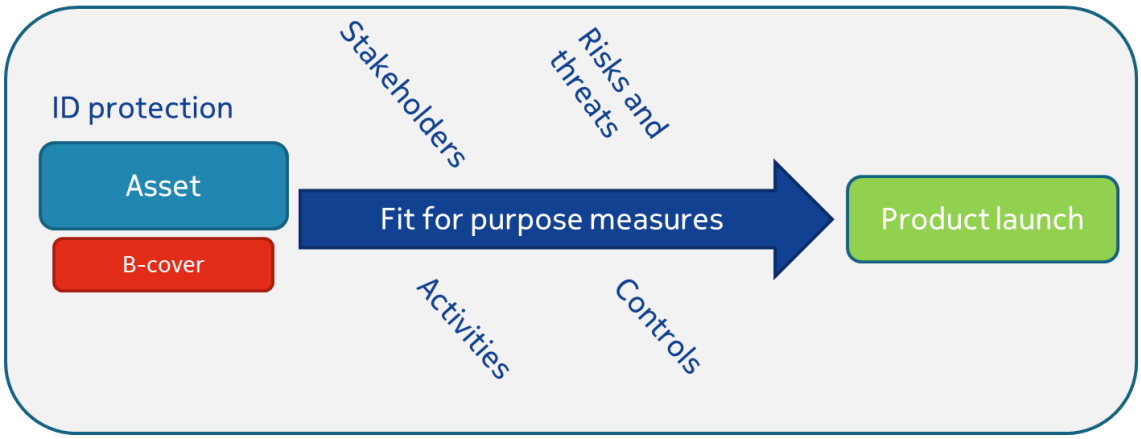
8.7 Easy Leak Impact -analyysi (mitä suojataan)

Olemme luoneet menetelmän, jonka avulla pystytään analysoimaan tuleva tuote ja mitä siitä tulisi erityisesti suojata, sekä mitkä sidosryhmät tulevat käsittelemään tulevaan tuotteeseen liittyvää tietoa. Menetelmässä arvioidaan tuotteen ulkoasuun, käyttöliittymään, ominaisuuksiin ja teknologiaan liittyviä asioita sekä mitkä niistä ovat sellaisia, joihin suojaustoimenpiteet tulee kohdistaa. Menetelmä auttaa arvioimaan, kuinka pitkään tuotteeseen liittyviä tietoja tulee suojata. ELIA-analyysi on ollut oivallinen keino motivoida tuotekehitystä ja sen sidosryhmiä panostamaan enemmän tietovuotojen ennaltaehkäisytyöhön, koska analyysi auttaa heitä näkemään oman tuotteensa merkittävyyden turvallisuusnäkökulmasta.

8.8 Kontrollien valinta, jalkauttaminen ja seuranta

Olemme viime vuosien aikana keränneet ja luoneet turvallisuuskontrolleja, joiden avulla pyritään suojaamaan arvokasta tuotetietoa eri liiketoimintayksiköissä ja toiminnoissa. ELIA-analyysin jälkeen valitsemme tuoteohjelman kanssa kyseiselle tuotteelle sopivimmat kontrollit, joiden jalkauttamiseen tuoteohjelman eri vastuuhenkilöt sitoutuvat. Ajatellaan, että ELIA-analyysissa nousee esiin, että tuotteen takakansi on sellainen jota täytyy erityisesti suojata. Tämän jälkeen selvitetään, mitkä sidosryhmät tulevat käsittelemään takakansia ja minkalaisia toimintoja tähän liittyy. Tämän jälkeen arvioidaan toimintoihin liittyvät riskit eli mitkä tekijät voisivat aiheuttaa vuotoja. Tämän jälkeen valitaan suojaustoiminpiteet, joiden

jalkautusta jatketaan tuotteen julkaisuun asti. Kontrollien toimivuutta seurataan säännöllisesti ja epäkohtiin reagoidaan nopeasti.



Kuvio 7: Arvokkaan tuotetiedon suojaaminen sopivilla turvallisuuskontrolleilla.

8.9 Sisäisiä käytäntöjä turvallisuustietoisuuden jalkauttamisesta osana tuotetietovuotojen ennaltaehkäisyohjelmaa

Alkuvuodesta 2010 saimme toimeksiannon älypuhelinten tuotehallintayksiköltä, jonka koko henkilökunta tulisi kouluttaa niin, että he ymmärtävät vastuunsa ja osaavat jatkossa turvallisesti käsitellä tuotteidensa tietoa. Yksikön vetäjä nimesi meille tukihenkilön, joka auttoi koulutusmateriaalin luonnissa ja auttoi koulutusten organisoinnissa. Saimme luvan järjestää kolmen tunnin tilaisuuden jokaisessa toimistossa, jossa yksiköllä oli toimintaa. Luonnollisesti tämä käynnisti meissä reaktion, että haluamme kertoa kaikki asiat maan ja taivaan väliltä, mikä johti liian raskaaseen materiaaliin, joka sisälsi myös vähemmän tärkeitä asioita. Koulutusmateriaali sisälsi paljon kuvia, joista moni kuvasi käytännön esimerkkejä tuotetietovuotojen ennaltaehkäisymenetelmistä. Hyödynsimme koulutuksessa ”Why should I care”-kampanjan videota, jonka teemana oli tuotetiedonluokittelu ja kuinka sitä hyödennetään tarkoitti käytännössä.

Itse koulutustilaisuuden olimme jakaneet kolmeen osioon. Ensimmäiseksi kävimme läpi viime aikaisia vuotoja ja aiheeseen liittyviä haasteita, minkä jälkeen kysyimme yleisöltä, että haluavatko tulla mukaan talkoisiin. Tämän jälkeen heille kerrottiin, kuinka heidän tulee käsitellä tuotetietoa ja prototyyppejä päivittäisessä työssään. Keskimmäisessä osiossa mainittiin myös Nokian tuotetiedonkäsittelypolitiikka, yksilön vastuut ja mitä positiivista vuotojen ennaltaehkäisystä voi seurata. Koulutuksen viimeisessä osiossa laitoimme osallistujat ideoimaan tuotetietovuotojen ennaltaehkäisymenetelmiä. Ideointi tapahtui ensin yksin, minkä jälkeen siirryttiin ryhmiin. Lopuksi ideoita käytiin läpi yhteisesti.

Koulutuksen osallistujat pitivät tavastamme jalkauttaa turvallisuusviesti ja siitä, että he pääsivät itse osallistumaan ideointiin. Ihmiset arvostivat tapaamme kertoa avoimesti vuodoista, niiden seurauksista ja Nokian sisällä olevista vuotoihin liittyvistä turvallisuusepäkohdista. Toisaalta joidenkin mielestä kolmen tunnin pituinen koulutussessio oli liian pitkä, eivätkä he jaksaneet keskittyä koko aikaa. Tuotehallintayksikön kouluttamispyyntö auttoi meitä luomaan konseptin, jonka avulla turvallisuusviesti saadaan jalkautettua varsin menestyksekkäästi. Käytimme samaa menetelmää Nokian muotoiluyksikön kanssa, mutta hieman räätälöidyllä sisällöllä, koska muotoiluihmisten työ eroaa todella paljon tuotepäälliköiden tehtävistä.

8.9.1 Liiketoimintaa varten räätöity turvallisuuskoulutus

Keväällä 2010 saimme koulutuspyynnön yhdeltä Salossa toimivalta tuoteohjelmalta, jonka vetäjä halusi meidän kouluttavan tiimilleen tuoteohjelmaan liittyvät käytännön turvallisuustoimenpiteet. Pyyntöä tehdessään hän korosti erityisesti sitä, ettei halua kuulla mitään yleistä turvallisuusviestiä, vaan täysin heille räätälöidyn koulutuksen. Kyseessä oli melkoinen haaste, koska emme tunteneet vielä tarpeeksi hyvin tuoteohjelmien tapaa toimia. Onneksemme meillä oli käytössämme menestyksekkään N97-tuoteohjelman hyvät käytännöt, jonka pohjalle rakensimme esityksemme. Aikaa koulutukselle oli vain yksi tunti, joten koulutuksen sisältönä olivat vain keskeisimmät asiat. Koulutuksen alussa käytimme jo hyväksi todettua tapaa herättää ihmiset viime aikaisilla vuototapauksilla.

Koulutuksen aikana meille heitettiin useita haastavia kysymyksiä ja kommentteja, kuten miksi Applen tuotteet eivät vuoda, vuodothan tapahtuvat alihankkijoiden toimesta ja eihän meillä tuotekehityksessä ole mitään ongelmia, koska markkinointihan se vain vuotaa. Onneksi olimme miettineet haastavia kysymyksiä etukäteen, joten onnistuimme vakuuttamaan yleisön vastauksillamme. Tuollaiset haastavat tilanteet ovat olleet yleisiä koulutuksia pitäessämme, koska ihmisten tietämys on perustunut vanhoihin tietoihin ja huhupuheisiin. Oikean tiedon avoimella kommunikoimisella olemme saaneet vaikutettua ihmisten asenteisiin ja sitä kautta heidän motivaationsa panostaa tuotetiedon suojaamiseen työssään. Tuoteohjelman vetäjä oli erittäin tyytyväinen koulutuksen jälkeen. Hän sanoi, että oli positiivisesti yllättynyt siitä, miten hyvin esittämämme turvallisuusasiat olivat linjassa tuoteohjelman tekemisen kanssa. Positiivisen palautteen jälkeen oli helppo hyödyntää koulusmateriaaliamme muiden tuoteohjelmien kanssa.

