Verkkokoulutuksen vaikutus henkilöstön tietoturvallisuusosaamiseen teollisuusalan yrityksessä

Seppälä Eeli

2019 Laurea

Laurea-ammattikorkeakoulu

Verkkokoulutuksen vaikutus henkilöstön tietoturvallisuusosaamiseen teollisuusalan yrityksessä

Eeli Seppälä
Turvallisuusalan tradenomi
Opinnäytetyö
Toukokuu, 2019

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan tradenomi (AMK)

Eeli Seppälä

Verkkokoulutuksen vaikutus henkilöstön tietoturvallisuusosaamiseen teollisuusalan yrityksessä

Vuosi 2019 Sivumäärä 37

Opinnäytetyön aiheena oli selvittää tietoturvallisuusosaamisen lähtötaso eräässä yrityksen toimipisteessä, ja tietoturvakoulutuksen vaikutus siihen. Tämä opinnäytetyö on toiminnallinen. Opinnäytetyön toimeksiantajaa ei nimetä tässä työssä heidän pyynnöstään. Työn tuloksia tullaan hyödyntämään yrityksessä tietoturvallisuuskulttuurin kehittämisessä.

Opinnäytetyön teoreettisessa viitekehyksessä käsiteltiin tietoturvallisuutta, sen kehitystä ja tulevaisuudennäkymiä, sekä muita tähän opinnäytetyöhön liittyviä keskeisiä tekijöitä. Aluksi selvitettiin tietoturvallisuuden teoriaa ja perusperiaatteita. Tämän jälkeen tarkasteltiin yleisimpiä alaan liittyviä lainsäädännöllisiä määreitä ja standardeja, ja niiden merkitystä yrityksen tietoturvallisuuspolitiikkaa luotaessa. Lisäksi käsiteltiin tietoturvallisuuden kehitystä ja muutosta tulevaisuudessa. Osa käytetyistä lähteistä on yrityksen sisäiseksi luokiteltua tietoa, joten sitä käsitellään vain rajatusti ja otsikkotasolla. Tutkimuksen tavoitteena oli kehittää henkilöstön tietoturvallisuusosaamista. Työn tarkoituksena oli selvittää, kasvoiko osaaminen verkkokoulutuksen julkaisemisen jälkeen.

Kyselytutkimus toteutettiin kaksiosaisena, sähköisenä kyselytutkimuksena. Kyselyn jako vastaajille tapahtui toimeksiantajan sisäisten viestintäkanavien välityksellä. Kyselyn kysymykset muotoituivat verkkokoulutuksessa käytävien kokonaisuuksien pohjalta. Ensimmäisen kyselyn tarkoitus oli selvittää tietoturvallisuuden nykytila, ja toisen kyselyn tarkoituksena oli selvittää mahdollinen muutos vastauksissa koulutuksen järjestämisen jälkeen. Vastaajilta pyrittiin selvittämään esimerkiksi, miten he kokevat tietoturvallisuuden sekä olivatko tietoturvallisuuden näkökulmasta turvalliset työtavat tiedossa.

Tutkimuksen tulokseksi saatiin selville tilanne verkkokoulutuksen jälkeen. Tuloksista kävi ilmi, että aiempi tietoturvaohjeiden puute vaikutti vastaajien osaamiseen. Vastaajat osoittivat kuitenkin mielenkiintoa tietoturvallisuutta kohtaan, ja tiedostivat esimerkiksi oman vastuunsa. Tietoturvallisuusosaaminen ennen verkkokoulutusta oli verrattain heikolla tasolla. Koulutuksen käymisen jälkeen vastaajien tulokset olivat kuitenkin parantuneet huomattavasti, ja vastaajat kokivat myös itse koulutuksen parantaneen heidän osaamistaan.

Asiasanat: Tietoturvallisuus, tietoturvallisuusosaaminen, verkkokoulutus

Laurea University of Applied Sciences
Degree Programme in Security management

Abstract
Bachelor's Thesis

Eeli Seppälä

The effectiveness of an e-learning program on information security for personnel in an industrial company

Year 2019 Pages 37

The objective of this bachelors' thesis was to examine the level of information security knowledge in one of the company's offices, and what effect an e-learning program have on it. This thesis is functional. The commissioner for this thesis shall not be named on their request. The results will be used to increase information security awareness in the company.

The theoretical framework of the thesis examines information security, its development over the years and the future view. In the beginning of the framework is information security and its basic principles are covered. Some of the most common legislation and standards, and their meaning in creating an information security policy, are also covered. Some of the sources used for this thesis include the commissioner's internal information and therefore it is not disclosed in its full context.

The survey was executed in two parts. The distribution to the respondents was done in the company's internal communication channels. The questions were based on the e-learning material. The first surveys purpose was to map the present state of the knowledge in the area, and the second survey was conducted in order to scrutinize if there were any differences. The respondents were asked questions regarding for example information security in their job assignments and whether they knew how to do their work safely.

The result of the survey was a report of the situation after the e-learning program. The results showed the lack of knowledge in information security before the program, since there was not much information security in use. The respondents showed interest in information security in the first survey, and for example knew their responsibility in information security related matters. After going through the e-learning program the responses we're vastly improved, and the respondents themselves also thought that the program increased their expertise on the subject.