8.9.2 Turvallisuusenkelit

Jo talven 2010 aikana ryhdyimme kutsumaan itseämme Security Angel-nimellä, minkä tarkoituksena oli herättää huomiota liiketoimintayksiköiden keskuudessa, koska perinteinen

moi olen turvallisuusyksiköstä ei säväyttänyt ketään. Saimme paljon positiivista huomiota uuden nimen käytön johdosta, mikä osaltaan auttoi turvallisuusviestin viemisessä. Keväällä 2010 onnistuimme integroimaan tuotetietovuotojen ennaltaehkäisyohjelman osaksi älypuhelintuoteohjelmien tuotekehitystoimintaa, mikä tarkoitti Security Angel:in antamista tuoteohjelman turvallisuusresurssiksi. Turvallisuusenkeli-konsepti antoi meille mahdollisuuden kehittää turvallisuustietoisuuden levittämiskeinoja uudenlaisten ohjeistusten ja koulutusten muodossa.

8.9.3 Liiketoimintalähtöiset turvallisuusohjeistukset

Kesällä 2010 otimme käyttöön tuoteohjelma- ja liiketoimintayksikkökohtaiset ohjeet. Ensimmäisenä teimme Meego-turvallisuusohjeet, jotka kertoivat Meegon työntekijöille, että miten siihen liittyviä tuotetietoja tuli käsitellä. Tämän viestin jalkauttamiseen saimme erinomaista tukea Meegon johtoryhmältä, joka korosti turvallisuuden tärkeyttä heidän liiketoiminta-alueillaan ja kehotti työntekijöitään joko lukemaan ohjeen tai sitten osallistumaan koulutukseen, jossa ohjeen sisältö käytiin läpi vuototapausten kera. Liiketoimintayksikkökohtaisen ohjeen lisäksi rakensimme tuoteohjelmakohtaisen ohjeen, joka sisälsi vain muutaman sivun, kertoen mitä kyseisessä tuotteessa tuli suojata ja miten se tuli tehdä. Ohjeen keskeisin sanoma oli, että turvallisuusviesti tuli viedä jokaiselle, joka käsitteli julkaisematonta Meegoon liittyvää tuotetietoa.

N9-laitteella oli oma ohjeensa, joka kertoi työntekijöille, kuinka laitteen ulkoasua, käyttöliittymää ja käyttäjäkokemusta tuli suojata. Tämä viesti vietiin eteenpäin sisäisille ja ulkoisille sidosryhmille, Meegon johtoryhmän, työntekijöiden ja turvallisuusyksikön toimesta. Uudenlaisella turvallisuusviestinnällä oli suuri merkitys siinä, että N9-laite ei vuotanut ulos ennen julkistusta. Johto näytti työntekijöille omalla esimerkillään oikean toimintamallin, turvallisuutta jatkuvasti korostaen. Tämän jälkeen työntekijät ymmärsivät, että heidänkin panostaan tarvittiin onnistumiseen. Työntekijät olivat motivoituneita, koska ymmärsivät miksi vuotojen ennaltaehkäisy oli tärkeää ja mitä heidän odotettiin tekevän. Positiivinen turvallisuuskulttuuri levisi kulovalkean tavoin sisäisiin ja ulkoisiin sidosryhmiin, ohjaten heidät toimimaan ohjeiden mukaisesti. Yhtenä syynä N9-laitteen menestykseen oli myös se, että ihmiset ymmärsivät olevansa tekemisissä ainutlaatuisen tuotteen kanssa, eivätkä he halunneet salaisuuden karkaavan käsistään.

Meegon kanssa harjoittelu auttoi meitä ymmärtämään, miten ihmiset saadaan toimimaan turvallisuusohjeiden mukaisesti. Se myös synnytti parhaillaan käytössä olevan ohjeistusrakenteen, joka koostuu liiketoimintakohtaisista yleisohjeista, joita meillä on käytössämme kaksi erilaista: Lumia-turvallisuusohjeet ja Mobile Phones-turvallisuusohjeet. Kyseisistä ohjeista on myös olemassa versiot alihankkijoille. Näiden yleisohjeiden lisäksi

luomme yhdessä tuoteohjelmien kanssa lyhyet tuotekohtaiset ohjeet, joissa kerrotaan miten kyseistä tuotetta suojataan. Nämä ohjeet tehdään yhdessä tuoteohjelman kanssa ja kommunikoidaan keskeisille sidosryhmille tuoteohjelman alkaessa. Turvallisuustietoisuutta pidetään yllä koko tuoteohjelman ajan, nostamalla esiin tiettyjä ajankohtaisia teemoja, kuten prototyyppien käsittely juuri ennen kuin uusia prototyyppejä ryhdytään testaamaan. Viime aikoina on ollut tapauksia, jolloin tuote on julkaistu, mutta siihen liittyy vielä luottamuksellisia asioita, jotka ilmenevät laitteiden ominaisuuksien käyttörajoituksina. Tällaiset tapaukset ovat erittäin haastavia turvallisuusviestinnän kannalta, koska ihminen pystyy pitämään salaisuuden tiettyyn pisteeseen asti, eikä helposti motivoidu noudattamaan käyttörajoituksia. Tällaisissä tilanteissa kerromme ihmisille käyttörajoituksen syyn, joka yleensä liittyy sopimusvelvoitteeseen kumppanimme Microsoftin kanssa tai siihen ettemme halua asiakkaiden näkevän laitteita vajaavaisilla ominaisuuksilla. Parempia motivoimiskeinoja emme ole vielä tähän yhteyteen keksineet.

8.9.4 Muita turvallisuustietoisuuden lisäämisessä käytettyjä menetelmiä

Perinteisten koulutusten ja ohjeistusten lisäksi olemme kehittäneet muitakin turvallisuustietoisuuden lisäämiskeinoja. Meillä on paljon ohjeistuksia ja muuta hyödyllistä materiaalia sisäverkossamme, josta työntekijät voivat halutessaan niitä lukea. Olemme kuvanneet paljon videoita, joissa olemme haastatelleet Nokian johtokunnan jäseniä ja eri liiketoimintayksiköidemme edustajia, jotka ovat kertoneet omat näkemyksensä tietovuodoista, niiden seurauksista ja millaiseen tavoittetasoon meidän tulisi pyrkiä. Näiden videoiden lisäksi olemme saaneet loistavaa spontaania tukea toimitusjohtajalta ja muutamalta johtokunnan jäseneltä, jotka ovat yleisissä videoiduissa tilaisuuksissa korostaneet turvallisuuden ja tietovuotojen ennaltaehkäisyn merkitystä. Olemme brutaalisti hyödyntäneet näitä viestejä esityksistämme ja koulutusmateriaaleissamme. Johdon spontaanit viestit ovat auttaneet meitä merkittävästi uudenlaisen kulttuurin luomisessa.

Nokian sisällä on käytössä Facebookin kaltainen kohtaamispaikka, jossa ihmiset vaihtavat mielipiteitä erilaisista asioista. Olemme luoneet sinne oman kanavan turvallisuudelle, jossa nostamme esiin erilaisia aiheita. Sen tarkoituksena on luoda turvallisuudelle kasvot ja muutenkin tuoda esiin vaikeitakin asioita ja esimerkiksi kertoa ihmisille vuototapauksista ja niiden seurauksista. Kyseisen kanavan kautta työntekijät pystyvät osallistumaan turvallisuuskeskusteluun ja tuomaan esiin omia mielipiteitään ja kehitysehdotuksiaan. Luonnollisesti viemme viestiä myös palvelussa oleviin liiketoimintayksiköiden kanaviin, jotta saamme viesteillemme suuremman pintaa-alan. Aktiivinen osallistumisemme on auttanut osaltaan uudenlaisen ja avoimemman turvallisuuskulttuurin luomisessa, koska ihmiset ovat saaneet turvallisuudelle enkelin kasvot ja huomanneet, että voivat vaikuttaa itsekin turvallisuuteen.

9 Menetelmien valinta

Hankkeen tavoitteena on tuotetietovuotojen vähentäminen yhteistyökumppaniverkostossa, mikä tapahtuu uudenlaista turvallisuuskulttuuria luomalla. Muutos jalkautetaan ensin sisäisten sidosryhmien keskuudessa, koska ilman heidän tukeaan ja sitoutumistaan, ei muutoksen vieminen yhteistyökumppaniverkostoon tule onnistumaan suunnitellusti. Sisäisen jalkauttamisen jälkeen muutos viedään yhteistyökumppaniverkostoon, jossa jalkauttaminen kestää pisimpään, johtuen yritysten suuresta lukumäärästä. Kehityshankkeessa aikana tehtävä muutos pitää sisällään useita asioita, jotka yhdessä luovat uudenlaisen kulttuurin ja kestävän toimintamallin. Tarkoituksena on luoda avoin, läpinäkyvä, tasa-arvoinen ja yhdessä tekemisen kulttuuri, jossa Nokia ja sen yhteistyökumppanit jakavat yhteisen tavoitteen, mikä tässä tapauksessa on tuotetietovuotojen ennaltaehkäisy päivittäisessä toiminnassa. Uudenlaisella kulttuurilla pyritään siihen, että jatkossa nämä sidosryhmät oma-aloitteisesti huomioivat myös turvallisuuden toiminnassaan ja saavat siihen tarvittaessa apua Nokialta, esimerkiksi ohjeiden muodossa.

Riskienhallintaosaamista sekä tietoisuutta vahinkoriskeistä tulee parantaa, koska se luo pohjan proaktiiviselle ja liiketoimintalähtöiselle turvallisuustoiminnalle. Turvallisuustoiminpiteiden tulee olla jatkossa sellaisia, että ne huomioivat tuotetiedon liikkumisen prosesseissa ja kuinka sitä suojataan prosessin eri vaiheissa. Tuotetiedon suojaus prosesseissa tulee myös huomioida auditointikoulutuksissa, joka uudenlainen toimintatapa saadaan vietyä käytäntöön. Keskeisimmät turvallisuustoimenpiteet tulee myös integroida Nokian hankintayksiköiden prosesseihin, jotta ne sitä kautta tulevat osaksi päivittäistä toimintaa.