Keywords: Information security, Information security awareness, e-learning

Sisällys

1 Johdanto

Teknologian kehittyessä on yritysten reagoitava uusiin, erilaisiin ja alati kehittyviin riskeihin. Tietoturvallisuuspuolella tämä tarkoittaa yhä kehittyneempiä suoria uhkia yritysten infrastruktuuriin ja toimintaan esimerkiksi tietojenkalasteluyritysten muodossa. (Infradata 2018.) Alati kehittyvät uhat vaativat uusien teknisten ratkaisujen lisäksi myös yhä tehokkaampaa tiedottamista sekä uusia turvallisuusjohtamisen ja -organisoinnin keinoja (Nobles 2018).

Tietoturvallisuusriskit käyvät yrityksille kalliiksi. IBM:n vuonna 2018 tekemän tutkimuksen mukaan keskimääräinen tietovuoto maksoi yrityksille 3,86 miljoonaa Yhdysvaltain dollaria ($). Vaikka suurin osa tietovuotojen juurisyistä johtuu erilaisista hyökkäyksistä, näihinkin riskeihin voitaisiin varautua paremmin henkilöstön tietoturvallisuusosaamista lisäämällä. (IBM 2018.)

Suurin osa maailmalla tapahtuneista tietoturvallisuusmurroista johtuu pohjimmiltaan ihmisistä. Vuotoja tapahtuu sekä loppukäyttäjien sekä IT-henkilöstön toimesta, lähinnä siitä syystä, että hyökkäykset ja uhat ovat jatkuvasti kehittyviä, ja varsinkin suurissa yrityksissä on vaikeaa pysyä ajan tasalla ja tiedottaa näistä koko henkilöstöä. (Maurer 2015). Yleisimpiä ihmisten tekemiä tietoturvallisuusvirheitä on esimerkiksi erilaisten haittaohjelmia sisältävien verkkosivujen tai tiedostojen avaaminen, kirjautumistietojen jakaminen tai ylös kirjoittaminen tai henkilökohtaisten laitteiden käyttäminen työkäyttöön (Kaspersky Lab 2018).

Luvussa 1 esitellään tämän opinnäytetyön taustat, tavoitteet ja tarkoitus. Tämän lisäksi esitellään toimeksiantaja sekä tutkimuskysymykset. Luvuissa 3 ja 4 käydään läpi opinnäytetyön teoreettinen viitekehys, jossa käydään läpi tietoturvallisuutta yleisesti, tiedon luokittelun ja salauksen periaatteita, sekä alan kehitystä ja tulevaisuudennäkymiä. Luvussa 4 käsitellään valittua tutkimusmenetelmää sekä tutkimuksen kulkua. Luvussa 5 käydään läpi opinnäytetyön prosessi ja luvussa 6 työn tulokset. Opinnäytetyön lopussa on vielä johtopäätökset sekä oman työn arviointi kappaleessa 7.

1.1 Työn tausta ja toimeksiantaja

Toimeksiantajalla ei ollut aikaisemmin ollut voimassa olevaa laajamittaista tietoturvallisuuskoulutusta. Tietoturvallisuutta on koulutettu paikoittain ainoastaan henkilöille, jotka ovat koulutusta ehdottomasti tarvinneet työtehtävänsä suorittamiseen. Syksyllä 2018 julkaistu tietoturvallisuuskoulutus oli siis toimeksiantajalle ensimmäinen laatuaan.

Opinnäytetyön toimeksiantajaa ei nimetä tässä opinnäytetyössä heidän toiveestaan. Toimeksiantaja toimii teollisuuden alalla, ja heillä on useita toimipisteitä useassa eri maassa. Henkilöstön määrä lasketaan tuhansissa, ja laajamittainen tietoturvallisuuden hallitseminen tällaisessa ympäristössä on ymmärrettävästi sekä haastavaa että tarpeellista. Kyselytutkimuksen

kohteena olleessa toimipisteessä työskentelee noin 100 ihmistä. Yrityksen tietoturvapolitiikassa määritellään riittäväksi koetut suojauskeinot. Politiikka määrittelee raamit manuaalille, joka tehtiin tukemaan tietoturvallisuustietoisuuden lisäämistä yrityksessä. Manuaalin tarkoitus on olla peruskäyttäjälle helposti saatavilla oleva apuväline arkisiin tilanteisiin, jossa tietoturvakäytännöt eivät välttämättä muistu mieleen.

Verkkokoulutuksen sisältö pohjautuu samaan aikaan yrityksen sisäisessä tiedonjaossa julkaistuun tietoturvallisuusmanuaaliin. Perusteellisesta, yrityksen tietoturvallisuusstrategiaan pohjautuvasta manuaalista on pyritty valitsemaan tärkeimmät kokonaisuudet, jotka ovat tietoturvallisuuden näkökulmasta tarkasteltuna työntekijöille kaikkein olennaisimpia heidän jokapäiväisessä toiminnassaan. Manuaalia suunniteltaessa olikin sen pääpaino ymmärrettävyydessä ja selkeydessä, ja se pitäytyy lähinnä kansankielisinä keinoina tietoturvallisuuden parantamiseksi. Manuaali itsessään on kohtalaisen raskasta luettavaa, eikä se pelkästään asiakirjana ole riittävä keino työntekijöiden motivoimiseen tietoturvallisuuskulttuurin kehittämiseen. Verkkokoulutuksessa nämä asiat on käyty läpi tiivistetysti. Verkkokoulutuksen pyrkimyksenä oli saada vähintäänkin tärkeimmäksi koetut asiat opetettua henkilöstölle nopeasti ja tehokkaasti. Tärkeimmäksi koettuja osa-alueita oli esimerkiksi tietojenkalastusyrityksiä vastaan puolustautuminen, erilaiset turvalliset työtavat paikasta riippumatta sekä mahdollisista poikkeamista raportointi.