Muutoksen keskiössä ovat ihmiset sekä sisäisistä että ulkoisista sidosryhmistä. Vuototapaukset ovat osoittaneet, että suurin osa vuodoista johtuu ihmisten tekemisistä tai tekemättäjättämistä. Tämän vuoksi ihmiset sekä heidän sitouttamisensa ja turvallisuustietoisuuden tulevat olemaan menetelmien jalkauttamistoiminnan keskiössä.

9.1 Uudenlaisen toimintakulttuurin luominen

Sisäisillä sidosryhmillä on merkittävä rooli uuden toimintakulttuurin luomisessa, koska tavoitteeseen pääseminen vaati muutosta heidän ajattelutavassaan. Aikaisemmin ajateltiin, että pakollinen turvallisuuskommunikointi hoidetaan sopimusvaatimuksilla. Tämä toimintatapa oli tavallaan sanelupolitiikkaa, jonka avulla ajateltiin, että yhteistyökumppanit saadaan toimimaan asiakkaan haluamalla tavalla. Kyseinen tapa toimia ei kuitenkaan pitänyt sisällään kovinkaan paljon neuvotteluvaraa, jota pahensi se, että asiakkaan tahtotilakin oli ilmaistu sopimustekstinä, jonka sisältö ei ollut helposti ymmärrettävissä. Vaatimusten avulla

jalkauttamisella ei useinkaan päästä hyviin tuloksiin, koska kumppanit rakentavat vain minimitason turvallisuusjärjestelyt, eivätkä läheskään aina ymmärrä niidenkään sisältöä, saati merkitystä. Turvallisuustoimenpiteet on pääsääntöisesti jalkautettu vain, koska asiakas näin vaatii, ilman laajempaa ymmärrystä niiden tuomista mahdollisista positiivisista vaikutuksista molempien yritysten liiketoiminnalle. Mikäli Nokian luomat sopimusvaatimukset eivät auta hallitsemaan tuotetietovuotoihin liittyviä riskejä, niin silloin ollaan huonossa tilanteessa, koska yhteistyökumppanit ovat olleet pakotettuja tekemään asiat yhdellä tavalla, ilman oman maalaisjärjenkäyttöä.

Uudella toimintakulttuurilla tarkoitetaan avointa, selkeää ja toistuvaa kommunikointia sekä turvallisuusyhteistyön luomista Nokian ja yhteistyökumppanin välille. Avoimella kommunikoinnilla pyritään luomaan luottamus osapuolten välille, jonka avulla yhteistyön rakentaminen on helpompaa. Kommunikoinnin selkeydellä mahdollistetaan viestin, esimerkiksi edellytettävien turvallisuustoimenpiteiden sisällön ymmärtäminen. Viestinnän selkeys on äärimmäisen tärkeää etenkin silloin, kun kyseessä on pieni yhteistyökumppani, koska heillä ei ole käytössään turvallisuusasiantuntijoita, jotka yleensä ymmärtävät vaikeankin vaatimusdokumentin tai ohjeistuksen sisällön. Toistuvalla viestinnällä saadaan taas viestittyä, että asia on oikeasti tärkeää ja että tuotetietovuotojen ennaltaehkäisy on jatkuvaa työtä.

Turvallisuusyhteistyö tarkoittaa sitä, että Nokia ja yhteistyökumppani keskustelevat turvallisuusasioista säännöllisesti, jakavat hyviä käytäntöjä sekä tekevät muita turvallisuuteen ja riskienhallintaan liittyviä asioita yhdessä. Uudenlaisen toimintakulttuurin omaksuminen vaatii sisäisiltä sidosryhmiltä paljon, koska heidän täytyy laskea itsensä jalustalta ja kertoa kumppanille, että meillä on haasteita, johon toivomme apua heiltä. Aikaisemmin odotettiin yhteistyökumppaneiden ratkaisevan haasteet ilman Nokian osallistumista, mutta uudessa toimintakulttuurissa yhteiset haasteet tullaan ratkomaan yhdessä. Sisäisten sidosryhmien tulee ymmärtää, että heidän tulee ylläpitää suhdetta yhteistyökumppaneiden kanssa myös turvallisuusasioiden suhteen, mikä saattaa tuntua lisätyöltä. Turvallisuusyhteistyö tullaan integroimaan osaksi sisäisten sidosryhmien prosesseja ja sitä tukevia ohjeita laitetaan saataville sisäverkkoon. Uudenlaista kulttuuria tullaan ajamaan sisään koulutuksissa ja hankintayksikön workshopeissa. Sisäisten sidosryhmien ajattelutavan muutosta tuetaan turvallisuusyksikön toimesta, joka on sitoutunut antamaan resursseja auttamaan yhteistyön rakentamisessa.

9.2 Sisäisten sidosryhmien sitouttaminen

Kehityshankkeen alussa on tärkeää tutustua sisäisiin sidosryhmiin, jotta ymmärtää miten ne toimivat, mitä kehitettävää ympäristöstä löytyy ja miksi tietyllä tavalla toimitaan.

Toimintaympäristöön tutustuminen aloitettiin jo 2011 ja se vietiin loppuun helmikuussa 2012. Havaintojeni pohjalta on rakennettu koulutusmateriaali, joka pitää sisällään esimerkkejä vuodoista ja muista ympäristön turvallisuusepäkohdista. Koulutusmateriaalissa kerrotaan myös kohdeympäristöstä havaituista haasteita, sekä tuodaan esiin käytännönläheisiä keinoja siitä, miten organisaatiot ja niissä toimivat yksilöt voivat kehittää toimintaansa. Hankintayksikön johtoryhmä on antanut hyväksyntänsä materiaalin kommunikointiin yksikön henkilökunnalle. Kommunikointi tehdään workshop-mallilla, jossa osallistujat pääsevät vaikuttamaan session kulkuun. Workshoppien tavoitteena on sitouttaa työntekijät muutoksen läpivientiin, koska heitä tarvitaan turvallisuustoimenpiteiden jalkauttamiseen yhteistyökumppaniverkostossa. Samalla heidän turvallisuusosaamistaan pyritään parantamaan. Liiketoimintayksiköiden työntekijöillekin viedään viestiä siitä, että miten yhteistyökumppaneiden toimitaan silloin, kun osapuolten välillä siirretään julkaisematonta tuotetietoa.Viesti tullaan integroimaan osaksi sisäisiä koulutuksia ja ohjeistuksia.

9.3 Liiketoiminta-ja prosessilähtöisyyden tuominen osaksi toimintaa

Havaintojeni perusteella voidaan todeta, että sopimuksiin liitetään turvallisuusvaatimuksia vaihtelevasti ja yhteistyökumppaneiden turvallisuustason auditointeja tehdään satunnaisesti, eivätkä ne läheskään aina kohdistu sinne, missä arvokas tuotetieto liikkuu. Jatkossa jokaista tuotetietoa käsittelevää toimittajaa tullaan käsittelemään yhtenäisellä tavalla ja tämän toteutumista tullaan seuraamaan. Uudistuksen avulla saadaan huolehdittua, että perusasiat, kuten oikea sisältöiset ovat paikoillaan. Uudistus pitää muun muassa sisällään sen, että auditoijille tullaan järjestämään koulutuksia, jossa heidän liiketoiminta-ja prosessiosaamistaan tullaan kehittämään. Tarkoituksena on saada heidät kohdistamaan turvallisuuskatselmoinnit kaikkialle niihin prosesseihin, missä arvokasta tieto-omaisuutta käsitellään. Turvallisuuden katselmointi prosesseissa parantaa auditoinneista saatavia hyötyjä, ja on yksi uusi keino kyseisen ajattelutavan viemisessä yhteistyökumppaniverkostoon. Auditointikoulutusta on testattu turvallisuusyksikön työntekijöiden kanssa ja tulokset ovat olleet positiivisia. Materiaalin vaatii kuitenkin vielä useampien käytännön läheisten esimerkkien lisäämistä siihen. Turvallisuustoimenpiteet tullaan myös integroimaan hankitayksikön prosesseihin, koska sitä kautta ne saadaan osaksi normaalia kanssakäymistä toimittajien kanssa. Kyseiset turvallisuustoimenpiteet luotiin jo vuonna 2011, mutta jalkautus jäi kesken organisaatiomuutoksen vuoksi. Jalkautus viedään loppuun osana tätä hanketta.

9.4 Turvallisuustietoisuuden lisääminen yhteistyökumppaniverkostossa

Hyvien turvallisuuskäytäntöjen kommunikointiin yhteistyökumppaneille tullaan käyttämään useita menetelmiä. Kommunikoinnin tavoitteena on saada kumppanit ymmärtämään nykyisen

toimintakentän turvallisuushaasteet ja sitä kautta sitouttaa heidät jalkauttamaan turvallisuustoimenpiteitä. Viestintämateriaalin pyritään pitämään yhtenäisenä Nokian sisäisen viestintämateriaalin kanssa, koska pelisäännöt ovat samat kaikille osapuolille ja yhtenäisyys helpottaa käytännön työskentelyä osapuolten välillä. Materiaalin sisällön kanssa pyritään yksinkertaisuuteen ja selkeyteen, yhteys liiketoimintaan huomioiden. Yleisohje on luotu jo vuonna 2011 ja sitä räätälöidään toimittajan liiketoiminta-alueen mukaisesti, koska työskentelyn ominaispiirteet vaihtelevat rippuen esimerkiksi siitä, onko kyseessä markkinointi vai tuotekehitys. Liiketoimintalähtöisyys parantaa ohjeen omaksumista, koska yritys ja sen työntekijät löytävät siitä riippuvuuden omaan työhönsä.