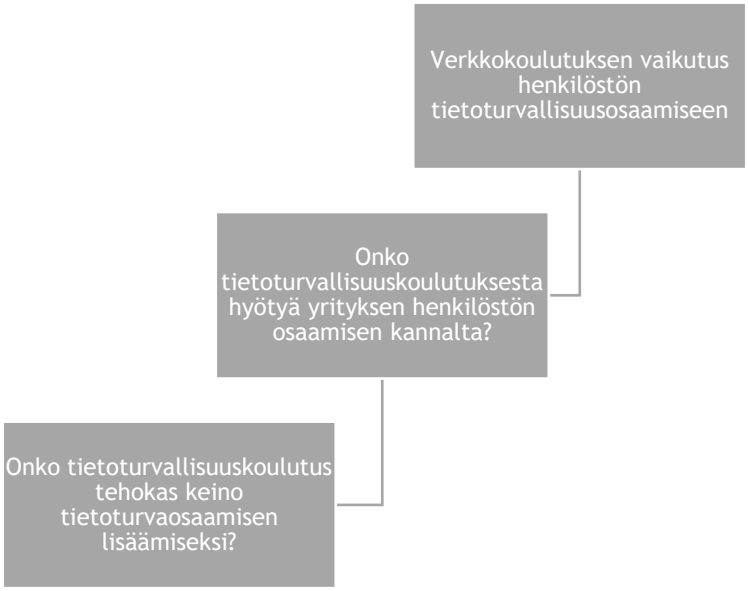
Tietoturvakoulutuksen ytimessä on erityisesti tietoisuuden levittäminen hyvän tietoturvallisuuskulttuurin ylläpidon tarpeellisuudesta. Sen lisäksi koulutuksessa on eriteltynä muutamia tärkeimpiä tietoturvallisuuden käsitteitä, sekä myös erilaisia keinoja, joilla jokainen työntekijä voi henkilökohtaisesti vaikuttaa yrityksen hallitseman tiedon suojaamiseen. Aiheesta teki mielenkiintoisen se, että tilannetta haluttiin tutkia nimenomaan ennen ja jälkeen koulutuksen.

Työ rajattiin koskemaan tietoturvallisuuden lähtötasoa sekä koulutuksen jälkeistä tulosta aluksi yhdellä yrityksen toimipisteistä. Johtuen toimipisteessä työskentelevien henkilöiden työn laadusta ja tietoturvallisuuden tärkeydestä tässä ympäristössä pitäydyttiin juuri tässä osassa laajamittaisemman tutkimuksen sijaan. Koulutuksen jalkautus tapahtui myös vaiheittain, ja kyseinen toimipiste oli ensimmäisiä, jossa koulutus otettiin järjestelmällisesti läpikäytäväksi.

1.2 Tutkimuskysymykset ja keskeiset käsitteet

Tämän opinnäytetyön tavoitteena on kehittää henkilöstön tietoturvaosaamista, ja löytää kehitettäviä osa-alueita verkkokoulutuksessa. Tähän tarkoitukseen tehtiin kaksi eri kyselyä yhden toimeksiantajan toimipaikan henkilöstölle, ennen ja jälkeen tietoturvallisuuskoulutusten pitämisen. Koulutukset järjestettiin verkkokoulutuksena.

Tämän opinnäytetyön tarkoituksena oli selvittää, saatiinko tietoturvallisuuskoulutuksen avulla lisättyä henkilöstön tietoisuutta ja osaamista tietoturvallisuuteen liittyvien riskien hallinnassa. Tutkimuksen pohjalta on yrityksessä tarkoitus tarjota tietoturvallisuuskoulutus yrityksen joka työntekijälle, ja selvittää mahdollisia lisäkoulutustarpeita tiettyihin tietoturvallisuuden osa-alueisiin liittyen. Suurikokoisessa yrityksessä täytyy miettiä myös, mitä kustannuksia kouluttamisesta syntyy, mikäli koulutus halutaan pitää jokaiselle työntekijälle. Näiden perusteiden pohjalta valikoitui tutkimuskysymyksiksi seuraavissa kappaleissa esitettävät kysymykset. Kuviossa 1 on esiteltynä tämän opinnäytetyön tutkimuskysymykset. Toiseen tutkimuskysymykseen ”Onko tietoturvallisuuskoulutus tehokas keino tietoturvaosaamisen lisäämiseksi?” on tarkoitus vastata ensimmäisen tutkimuskysymyksen vastauksen selvittämisen jälkeen.



Kuvio 1: Opinnäytetyön tutkimuskysymykset

Opinnäytetyössä etsitään vastauksia seuraaviin kysymyksiin: Onko tietoturvallisuuskoulutuksesta hyötyä yrityksen henkilöstön osaamisen kannalta? Onko tietoturvallisuuskoulutus tehokas keino tietoturvatietoisuuden lisäämiseksi? Ensimmäinen tutkimuskysymys liittyy suoraan kyselytutkimuksesta saatujen tulosten analysointiin. Valmiiksi asetettuja mittareita ei ollut, sillä yrityksessä ei aiemmin ollut tutkittu tietoturvallisuuden tasoa. Lähtökohtana oli, että kyselyiden tuloksia vertaillaan, ja tutkitaan prosentuaalisia muutoksia vastausten välillä johtopäätösten tekemiseksi.

Ensimmäisen tutkimuskysymyksen tulosten perusteella oli tarkoitus tutkia, onko verkkokoulutus kustannustehokas tapa tuoda tietoisuutta ilmi, vai pitäisikö sen levittämiseksi mahdolli-

sesti keksiä muita keinoja. Kaikkien työntekijöiden saavuttamiseksi vaaditaan joka tapauksessa paljon soveltamista, aikaa ja rahaa, eli tehokkaimman keinon löytäminen on tärkeää myös jatkuvuuden kannalta.