Keskeinen viesti jaetaan kahdelle eri kohderyhmälle: yhteistyökumppaniyrityksen johdolle ja sen Nokian projektissa työskenteleville työntekijöille. Johdon viestissä korostetaan, millaisia turvallisuusjärjestelyitä Nokia edellyttää kumppanilta ja miksi. Työntekijöille taas kerrotaan käytännölliset ohjeet, jotka kertovat miten tuotetietoa ja prototyyppejä tulee käsitellä, unohtamatta miksi näin tulee toimia. Testasimme kyseistä vuonna menetelmää useiden yhteistyökumppaneiden kanssa vuosina 2011-2012 ja olemme ottaneet sen osaksi normaalia turvallisuustyötä. Tulokset ovat olleet positivisia, koska vuodot ja muut turvallisuusepäkohdat ovat vähentyneet kyseisissä kohdeympäristöissä. Ohjeistukset kommunikoidaan yhteistyökumppanille kahdessa vaiheessa, joista ensimmäinen tapahtuu sopimusta tehdessä. Toinen vaihe on projektin aloituspalaveri. Aloituspalaverissa sovitaan, että kuinka yhteistyökumppani jalkauttaa ohjeistuksen työntekijöilleen. Kehityshankkeen osana tullaan luomaan extranet, josta kumppanit löytävät viimeiset ohjeistukset ja muut hyvät käytännöt tuotetietovuotojen ennaltaehkäisyyn. Tämän jälkeen järjestetään seminaari, johon kutsutaan keskeisimmät yhteistyökumppanit kuulemaan viimeisimmät turvallisuusasiat liittyen tuotetietovuotojen ennaltaehkäisyyn.

9.5 Vahinkoriskien arviointi osaksi hankintaprosessia

Turvallisuustoiminta yhteistyökumppaniverkostossa ei ole ollut tarpeeksi riskienhallintalähtöistä. Tällä tarkoitan sitä, että sisäiset sidosryhmät ja yhteistyökumppanit eivät ole läheskään aina arvioineet toimintaan liittyviä riskejä turvallisuusnäkökulmasta, mikä on johtanut siihen, että turvallisuustoimenpiteet eivät ole olleet riittävällä tasolla tai ne on kohdistettu vääriin paikkoihin. Tätä osa-aluetta tullaan parantamaan kehityshankkeen aikana. Sisäisten sidosryhmien riskienhallintaosaamista tullaan kehittämään osana heille järjestettäviä koulutuksia ja workshoppeja, sekä integroimalla riskienarviointia vaativa vaihe hankintayksikön prosesseihin. Vaiheen kulku tullaan myös ohjeistamaan. Sisäinen Kehittämistyö riskienhallinnan osalta on käynnissä ja se valmistuu huhtikuun 2012 loppuun mennessä. Itse jalkauttamiseen menee kauemmin aikaa.

9.6 Yhteistyökumppaneilta edellytettävä turvallisuuskyvykkyys

Jotta voidaan tehdä nykytila-analyysi ja jatkossa seurata eri toimittajien kyvykkyyden kehittymistä, on tärkeää määrittää ne turvallisuustoimenpiteet, joita tullaan seuraamaan. Kyseiset toimenpiteet tulee olla jalkautettuna jokaisella kumppanilla. Seurattavat turvallisuustoimenpiteet määriteltiin jo tammikuussa 2012, jotta niiden pohjalta tehtävää tiedonkeruuta voitiin alkaa testaamaan. Tiedonkeruuta varten on tehty lomake, johon tiedot tallennetaan. Tarkoituksena oli määrittää vain muutama keskeinen asia, joiden avulla voidaan tehokkaimmin ennaltaehkäistä tuotetietovuotoja. Salassapito-ja tuotelainasopimukset tulee olla tehtynä, ennen kuin tietoa tai prototyyppeja voidaan jakaa yhteistyökumppanille. Viimeisin versio yleisistä turvallisuusvaatimuksista tulee olla liitettynä sopimukseen. Nämä vaatimukset pitävät sisällään myös tuotetiedonkäsittelyyn liittyviä erityisvaatimuksia. Yhteistyökumppanin turvallisuustason nykytila tulee olla katselmoituna, joko itsearvoinnin perusteella tai auditoinnin perusteella. Kyseisessä toimenpiteessä löydetyt puutteet tulee olla korjattuna yhteisesti sovitun ajan puitteissa.

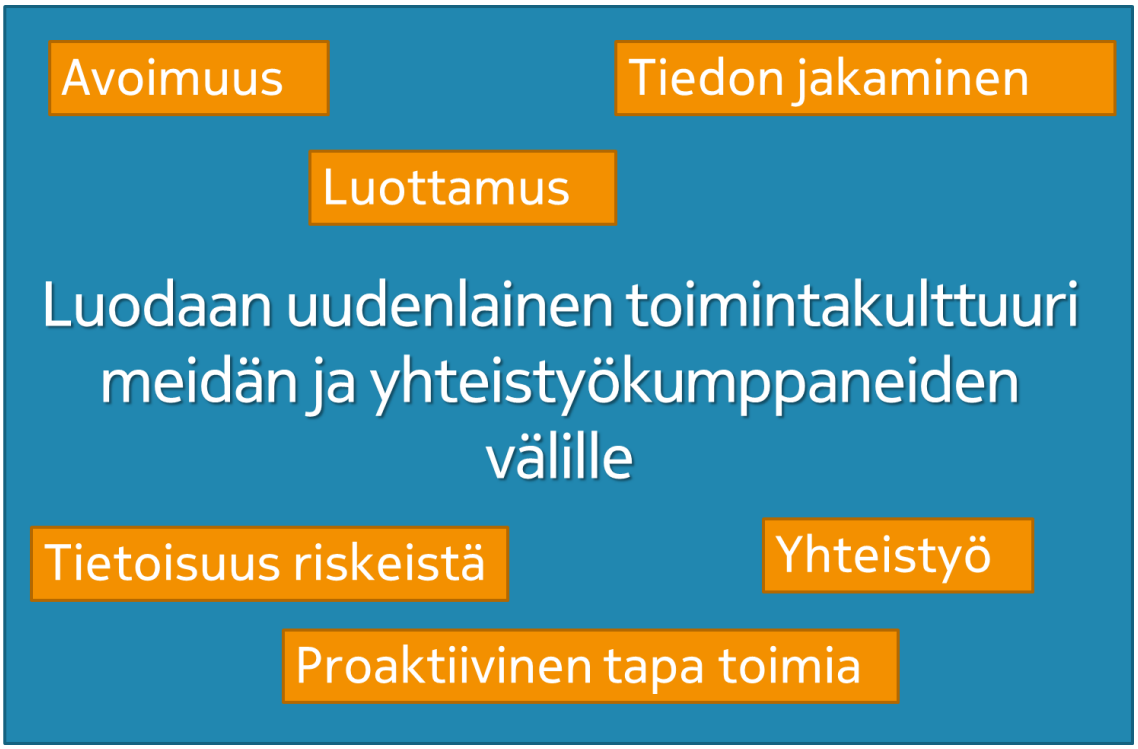
Yhteistyökumppanin johdon tulee olla tietoinen projektiin liityvistä riskeistä ja niitä pienentävistä toimenpiteistä. Johdon tulee myös osoittaa sitoutumisensa turvallisuustason ylläpitämiseen ja mahdolliseen kehittämiseen. Yhteistyökumppanin projektiryhmä tulee perehdyttää tuotekohtaiseen turvallisuusohjeeseen, joka määrittää ne käytännön toimenpiteet, jotka yksilöltä vaaditaan tuotetiedon suojaamisen varmistamiseksi. Perehdytys tapahtuu tilanteesta riippuen, joko Nokian tai yhteistyökumppanin vastuuhenkilön toimesta. Yhteistyökumppanin tulee käyttää prototyyppien rekisteröintityökalua, jonka avulla tiedetään, kenellä kyseinen laite on käytössä. Mikäli toimittavan kyvykkyyksissä on puutteita, ne tullaan korjaamaan kehittämishankkeen aikana. Yhteistyökumppanilta edellytetään myös kyvykkyyttä reagoida mahdollisiin vuototilanteisiin ja informoimaan Nokiaa välittömästi.

9.7 Menetelmien jalkauttaminen vaihe 1

9.7.1 Kulttuurin muuttaminen

Yhtenä jalkauttamisen keskeisenä teemana on ollut kulttuurin muuttaminen, jotta pystyttäisiin luomaan luottamuksen ilmipiiri, jossa ihmiset toimivat vastuullisesti. Viestiä on välitetty sekä sisäisissä koulutuksissa että yhteistyökumppaneiden kanssa toimittaessa. Sisäisesti on osoitettu ihmisille, että vuotoja tapahtuu useiden eri tahojen toimesta, eivätkä yhteistyökumppanin työntekijät vuoda yhtään enempää kuin omat työntekijät. Yhteistyökumppanien kanssa viestittäessä on korostettu Nokian luottamusta siihen, että he osaavat toimia vastuullisesti ja huolellisesti käsitellessään Nokian arvokasta materiaalia. Luottamusta on rakennettu myös kertomalla avoimesti Nokian haasteista tietovuotojen

kanssa. Alla olevasta kuvasta näkyy kommunikoituja arvoja, joiden avulla on lähdetty kehittämään kulttuuria.



Kuvio 8: Uudenlaisen kulttuurin rakentaminen.