1.3 Keskeiset käsitteet

Tietoturvallisuus: Tietoturvallisuudella tarkoitetaan keinoja ja prosesseja, joilla varmistetaan suojattavan tiedon käytettävyys, luottamuksellisuus ja eheys. Suojattava tieto voi olla missä muodossa tahansa, esimerkiksi sähköisenä tai printattuna. Keinoja tietoturvallisuuden ylläpitämiseksi voi olla esimerkiksi sähköiset ja fyysiset suojakeinot tai tietoa käsittelevien henkilöiden kouluttaminen tiedon suojaamiseksi. (Valtionhallinnon tietoturvasanasto 2018 109.)

Tietoturvallisuusosaaminen: Tietoturvallisuusosaamisen lisäämisellä pyritään vaikuttamaan asenteisiin ja tapoihin, joilla tietoturvallisuuskulttuuria saadaan ylläpidettyä yrityksen sisällä. Tietoisuuden ylläpitämisellä pyritään saada henkilöstö tietoiseksi mahdollisista riskeistä sekä saada aikaan aktiivista toimintaa niiden estämiseksi ja tunnistamiseksi. (Martin 2014.)

Tietoturvallisuusmanuaali: Tietoturvallisuusmanuaalilla tarkoitetaan tässä työssä yrityksen sisäisessä tiedonjaossa olevaa ohjeistusta tietoturvallisuuden hallinnasta ja koulutuksesta yrityksen sisällä. Manuaalin keskeisimpänä tarkoituksena on lisätä tietoturvallisuustietoisuutta ja – osaamista yrityksen työntekijöiden keskuudessa. (Information security manual 2018.)

2 Tietoturvallisuuden kehitys ja tulevaisuuden näkymät

Tietoturvallisuus on jatkuvasti kehittyvä ja kasvava ala. Vuodesta 2017 tietoturvallisuuteen maailmanlaajuisesti yritysmaailmassa kulutettu summa on kasvanut 101 miljardista dollarista vuonna 2019 ennustettuun 124 miljardiin dollariin. (Gartner, 2018.) Alan kasvu johtuu niin uusien keinojen löytämisestä ja kehittämisestä uusien tietoturvallisuusriskien hallintaan, mutta myös yritysten heräämisestä sen tarpeellisuuteen. Tietoturvallisuuden kehitys tulee ennusteiden mukaan jatkumaan yhtä valtavana. Uusien ratkaisujen löytäminen ja ylläpitäminen avaa kymmeniä tuhansia työpaikkoja maailmanlaajuisesti. Yhdysvaltain työllisyysviraston arvion mukaan tietoturvallisuusanalyytikoita tulee vuonna 2026 olemaan lähes 30000 enemmän. Prosentteina tämä tarkoittaa 28 % kasvua vuosien 2018–2026 välillä. (Information security analysts 2019.)

Työpaikkojen ja sijoittamisen määrän kasvu ei tietenkään välttämättä ole pelkästään positiivinen asia, sillä kaikki tämä tapahtuu laillisesti toimivien tahojen kustannuksella. Vuonna 2018 tapahtui maailmanlaajuisesti yli 6500 tietomurtoa, joista kaksi kolmasosaa tapahtui yrityssektorilla. Suurimpana uhkana pysyi edellisistä vuosista hakkeroinnista johtuneet tietomurrot. (Constantin 2019.)

Positive Technologisien tutkimuksen mukaan (Cybersecurity threatscape: Q2 2018) vuosien 2017 ja 2018 välillä kyberhyökkäysten määrä kasvoi 47 %:lla. Saman tutkimuksen mukaan suurin osa näistä hyökkäyksistä kohdistui yrityksiin, ja käyttivät lähes kaikkia mahdollisia keinoja tietojen hankintaan: hakkerointia, sosiaalista manipulointia salasanojen saamiseksi ja yhteistyökumppaneihin iskemistä.

Prosentuaalisesti suurimpana kohteena hyökkäyksissä oli yritysten hallitsema tieto 40 %:lla. Tarkempana tietona työ osasi kertoa, että juuri henkilötiedot ovat hakkereiden kohteena, sillä niitä on helppo myydä eteenpäin. Usein henkilötietojen hakkerointiin liittyy uusiutumisen mahdollisuus, sillä osoitteet ja tiedot ovat tällöin usein myös muiden hakkereiden tiedossa tai myytynä toiselle taholle. Positive Technologies ennustaa jatkuvaa, nopeaa kasvua tietoja tavoittelevassa hakkeroinnissa, vaikka ennustaminen onkin lähes mahdotonta näin nopeasta kehityksestä puhuttaessa. (Positive Technologies 2018.)

2.1 Tietoturvallisuusuhkien hinta yrityksille

Suurilla ja paljon julkisuutta saavilla tietovuodoilla on yrityksiin sekä rahallista että maineellista vaikutusta. Vakavat tietoturvaloukkaukset ajavat pois niin asiakkaita kuin yhteistyökumppaneitakin, ja usein kuluttajaluottamuksen menetys näkyy yrityksissä vielä vuosienkin päästä. Keskimääräinen tietovuoto maksaa yrityksille maailmanlaajuisesti noin 4 miljoonaa dollaria. (Shepard 2018.)

Esimerkiksi loppuvuodesta 2018 Marriott –hotelliketjuun kohdistuneessa tietovuodossa hakkerit pääsivät käsiksi yli 350 miljoonan ihmisen henkilötietoihin, passinumeroihin sekä osoite –ja pankkitietoihin. Toistaiseksi Marriot on joutunut maksamaan vuodosta jo 28 miljoonaa dollaria suorina korvauksina, ja on edelleen haastettuna oikeuteen monesta rikkeestä. Usein suorat menetykset esimerkiksi juuri korvauksiin kuitenkin ovat vain noin 10 % kokonaiskustannuksista, mutta vaikutukset näkyvät usein vasta useamman vuoden päästä. (Kovacs 2019.) Internet-palveluntarjoaja TalkTalk puolestaan menetti arviolta 60 miljoonan punnan tulot ja lähes 100000 asiakasta, kun se menetti tietomurrossa yli 150000 asiakkaan henkilökohtaiset tiedot. (Burgess 2016.)

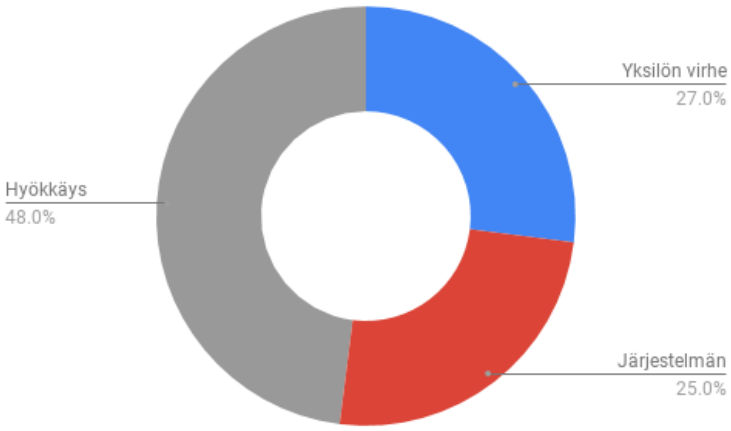
Myös GDPR asettaa kovia rangaistuksia henkilötietoihin kohdistuvista tietoturvaloukkauksista. Vakavasta tietovuodosta on asetettu 20 miljoonan euron sakko, tai 4 % vuotuisesta liikevaihdosta, kumpi vain sattuu kyseisellä yrityksellä olemaan isompi. Lievemmästä rikkomuksesta vastaavat luvut ovat 10 miljoonaa ja 2 %, mutta silti huomattava summa. (GDPREU 2018.)

2.2 Tietoisuuden lisääminen

Tietoisuuden lisäämisellä pyritään vaikuttamaan asenteisiin ja tapoihin, joilla tietoturvallisuuskulttuuria saadaan ylläpidettyä ja kehitettyä yrityksen sisällä. Tietoisuuden pohjalla on

tarkoitus saada työntekijät ja yritysjohto tunnistamaan tietoturvallisuusriskejä ja reagoimaan niihin sovitulla tavalla. Infosecin mukaan (Security awareness, 2018) tietoturvallisuustietoisuuden levittäminen on tärkein ja tehokkain keino riskien hallintaan turvallisuuden osa-alueella. Esimerkiksi tietojenkalasteluhyökkäykset (phishing) ovat nousussa, ja ne suurimmaksi osaksi niiden onnistuminen on ainoastaan uhrin hyväuskoisuuden varassa. Tietoisuutta levittämällä ja opettamalla työntekijöitä tunnistamaan ja näitä hyökkäyksiä sekä oikealla tavalla raportoimaan niistä pystyttäisiin niistä välttämään. (SFS-EN ISO/IEC 27002:2017, 18-20.)

Ihmiset ovat tietoturvallisuudesta puhuttaessa heikoin lenkki. Parhaatkaan fyysisen turvallisuuden keinot ja virustorjuntateknologia eivät auta, mikäli työntekijä niin sanotusti vapaaehtoisesti luovuttaa tärkeitä tietoja ulkopuolisille toimijoille. Tietoturvallisuustietoisuuden levittämistä ei voi jättää työntekijän harteille tai itse opeteltavaksi, vaan muutoksen ja kehityksen on lähdettävä yritysjohdosta ja yrityksen strategiasta asti. (SFS-EN ISO/IEC 27002:2017, 18–19.) Kouluttamisen lisäksi tulisi työntekijöitä esimerkiksi palkita onnistuneista poikkeamien raportoinnista, tietojenkalastus- ja muiden hakkerointiyritysten huomaamisesta ja estämisestä. Kuviossa 2 on kuvattuna vuonna 2018 tehdyn tutkimuksen mukaan ihmisten virheistä johtuvat tietomurrot.



Kuvio 2: Luonnollisten henkilöiden tekemistä virheistä johtuvat tietoturvamurrot. (IBM 2018)

Keinoja tietoturvallisuuden lisäämiseksi on monia. Tehokkaimpiin keinoihin lukeutuu työntekijöiden osallistaminen tietoturvallisuusdokumentointia kehittäessä, erilaiset esitykset ja seminaarit, sisäisessä verkossa tiedottaminen, verkkokoulutukset, sekä jatkuva henkilöiden välinen kommunikointi. (How to perform training & awareness for ISO 27001 and ISO 22301, 2014.)

Kouluttamisen säännöllinen järjestäminen on tärkeää. Säännöllisyyden täytyy kuitenkin olla järjestetty niin, että työntekijät eivät koe sitä taakkana, joka taas vaikuttaisi sen tehokkuuten. Tärkeämpää on saada henkilöt ymmärtämään sen tärkeys yrityksen toiminnan kautta.