9.7.2 Sisäisten sidosryhmien sitouttaminen

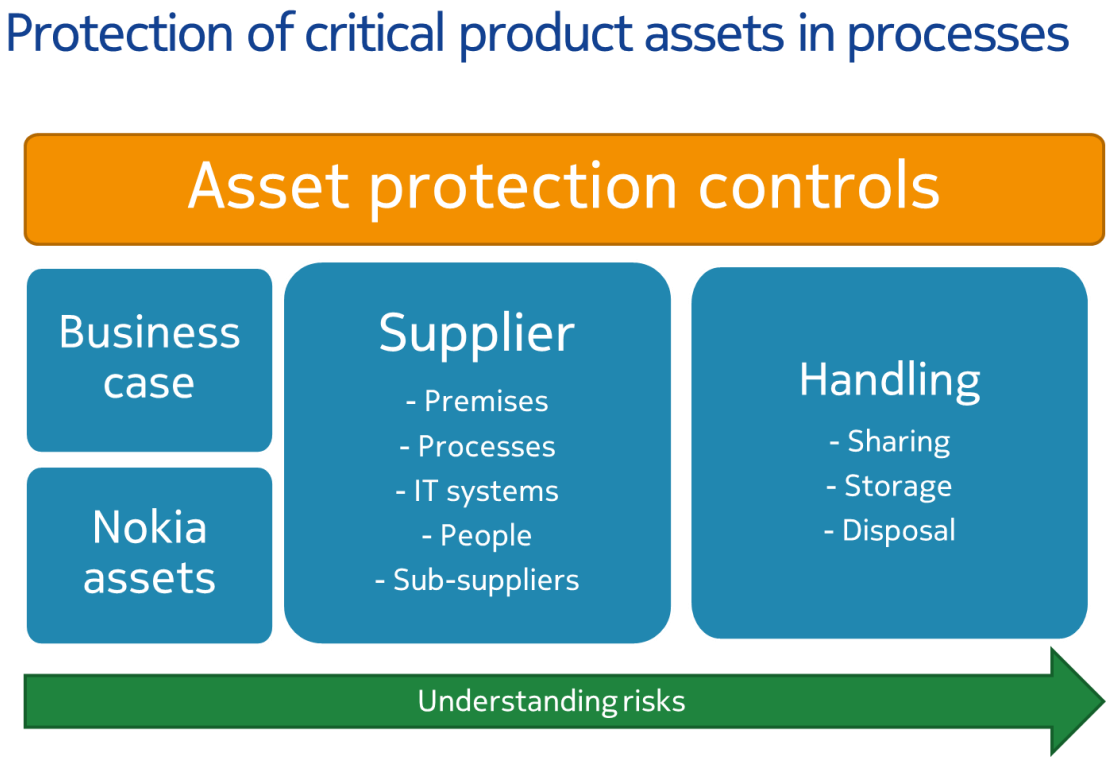
Nokian hankintayksikön työntekijät koulutettiin huhtikuun 2012 ja kesäkuun 2012 välisenä aikana. Koulutuksia varten kasattiin 1,5 tunnin pituinen koulutusmateriaali, jota jalkautettiin luokkahuonekouluksina ja virtuaalikoulutuksina. Koulutuksessa käytiin läpi sisäisiä turvallisuusohjeita sekä esiteltiin, kuinka tuotetietovuotoja ennaltaehkäistään yhteistyökumppaniverkostossa ja mitä on heidän roolinsa tässä työssä. Muille sisäisille kommunikoitiin samanlaisia asioita heille räätälöidyissä koulutuksissa. Smart Devices ja Mobile Phones yksiköiden ohjeisiin lisättiin yksi sivu, jossa kerrottiin kuinka yhteistyökumppanien kanssa tulee toimia, kun käsitellään luottamuksellista tuotetietoa.

9.7.3 Liiketoiminta –ja prosessilähtöisyyden tuominen osaksi toimintaa

Jalkautusvaiheen aikana yhtenäistettiin tapaa käsitellä yhteistyökumppaneita, jotka käsittelevät julkaisematonta tuotetietoa. Turvallisuustoimenpiteet määritettiin ja integroitiin osaksi kumppanin valintaprosessia. Muodollisten kontrollien, kuten sopimusten lisäksi lisättiin yksi sosiaalinen kontrolli, jolla pyritään vaikuttamaan yhteistyökumppaneiden työntekijöiden

turvallisuuskäyttäytymiseen. Turvallisuusperehdytys otettiin osaksi turvallisuusyhteistyötä kumppanin kanssa.

Aikaisemmin haasteena olivat väärin kohdistelut auditoinnit, jotka keskittyivät pääosin yleisiin turvallisuusjärjestelyihin. Arvokkaan tiedon liikkeet prosesseissa ja ihmisten turvallisuusosaaminen jäivät vähemmälle arvioinnille, vaikka juuri nämä asiat ovat merkittäviä, kun tarkoituksena on ennaltaehkäistä vuotoja. Jalkautusjakson aikana luotiin sisäistä koulutusmateriaalia ja käytiin keskusteluita auditoijien kanssa, jotta nämä kohdistaisivat katseensa myös prosesseihin ja ihmisiin. Viestiä vietiin muun muassa alla olevan kuvan ja käytännön esimerkkien avulla. Tämä viesti oli myös osana hankintayksikön koulutuksia.



Kuvio 9: Tuotetiedon suojaaminen prosesseissa.

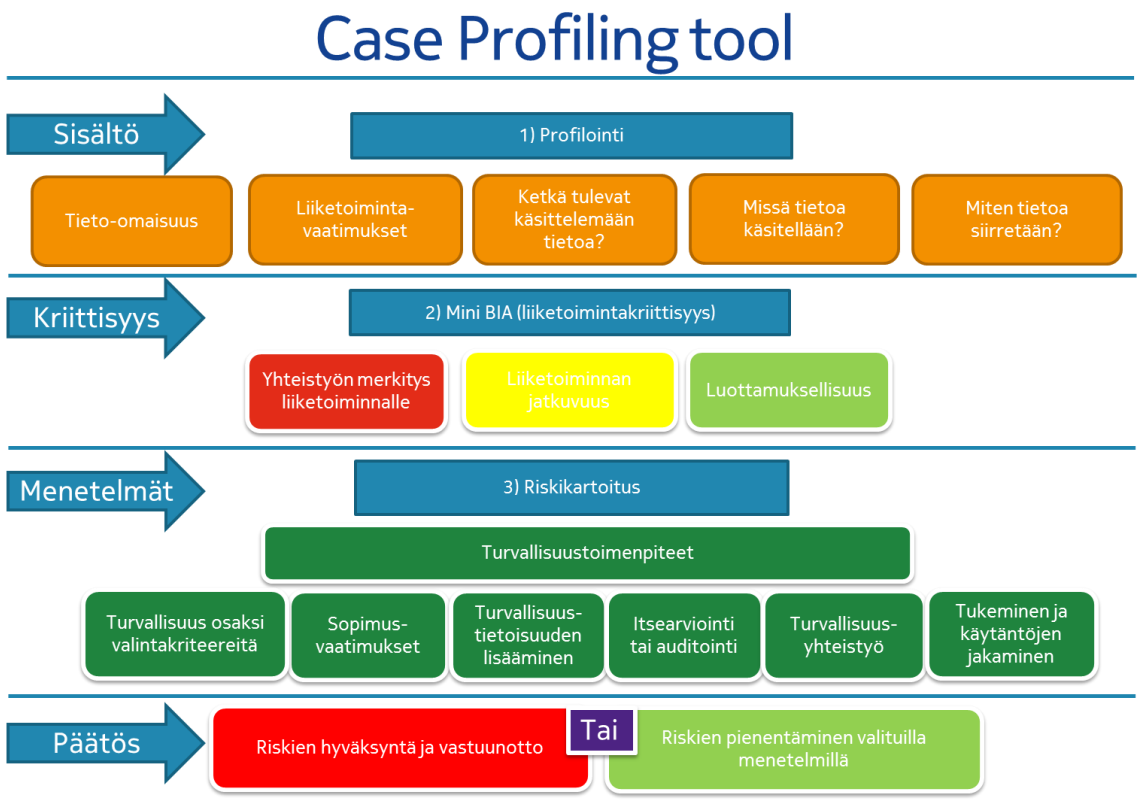
9.7.4 Turvallisuustietoisuuden lisääminen yhteistyökumppaniverkostossa

Tämä osa-alue on vienyt eniten aikaa, koska yhteistyökumppaniverkostomme on laaja ja pitää sisällään erilaisista kulttuurista tulevia yrityksiä sekä ihmisiä. Keskitimme turvallisuustietoisuuden lisäämiseen Mobile Phones ja Smart Devices yksiköiden yhteistyökumppaneihin. Jakson aikana koulutimme ja perehdytimme useita kymmeniä yhteistyökumppaneita ja jossain tapauksissa heidän käyttämiään alihankkijoita. Koulutuksen

lisäksi jaomme heille prototyyppien käsittelyohjeita ja liiketoimintayksikkökohtaisia tuotetietojen käsittelyohjeita, joista olimme tehneet kumppaniversiot. Edellä mainittujen ohjeiden lisäksi teimme kaksi uutta liiketoiminta-alue kohtaista ohjetta. Toinen tehtiin Design-yksikkömme yhteistyökumppaneille ja toinen puolestaan määritteli miten varhaisen vaiheen kuluttajatutkimukset tehdään turvallisesti. Koulutuksia tehtiin luokkahuoneissa ja virtuaalisesti. Osassa tapauksissa koulutimme muutaman henkilön yhteistyökumppaniyrityksestä, jotka puolestaan kouluttivat muun henkilöstön. Välillä taas me koulutimme koko henkilöstön, erityisesti silloin kun kyseessä oli pieni yritys.

9.7.5 Vahinkoriskien arviointi osaksi hankintaprosessia

Loimme yhdessä hankintayksikön kanssa vaiheen heidän prosessiinsa, jossa arvioidaan yhteistyöhön liittyvät vahinkoriskit ja tietenkin valitaan keinot riskien pienentämiseksi. Tämän vaiheen tekemistä varten olemme luoneet työkalun, joka helpottaa ja jopa nopeuttaa arvioinnin tekemistä. Työkalun nimi on case profiling tool ja sen tarkoituksena on auttaa hankintayksikön työntekijöitä ymmärtämään yhteistyöhön liittyvät riskit ja sitten valitsemaan sopivimmat turvallisuuskontrollit riskien pienentämiseksi. Aiheesta järjestettiin useita tietoiskuja jalkauttamisvaiheen aikana. Alla oleva kuvio näyttää millaisia vaiheita työkalu pitää sisällään.



Kuvio 10: Case profiling tool.

9.7.6 Yhteistyökumppaneilta edellytettävä turvallisuuskyvykkyys

Yhteistyökumppaneilta edellytettävä kyvykkyys kommunikoitiin Nokian hankintayksikölle osana kevään 2012 koulutuksia. Samoja asioita on kommunikoitu yhteistyökumppaneille, osana heidän perehdytyksiään. Myös auditointeja tekeville henkilöille on painotettu, että kumppanin kyvykkyys on arvioitava osana auditointia.

Tuotetietovuotojen ennaltaehkäisyyn liittyvät vaatimukset

Vaatimus (pakollinen)	Kontrolli (muodollinen / sosiaalinen)
Salassapito- ja tuotelainasopimukset	Muodollinen
Yleiset turvallisuusvaatimukset sopimuksessa	Muodollinen
Kumppanin turvallisuuskyvykkyys on katselmoitu	Muodollinen
Kumppanin johto on sitoutunut turvallisuuteen	Muodollinen & sosiaalinen
Prototyypit on rekisteröity Nokian järjestelmään	Muodollinen
Liiketoimintakohtaiset ja käytännölliset ohjeet on kommunikoitu kumppanin työntekijöille	Sosiaalinen
Kumppanilla on riittävä kyvykkyys reagoida tietovuotoihin	Muodollinen & sosiaalinen
Vapaavalintainen	**Kontrolli (muodollinen / sosiaalinen)**
Nokian käytäntöjen hyödyntäminen protolähetyksissä	Muodollinen & sosiaalinen
Riskienhallintayhteistyö	Sosiaalinen

Taulukko 4: Tuotetietovuotojen ennaltaehkäisyyn liittyvät vaatimukset.

9.7.7 Korkean riskitason projektin turvallisuusjärjestelyt

Saimme kesäkuun alussa yhteydenoton eräästä liiketoimintayksiköstä, joka oli aloittamassa korkean riskitason projektia kahden yhteistyökumppanin kanssa. Tässä tapauksessa korkea riskitaso liittyi suoraan projektissa käsiteltäviin tietoihin. Projektin aineistona oli erittäin varhaisia malleja tulevasta tuotteesta ja videoita käyttöliittymästä. Nämä tiedot piti jakaa näille kahdelle yhteistyökumppanille. Kun kyselimme lisää projektista, niin saimme selville, että osana projektia toinen yhteistyökumppani lähettää arvokasta materiaalia omille alihankkijoilleen useaan kohteeseen ympäri maailmaa. Muutenkin kävi selväksi, etteivät

mukana olleet yhteistyökumppanit olleet kovinkaan kyvykkäitä turvallisuusasioissa. Käytännössä tämä tarkoitti sitä, että meidän täytyi ottaa hieman vahvempi rooli, jotta saamme varmistettua, ettei mitään ikävää tapahdu.

Teimme kohdeympäristöihin sopivat turvallisuusohjeet, jotka keskittyivät arvokkaan tiedon suojaamiseen. Tämän jälkeen kävimme ohjeet läpi yhteistyökumppanien ja heidän alihankkijoidensa kanssa. Tämän jälkeen organisoimme arvokkaiden laitteiden ja videoiden siirtämisen ympäri maailmaa. Organisoimme myös tarkastuskäynnit kohteisiin, joissa laitteita ja tietoa säilytettiin. Tämä projekti vaati paljon resursseja, mutta toisaalta sillä päästiin liiketoiminnan asettamaan tavoitteeseen ja saimme myös kehittyä usean yrityksen turvallisuuskyvykkyyttä liittyen arvokkaan tuotetiedon käsittelyyn.

9.8 Arviointi toimenpiteiden toimivuudesta

Jalkautetut menetelmät tuottivat hyviä tuloksia. Esimerkiksi Mobiles Phones-yksikköä tukevassa yhteistyökumppaniverkostossa ei tapahtunut yhtään vuotoa. Tämä osoittaa, että valitsemamme turvallisuuskulttuurin ja turvallisuusviestien jalkautusmenetelmät toimivat laajassa mittakaavassa. Saimme paljon positiivista palautetta yhteistyökumppaneilta, koska lähestymistapamme poikkesi merkittävästi siitä, mihin he olivat tottuneet. He selvästi arvostivat läpinäkyvää ja vuorovaikutteista lähestymistapaa. Sisäisten sidosryhmien koulutukset sujuivat hyvin ja havaitsimme, että viesti meni perille, koska hankintayksikön suunnasta tulevat yhteydenotot kasvoivat merkittävästi. Jalkauttamamme muutokset hankintaprosessiin ja uusi työkalu lisäsivät varmasti osaltaan yhteydenottojen määrää. Korkean riskitason projektin aikana opimme, miten tuollaiset tiukan aikataulun omaavat ja erittäin haastavat projektit hoidetaan tyylikkäästi.

Käytännössä valitut menetelmät toimivat halutulla tavalla. Ainoana haasteena olivat Nokian sisäiset järjestelyt, joiden seurauksena irtisanottiin paljon työntekijöitä. Vähennykset koskettivat kovasti hankintayksikköä, mikä tarkoitti sitä, että keväällä opitut turvallisuusasiat unohtuivat, koska ihmisten mieli oli muualla. Tämän lisäksi henkilöiden rooleihin tuli muutoksia ja monien työkuorma kasvoi merkittävästi. Käytännössä tämä tarkoitti sitä, että jalkauttamisvaiheen loppupuolella tuotetietovuotojen ennaltaehkäisytoiminta ei ollut kovinkaan tehokasta. Elokuussa tapahtui muutamia vuototapauksia Kiinassa, joissa yhteistyökumppaneiden työntekijät julkaisevat julkaisemattomia tuotekuvia internetissä. Parissa tapauksessa tietoja vuotanut henkilö oli vähän aikaa sitten koulutettu, joka oman yrityksensä tai Nokian toimesta. Nämä tapaukset osoittivat meille, että sosiaalinen paine ja internet-kulttuuri ovat monesti vahvempia, kuin turvallisuusviesti.

9.9 Uusien menetelmien valinta ja jalkauttaminen

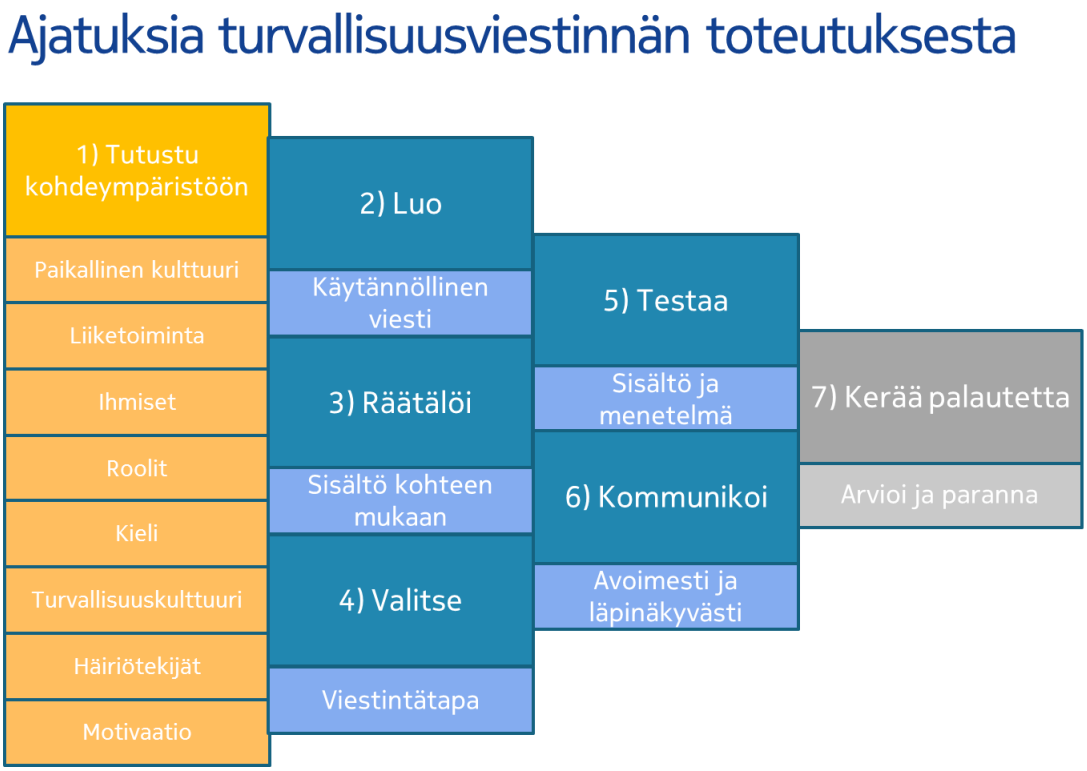
Jalkauttamisen ensimmäisessä vaiheessa hyödynnetyt menetelmät osoittautuivat toimiviksi ja niiden jalkauttamista tullaan jatkamaan. Seuraavan vaiheen panostukset tulevat olemaan pääosin siinä, miten saamme Kiinassa tapahtuvat vuodot vähenemään, kuitenkin niin, että painopiste on yhteistyökumppaneiden työntekijöiden motivoinnnissa ja heidän turvallisuustoisuutensa kehittämisessä. Painopiste on siis viestinnässä ja tietenkin uusien menetelmien kehittämisessä.