Toimintaohjeiden levittäminen mahdollisimman monelle on yrityksille tärkeää, ja usein tietoturvakoulutus suositellaankin liittämään jo työntekijän perehdytysprosessiin. (Laaksonen ym. 2006, 255–256.)

Toimeksiantajalla tehokkaimmaksi keinoksi tietoturvallisuustyön aloittamiseen koettiin verkkokoulutuksen järjestäminen sen monimuotoisen toimialan ja suuren henkilöstömäärän takia. Tämän lisäksi yrityksessä on verkkokoulutuksen jälkeen lanseerattu kuukausittainen tietoturvallisuustiedote, jossa käydään läpi uusimpia uhkia ja keinoja niitä vastaan puolustautumiseen, samalla muistuttaen seikoista liittyen raportointiin ja muihin verkkokoulutuksessa käytyihin ohjeisiin.

3 Tietoturvallisuudesta

Perinteisesti tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden turvaamista. Luottamuksellisuudella tarkoitetaan sitä, että käsiteltävät tiedot ovat ainoastaan saatavilla sille tarkoitetuille henkilöille. Käytettävyydellä tarkoitetaan tiedon saatavuuden hallintaa. Eheys tarkoittaa, että tiedon laadusta ja sisällöstä on takeita, ja niitä ei ole merkitsemättä muokattu (Hakala, Vainio & Vuorinen 2006, 5-6.)

Myöhemmin, alan kehittyessä, on kuitenkin perinteiseen määritelmään koettu tarpeelliseksi tuoda uusia osatekijöitä johtuen edellisen määritelmän riittämättömyydestä nykytilanteessa. Kiistämättömyydellä (non-repudiation) tarkoitetaan järjestelmän kykyä tunnistaa ja todistaa järjestelmää käyttävän henkilön tiedot. Kiistämättömyys taataan kahdella keinoilla: tunnistamalla henkilö jonkin tunnisteen avulla (sähköinen, biometrinen) ja todistamalla hänen luotettavuutensa järjestelmässä (Conrad, Feldman & Misenar 2019.) Toinen lisäys, pääsynhallinta (access control) tarkoittaa henkilöiden tunnistamista ja heidän luvallista pääsyään järjestelmässä säilytettäviin tietoihin. Pääsynhallinnan keinoin pystytään esimerkiksi rajaamaan henkilöiden oikeuksia tiedonhallintajärjestelmän sisällä, ja näin pitämään kriittiset tiedot poissa asiaankuulumattomien henkilöiden käsistä. (Martin, J. 2018.)

Terminä tietoturvallisuus herättää usein asiaan perehtymättömien mielessä erilaisten teknisten ratkaisujen hallintaa, kun tosiasiassa se on paljon muutakin (Venable 2017). Tästä syystä myös suuri osa organisaatioista kokee ainoastaan teknisten ratkaisujen olevan riittäviä puuttumatta lainkaan riskeihin liittyen esimerkiksi puhuttuun tai paperilla olevaan tietoon, tai tiedon fyysiseen säilyttämiseen missä tahansa muodossa. Tietoturvallisuus on pitkälti kokonaisuuden hallintaa, ja jonkun osa-alueen hoitamatta jättäminen vaarantaa koko järjestelmän.

Tietoturvallisuus on pohjimmiltaan tietynlaisen muurin rakentamista hallittavan tiedon ympärille. (Laaksonen, Nevasalo & Tomula 2006, 17.) Teknisten ratkaisujen lisäksi tietoturvallisuuden keinot pätevät myös fyysiseen, esimerkiksi printattuun ja suulliseen tietoon. Syitä tietoturvallisuuden hallintaan yrityksessä on monia. Usein syyt ovat kuitenkin joko taloudellisia,

henkilökohtaisia tai poliittisia. Laaksonen ym. (2006, 118) mainitsevat esimerkkeinä tilanteita, joissa työntekijä kokee tulleensa kaltoin kohdelluksi ja haluaa aiheuttaa yritykselle vahinkoa. Toinen syy voi olla esimerkiksi vuotaneiden henkilötietojen myynti eteenpäin muun muassa roskapostia lähettävien organisaatioiden listoille. Yrityksellä on joka tapauksessa lukemattomia syitä tietoturvallisuuden hallintaan ja ylläpitämiseen liittyen, ja yritysten onkin nykypäivänä mahdotonta pyörittää menestyvää liiketoimintaa ilman tietoturvallisuutta. (Laaksonen ym. 2006, 118.)

3.1 Fyysinen ja tekninen toimintaympäristö

Toimitilojen fyysisen ympäristön hallinta on kaiken tietoturvallisuustoiminnan pohja. Ilman luotettavaa ja turvallista ilmapiiriä tiedon hallinnalle, ei voida tiedon luotettavuudesta ja oikeellisuudesta olla ikinä varmoja. Ongelmana ei ole pelkästään tietovuotojen ja tiedon vääristymisen vaara, vaan tietoa täytyy pystyä suojaamaan myös tulipaloilta, kosteusvahingoilta, sähköhäiriöiltä sekä pölyltä. Usein yrityksille on myös tärkeää luokitella tiloja eri turvallisuusluokitusten mukaan riippuen siitä, kuinka kriittinen mikin tila on. Korkean riskiluokan tiloja ovat usein esimerkiksi hallinnolliset tilat, erilaiset tietotekniset tilat sekä tuotantotilat. Fyysisen turvallisuuden hoitamiseksi voidaan organisaatioissa käyttää apuna esimerkiksi SFS-EN ISO/IEC 27001:2017 -standardia tai VAHTI -ohjetta. (Tietoturvallisuudella tuloksia 2007; SFS-EN ISO/IEC 27001:2017.)

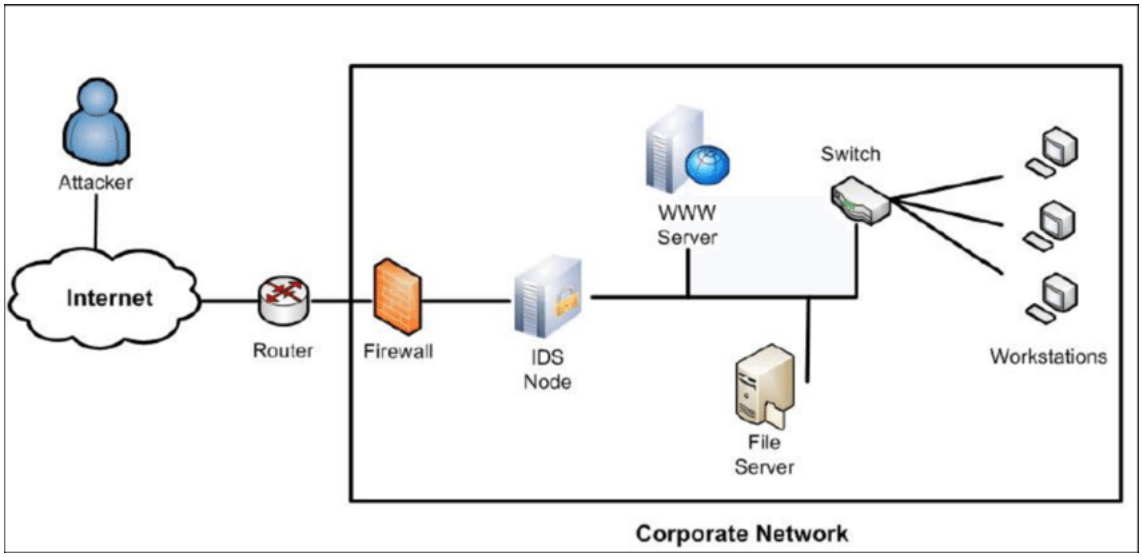
Fyysisen ympäristön lisäksi täytyy teknisestä toimintaympäristöstä kehittää mahdollisimman turvallinen. Perinteisiä keinoja, kuten palomuurien ja virussuojien asentamista ja ylläpitämistä pidetään nykyään itsellään riittämättöminä, mutta ne ovat silti ehdottoman tärkeitä. Kaiken teknisen ympäristön hallinnassa on tärkeää huomata, että esimerkiksi tietosuojalaki (1050/2018) sekä laki sähköisen viestinnän palveluista (917/2014) asettavat määrityksiä esimerkiksi verkon valvontaan ja käyttäjätunnusten hallintaan liittyen.

Identiteetinhallinnan avulla pyritään rajoittamaan henkilöiden pääsyä tietoon ja järjestelmiin, joihin heillä ei ole oikeutta. Identiteetinhallinta on teknisten ja hallinnollisten tietoturvakeinojen yhdistelmä. Pohjimmiltaan identiteetinhallinta on käyttöoikeuksien hallintaa. Pääasiassa sitä ylläpidetään tarkastamalla ja testaamalla pääkäyttäjien salasanojen vahvuutta, luomalla, päivittämällä ja poistamalla käyttöoikeuksia henkilöitä käyttäjätunnusten elinkaaren aikana. (Laaksonen ym. 2006, 173–180.)

Tietoverkon teknisellä suojaamisella tarkoitetaan toimenpiteitä sekä ratkaisuja, joilla pyritään estämään haittaohjelmien sekä tunkeutujien pääsy yrityksen verkkoon tai laitteille. Keinoja tietoverkon suojaamiseen voi olla esimerkiksi yrityksen sisäisen verkon rakenteen suunnittelu sekä palomuurien asennus ja ylläpito. Palomuurien suunnittelun täytyy olla sellaisella tasolla, että se ei aiheuta ongelmia esimerkiksi yrityksen sisäisen verkon ulkopuolisten organisaatioiden kanssa toimimiseen, ja todella toimii ainoastaan turvallisuusmääreenä. (Laaksonen

ym. 2006, 181–188.) Tietoverkon teknistä suojaamista suunnitellessa on tärkeää ottaa huomioon myös ulkoisten verkkojen ja etätyön tuomat ongelmat.

Muita keinoja tietoverkon suojaamiseen on esimerkiksi erilaiset tunkeutumisen havaitsemisen (IDS) sekä torjunnan (IPS) järjestelmät. Näiden järjestelmien perusperiaatteena on tunnistaa yrityksen verkon ja tietoliikenteen normaalitilanne, ja puuttua ja ilmoittaa siinä tapahtumiin poikkeamiin esimerkiksi määrittämällä erilaisia hyökkäysmalleja. Nämä järjestelmät ovat usein tehokkainta sijoittaa kriittisten palvelimien eteen alla olevan kuvion 3 mukaisesti, jotta mahdollisimman suuri osa haitallisesta tietoliikenteestä suodattuisi muiden suojauskeinojen, esimerkiksi palomuurin kautta. Täten vähennetään IDS- ja IPS -järjestelmiin kohdistuvaa taakkaa, ja vähennetään turhia hälytyksiä. (Laaksonen ym. 2006, 188–191.)



Kuvio 3: IDS -järjestelmän sijainti yrityksen tietoverkossa (Researchgate).