9.9.1 Sisäiset sidosryhmät

Hankintayksikön työntekijät koulutettiin kevään 2012 aikana, joten tässä jalkautusvaiheessa ei ollut tarvetta vastaavanlaiseen koulutusrupemaan. Hankintayksikön johto kuitenkin halusi, että syksyllä järjestetään yksi session osana yksikön sisäistä osaamisen kehittämistä. Tietotietovuotojen ennaltaehkäisy asiat tuli myös integroida osaksi hankintaprosessiin liittyvää yleistä turvallisuuskoulutusmateriaalia.

9.9.2 Yhteistyökumppaneiden turvallisuustietoisuuden parantaminen

Huomasimme elokuussa, että turvallisuusviestimme ei ollut saavuttaneet tarpeeksi useita Kiinassa toimivia kumppaneitamme. Tämä näkyi muun muassa vuotoina sellaisissa ympäristöissä, jotka eivät aikaisimmin olleet tärkeitä tuotetietovuotojen ennaltaehkäisynäkökulmasta. Toisaalta nämä ympäristöt olivat erittäin haastavia, koska kyseessä oli valmistusteollisuus Kiinassa, mikä tarkoitti muutoksia viestinnän toteutuksessa. Rakensimme alla olevan kuvion tukemaan turvallisuusviestinnän suunnittelua ja jalkauttamista uusissa kulttuureissa.



Kuvio 11: Ajatuksia turvallisuusviestinnän toteuksesta monikulttuurisessa ympäristössä.

Päätimme järjestää Kiinassa seminaarin siellä toimiville yhteistyökumppaneille, koska halusimme kommunikoida heille yhtenäisen viestin. Seminaaria suunnitellessamme pohdimme, että miten saisimme tilaisuudesta mahdollisimman vuorovaikutteisen. Ratkaisuksi keksimme, että jaemme seminaarin muutamiin osiin, joiden välissä olisi yhteisiä ideointihetkiä, joiden tuotokset kirjataan tauluille ja käydään läpi. Ensiksi pohdimme yhdessä, miten vuodot syntyvät. Tämän jälkeen ideoimme yhdessä tuotetietovuotojen ennaltaehkäisykeinoja. Tarkoituksena oli saada osapuolet jakamaan omien yritystensä käytössä olevia hyviä käytäntöjä. Yhdessä puheevuorossa esittelimme Nokian käyttämät ennaltaehkäisymenetelmät. Seminaari päättyi yhteiseen lounaaseen, koska halusimme sen avulla parantaa osallistujien yhteisöllisyyttä ja osaltaan jatkaa keskustelua aiheen parissa. Tilaisuudessa kerätyn palautteen perusteella osallistujat pitivät sitä onnistuneena. Seminaarin jälkeiset vuototilastot osoittavat myös, että tilaisuus oli yksi niistä tekijöistä, jotka auttoivat meitä pysäyttämään Kiinassa olleen vuotoepidemian.

Kuva 2: Tuotetietovuotojen ennaltaehkäisyseminaari Pekingissä.

Jatkoimme luonnollisesti yhteistyökumppaneiden kouluttamista ja ohjeistamista tietovuotovuotojen ennaltaehkäisyn saloihin. Tämän lisäksi loimme viestin hankintayksikön johtajalle, joka puolestaan lähetti sen kaikkien yhteistyökumppaniemme toimitusjohtajille. Tällä tavoin olemme saaneet vietyä viestiämme yhteistyökumppaniemme organisaatioiden eri tasoille.

9.9.3 Luottamuksellisten mekaniikkaosien suojaaminen

Uusimpien matkapuhelinten ulkoasuun liittyvät mekaniikkaosat paljastavat vuotaessa suurimman osa tulevan laitteen ulkonäöstä. Kuten aikemmin kirjoitin, niin laitteen laitteen ulkoasu on yksi keskeisimmistä suojattavista kohteista. Tämän vuoksi tuotekehitysyksikömme oli ideoinut kontrolleja, joiden tarkoituksena on varmistaa, ettei meidän mekaniikkaosiamme varasteta tai vuodeta ulos niiden ollessa yhteistyökumppanin tiloissa. Suojaustoimenpiteet pitävät sisällään osien merkkaamisen ja tarkan inventaarion pitämisen. Osia säilytään pääsynvalvotulla alueella jonne pääsevät vain harvat yhteistyökumppanin työntekijät. Yhteistyökumppani ei saa siirtää yhtään mekaniikkaosaa ilman Nokian lupaa. Ylimääräisten tai rikkoutuneiden osien tuhoaminen tapahtuu Nokian valvonnan alla. Tällä tavalla varmistutaan myös sitä, etteivät laitteet päädy kopiopuhelinvalmistajien käsiin. Suojaustoimenpiteet on kirjattu ohjeeksi, joka on kommunikoitu yhteistyökumppanille.

9.10 Arviointi toimenpiteiden toimivuudesta

Syksyllä menetelmiä valitessamme suurimmat haasteemme olivat Kiinassa. Tehostimme toimintaamme siellä ja onnistuimme löytämään toimivat jalkauttamismenetelmät, jotka vaikuttivat ihmisten turvallisuuskäyttäytymiseen ja paransivat prosessien turvallisuutta. Tämä osoittaa, että on tärkeää panostaa molempiin, turvallisuustietoisuuden kehittämiseen sekä prosesseihin, tiloihin ja tietojärjestelmiin liittyviin järjestelyihin. Seminaari oli oivallinen tapa tuoda toimijat yhteen huoneeseen, ideoida yhdessä sekä kommunikoida Nokian tahtotila tuotetietovuotojen ennaltaehkäisytyössä. Mekaniikkaosien suojaamistoimenpiteet ovat toimineet hyvin testituotteiden osalta ja nyt käytäntöjä tullaan hyödyntämään muissakin tuotteissa. Kokonaisuudessaan valitut turvallisuuskontrollit ja jalkauttamismenetelmät ovat auttaneet meitä vähentämään tuotetietovuotoja niissä ympäristöissä minne nämä toimenpiteet on päästy ulottamaan. Toisaalta tämä toimintatutkimus on vahvistanut näkemystämme siitä, että hyvällä yhteistyöllä ja sosiaalisiin kontrolleihin panostamalla päästään hyviin tuloksiin.

9.11 Johtopäätökset

Toimintatutkimuksen tavoitteena oli selvittää, millaisilla menetelmillä voidaan ennaltaehkäistä tuotetietovuotoja Nokian kansainvälisessä yhteistyökumppaniverkostossa. Osana tutkimusta tehtiin laaja-alainen nykytila-analyysi, jossa selvitettiin erilaisia tekijöitä, liittyen tuotetietovuotoihin ja niiden ennaltaehkäisytyön nykytilaan Nokian kansainvälisessä yhteistyökumppaniverkostossa. Analyysissä arvioitiin muun muassa viime vuosina toteutuneita tuotetietovuotoja ja niiden syitä, erilaisia sisäisiä ja ulkoisia tekijöitä, kuten Nokian turvallisuuskulttuuria. Nykytila-analyysin pohjalta pystyttiin identifioimaan useita kehittämisalueita, joiden parantamiseksi ryhdyttiin kehittämään ja jalkauttamaan parannustoimenpiteitä. Toimenpiteet pohjautuivat osittain tietoturvallisuuden kansainvälisiin hyviin käytäntöihin ja suurimmaksi osaksi Nokian sisällä hyviksi todettuihin tuotetietovuotojen ennaltaehkäisy menetelmiin. Toimintatutkiksen aikana näitä toimenpiteitä jalkauttiin sekä sisäisten sidosryhmien että yhteistyökumppanien keskuudessa. Toimenpiteiden pääpainopisteet olivat uudenlaisen kulttuurin luomisessa, sekä julkaisemattoman tuotetiedon parissa työskentelevien ihmisten turvallisuustietoisuustason nostamisessa. Kehittämistoiminnan painopiste oli liiketoimintalähtöisessä, sosiaalisia kontrolleja hyödyntävässä ihmisläheisessä ja avoimessa lähestymistavassa.

Tutkimuksen onnistumista arvioida neljää eri tekijää arvioimalla. Vuoden 2011 tilastojen mukaan 15% selvitetyistä tuotetietovuodoista tapahtui yhteityökumppaniverkoston toimesta. Ennaltaehkäisevien toimenpiteiden laajamittainen jalkauttaminen aloitettiin vuoden 2012 alkupuolella ja toiminta on jatkunut säännöllisesti vuoden 2013 helmikuun loppuun asti. Seuranta-aikana yhteistyökumppaniverkoston toimesta tapahtuneet tuotetietovuodot ovat pudonneet selvästi. Vuoden 2012 tilastojen mukaan yhteistyökumppaniverkostosta tulleiden

vuotojen osuus oli 11% ja vuoden 2013 kahden ensimmäisen kuukauden osalta 10%. Vuototilastojen mukaan voidaan siis todeta, että toimenpiteet ovat tehonneet toivotulla tavalla eli vuotoja laskevasti. Toisena arvioimistekijä voidaan pitää ennaltaehkäisevien toimenpiteiden toimivuutta niissä liiketoimintaympäristöissä, joihin on panostettu eniten. Mobile Phones-yksikön yhteistyökumppaneiden turvallisuustietoisuuden parantamiseen panostettiin kovasti vuoden 2012 aikana, minkä johdosta yksikään sitoutetuista ja koulutetuista yhteistyökumppaneista tai heidän työntekijöistään ei vuotanut tuotetietoa.

Kiinassa tapahtui useita vuotoja elo-syyskuussa 2012, mikä sai meidät analysoimaan tilannetta tarkemmin ja pohtimaan miten vuodot saisi loppumaan. Päätimme hyödyntää jo toimiviksi havaitsemiamme menetelmiä, tosin Kiinan kulttuurin huomioiden. Kutsuimme Kiinassa toimivat merkittävimmät yhteistyökumppanimme seminaariin, jossa aihetta käsiteltiin osapuolten kesken vuorovaikutteisesti ja rakentavasti. Tämän seminaarin jälkeen meillä ei ole ollut tunnistettuja tuotetietovuotoja, joiden taustalla olisivat olleet yhteistyökumppanit tai heidän työntekijänsä. Neljäntenä kohtana voidaan arvioida, tuottiko tutkimus uutta tietoa turvallisuusalalle? Tutkimusaineistoa kasatessani kävi ilmi, että tuotetietovuotojen ennaltaehkäisytyötä ei ole laajasti käsitelty teoriassa, eikä tutkimusten muodossa. Olemassa olevat tutkimukset ja julkaisut korostavat enemmänkin muodollisia kontrolleja eli lainsäändäntöön ja sopimuksiin liittyviä asioita. Tutkimuksessani hyödynnettiin useita menetelmiä, ja niitä jalkautettiin suhteellisen menestyksekkäästi eri kulttuureista tulleiden sidosryhmien keskuudessa. Tutkimuksessa syntynyt uusi tieto osoittaa, että sosiaalisia kontrolleja painottava jalkauttamismenetelmä tuottaa positiivisiä tuloksia tuotetietovuotojen ennaltaehkäisytyön näkökulmasta.

Johtopäätöksenä voidaan todeta, että Nokian yhteistyökumppaniverkostossa hyödynnetyt tuotetietovuotojen ennaltaehkäisevät menetelmät ovat tuottaneet toivotun tuloksen. Nokian tapa tehdä tuotetietovuotojen ennaltaehkäisytyötä on erilainen suhteessa monien muiden yritysten tapaan tehdä turvallisuustyötä yhteistyökumppanirajapinnassa. Tämä toimintatutkimus on auttanut Nokiaa löytämään toimivia menetelmiä, jotka tukevat sen avointa ja luottamukseen perustuvaa turvallisuuskulttuuria. Jatkossa tulemme käyttämään rakentamaamme jalkauttamismallia, jossa luodaan liiketoimintalähtöisiä ja käytännöllisiä ohjeita. Nämä ohjeet kommunikoidaan säännöllisesti yhteistyökumppaneille. Kommunikointia suunnitellessa huomioidaan kohdeyleisön kulttuuri ja itse kommunikointi tehdään avoimella sekä läpinäkyvällä tavalla. Mallia hyödyntämällä pyritään luomaan yhteinen turvallisuuskulttuuri, jossa kaikilla osapuolilla selvyys tavoitteista ja kuinka ne voidaan saavuttaa.

Lähteet

Adler, N.J. 1986. International Dimensions of Organizational Behavior. Kent Publishing Company.

Akamp, M. & Müller, M. 2012. Supplier management in developing countries. Journal of Cleaner Production.

Albrechtsen, E. Hovden, J. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers and Security 29.

Augustine, N. R. 1995. Managing the crisis you tried to prevent. Harward Business Review. (73(6).

Davis, A. 2010. Managing third parties – an information security perspective. Network Security.

Delerue, H. Lejeune, A. 2011. Managerial secrecy and intellectual asset protection in SMEs: The role of institutional environment. Journal of International Management 17.

Dhillon, G. 1997. Managing Information System Security, MacMillan Press Ltd, Great Britain.

Ebru, Y.Y. Gizem, A. Serpil, A. Nuran, B. 2010. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International Journal of Information Management 31.

Ferraro, G. P. 2005. The Cultural Dimensions of International Business. 5th Edition. Upper Saddle River. Pearson Prentice Hall.

Gudykunst, W.B. & Mody, B. 2002. Handbook of International and In-tercultural communication. 2nd Edition. Sage Publications Inc.

Helms, M.M. Ettkin, L.P. Morris, D.J. 2000. Viewpoint: The Risk of Information Compromise and Approaches to Prevention. Journal of Strategic Information Systems 9.

Hirsjärvi, S, Remes, P. Sajavaara, P. 1998. Tutki ja kirjoita. Tampere: Tammer-Paino Oy

Hofstede, G. 1993. Kulttuurit ja organisaatiot. Mielen ohjelmointi. Juva: WSOY.

Sussman, L. 2008. Disclosure, leaks, and slips: Issues and strategies for prohibiting employee communication. Business Horizons 51.

Information Security Forum. 2013. Securing the supply chain. Information security forum limited.

Information Security Forum. 2012. The standard of good practice. Information security forum limited.

ISO 9001. 2008. Quality management systems - requirements.

ISO/IEC 17799. 2005. Information technology – security techniques – code of practice for information security management. Switzerland.

BS ISO/IEC 27001. 2005. Information technology – security techniques – information security management systems – requirements. British Standard Institute.

BS ISO/IEC 27005. 2008. Information technology – security techniques – information security risk management.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Tampereen Yliopistopaino Oy. Tampere: Juvenes Print.

Karjalainen, M. 2011. Improving employees' information systems (IS) security behavior. University of Oulu.

Kraemer, S. Carayon, P. Clem, J. 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computer & Security Vol. 28, No 7.

Kuheli, R.S. 2010. Assessing insider threats to information security using technical, behavioral and organizational measures. Information security technical report 15.

Kuusisto, T. Ilvonen I. 2003. Information security culture in smalla and medium size enterprises. Frontiers of E-business Research.

Leppänen, Juha. 2006. Yritysturvallisuus käytännössä. Jyväskylä: Gummerus Kirjapaino Oy.

Li, W. Humphreys, P. K. Yeung, Andy. Cheng T.C.E. 2012. The impact of supplier development on buyer competitive advantage: A path analytic model. Int. J. Production Economics 135.

Loisa, M. 2002. Uuden tiedon luominen ja skenaariomenetelmä. Lappeenrannan teknillinen yliopisto.

Martins, A., Eloff, J. 2003. Information Security Culture, Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt. IFIP Conference Proceedings.

Mäkilouko, M. 2003. Multicultural Leadership – Strategies for Improved Per-formance. 1st Edition. Helsinki: Multiprint Oy.

Norman, P. 2001. Are your secrets safe? Knowledge protection in strategic alliances. Business Horizons.

Nykänen, K. 2011.Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Oulun Yliopisto.

Ojasalo, K. Moilanen, T. Ritalahti, J. 2009. Kehittämistyön menetelmät. WSOYpro Oy.

Pagnattaro, M.A. 2012. Preventing know-how from walking out the door in China: Protection of trade secrets Business Horizons.

Porvari, P. 2012. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Aalto University publications series. Helsinki: Unigrafia Oy.

Prajogo, D. Chowdhury, M. Yeung Andy, C.L. Cheng, T.C.E. 2012.The relationship between supplier management and firm's operational performance: A multi-dimensional perspective. Int. J. Production Economics 136.

Puhakainen, P. 2006. A Design Theory for Information Security Awareness. Ph.D. Thesis. University of Oulu, Dept Information Processing Science.

Richien, B. Brindley, C. 2007. Supply Chain Risk Management and Performance- a Guiding Framework for future development. International Journal of Operations and Production Management 27.

Siponen, T. 2000. A conceptual foundation for organizational information security awareness, Information Management & Computer Security 8/1.

Valtiovarainministeriö. 2003. Valtionhallinnon tietoturvakäsitteistö (VAHTI 4/2003). Helsinki: Edita Prima Oy.

Von Solms, B. 2000. Information Security - The Third Wave? Computers and Security 19.

Wagner, S, M. A strategic approach to professional supplier management. National productivity review 19 (3).

Yuan, L. En, X. Hock-Hai, T. Mike, W.P. 2010. Formal control and social control in domestic and international buyer–supplier relationships. Journal of operations management.

Sähköiset lähteet

@evleaks. https://twitter.com/evleaks. Viitattu 27.4.2013.

Kulttuuriguru. Kansainvälinen viestintä. Novomok Ltd.
http://www.uraverkko.net/kulttuuriguru/kulttuuri2.html. Viitattu 16.3.2013.

Laihonen, H. 2005. Peste-analyysi.
http://matwww.ee.tut.fi/hmopetus/hmjatkosems04/liitteet/JOS_hypermedia_Laihonen200505.pdf Viitattu 20.11.2012.

Li, C. 2013. Apple Corp Supplier Foxconn Workers Protest in China, Jiangxi Over Low Wages.
http://www.cristyli.com/?cat=186. Viitattu 28.3.2013.

Nokian liiketoiminnan esittely. Nokia. http://www.nokia.com/fi-fi/tietoa-nokiasta/yritys/tietoa-meista/tietoa-meista. Viitattu 26.2.2012.

Rikoslaki. 1990. (24.8.1990/769) Viitattu 10.3.2013.

Salo-Lee, Liisa 2003. Kulttuurien välinen viestintä.
http://www.jyu.fi/viesti/verkkotuotanto/yviperust/artikkelit/kulttuurienvalinen_viestinta.html. Viitattu 28.3.2013

Socialwavelenght. Social media mega trends. 2012.
http://www.socialwavelength.com/pdfs/Social_Media_Megatrends.pdf Viitattu 20.11.2012.

Tekes. 2012. Kansainväliset ilmiöt ja globaalit megatrendit.
http://www.tekes.fi/fi/community/Kansainv%C3%A4liset_ilmi%C3%B6t_%E2%80%93_globaalit_megatrendit/1066/Kansainv%C3%A4liset_ilmi%C3%B6t_%E2%80%93_globaalit_megatrendit/2354 Viitattu 5.12.2012.

Tulevaisuustutkimuksen oppimateriaali. 2012. http://www.tulevaisuus.fi/topi/ Viitattu 22.11.2012.

Työ-ja elinkeinoministeriö. 2009. Megatrendit.
http://www.tem.fi/files/22696/Megatrendit.pdf Viitattu 20.11.2012

Viestintävirasto. 2012. Katsaus viestintäviraston toimintaympäristöön 2012-2016.
http://www.epaper.fi/reader/?issue=24413;5ff45128081eeac1b906abcbc3037ae3;15 Viitattu 25.12.2012.

Kuvat

Kuviot

Taulukot