Kaikkien yllä mainittujen seikkojen lisäksi ovat virustorjuntaohjelmat kuitenkin yleisin ja tiedetyin keino. Virustorjunnassa on hyvä ottaa huomioon, että ainoastaan työasemien virustorjunta ei itsessään ole riittävä keino, vaan sen lisäksi tulisi suojata myös selainliikenne ja palvelimet, sekä erilaiset tuotannon järjestelmät. Virustorjuntaohjelmat ovat paras keino esimerkiksi sähköpostin välityksellä liikkuvien virusten suojaamiseksi heti käyttäjän varovaisuuden jälkeen. (Laaksonen ym. 2006, 202-205.)

Nykyään suurimman uhkan aiheuttavat IoT (Internet of Things) -laitteet, eli verkkoon yhdistetyt arkipäivän laitteet kuten jääkaapit. Laitevalmistajat harvemmin puuttuvat turvallisuusuhkiin, sillä usein ne vaikuttaisivat käytettävyyteen. IoT -laitteisiin on suhteellisen helppo murtautua, ja useat tieto- ja kyberturvallisuusyritykset ovatkin jo keksineet ratkaisuja ongelman ratkaisemiseksi. (Zacks, 2018.)

Tietojärjestelmien turvaamiseksi täytyy ne suunnitella pääosin niin, että muiden teknisten keinojen kuten palomuurien kaatumisella ei ole niihin vaikutusta. Tietojärjestelmien turvallisuuteen voidaan vaikuttaa esimerkiksi standardien mukaisilla asetuksilla, joissa puututaan esimerkiksi salasanojen laadun vaatimuksiin sekä käyttäjien oikeuksiin ja jäljitettävyyteen. Järjestelmiä tulisi myös auditoida säännöllisesti, ja pitää huolta esimerkiksi tietoturvapäivitysten asentamisesta tai salasana-asetusten päivittämisestä. Auditointiin suositellaan ulkoisten toimijoiden palveluita, sillä ne ovat usein huomattavasti kustannustehokkaampia. (Laaksonen ym. 2006, 214–217.)

3.2 Lainsäädäntö

Yrityksiin kohdistuu useita lainsäädännöllisiä vaatimuksia ja velvoitteita tietoturvallisuuden osalta. Niin kotimainen kuin kansainvälinenkin lainsäädäntö asettaa yrityksille ja organisaatioille velvoitteita tietoturvallisuuden hallintaan. Velvoitteet ja määräykset ovat usein yleisluontoisia, ja niiden vaatimusten tavoittaminen sekä riittävän tason saavuttaminen on jätetty organisaation itsensä huolehdittavaksi. (Laaksonen ym. 2006, 18.)

Suoranaista tietoturvallisuuslakia ei Suomessa ole käytössä. Valtionhallituksen asetus tietoturvallisuudesta valtionhallinnossa (681/1.7.2010) asettaa raamit tietoturvallisuuden hallinnasta valtionvirastoissa, mutta yrityksille vastaavanlaista ei ole, vaikka siitä puhetta onkin ollut vuosien varrella. Useissa muissa laeissa ja säädöksissä kuitenkin sivuutetaan tietoturvallisuutta.

Vuoden 2018 toukokuussa voimaan tullut General Data Protection Regulation (GDPR) on EU:n tietosuoja-asetus, joka määrittelee pitkälti yritysten ja organisaatioiden tavat hallita henkilötietoja. Tietoturvallisuuden osalta GDPR asettaa myös vaatimuksensa, vaikka jättää käytännön toteutuksen yrityksen vastuulle. Yritykset joutuvat GDPR:n velvoittamana esimerkiksi salaamaan käsiteltävät henkilötiedot, sekä tietoturvallisuudenkin kolmen perusperiaatteen mukaisesti takaamaan teknisin keinoin henkilötietojen saatavuuden, eheyden ja käytettävyyden. (GDPR, Jakso 2, artikla 32) Tämän lisäksi yritykset ovat ylläpitämään rekisteriä tietovuodoista, ja raportoimaan niistä viranomaisille mikäli tietoturvaloukkauksesta aiheutuu vahinkoa henkilölle, jonka henkilötietoja käsitellään. (GDPR, Jakso 2, artikla 34.) GDPR:n julkaisun pohjalta astui Suomessa voimaan 2018 myös uusi Tietosuojalaki (1050/2018), jossa täsmennetään ja täydennetään sen sisältöä, sekä sovelletaan sitä myös kansallisesti. (Tietosuojalaki, 1§. 2018.)

3.3 Standardit

Laaksosen ym. (2006, 19) mukaan yritykset haluaisivat enemmän ohjeistusta viranomaistahoilta liittyen tietoturvallisuuden johtamiseen lainmukaisuuden takaamiseksi. Yritykset usein siis toimivat niin sanottujen parhaiden toimintatapojen mukaan lain asettamien määräysten

sijaan. Tässä isoa roolia pelaavat kansainvälisesti hyväksytyt ja arvostetut standardit ja ohjeistukset, joiden pohjalta useat yritykset rakentavatkin tietoturvallisuuspolitiikkansa.

Standardisointi tarkoittaa yhteisten toimintatapojen laatimista. Ne on luotu helpottamaan viranomaisten, organisaatioiden sekä kuluttajien elämää. Standardisointi pyrkii yhdistämään toimintatapoja sekä turvallisuutta, suojelemaan kuluttajaa sekä helpottamaan kaupankäyntiä. (SFS-EN ISO/IEC 27001:2017.)

Standardien laatiminen tapahtuu työryhmien ja komiteoiden yhteisten intressien tuotoksena. Standardien kehitysprosessissa on usein mukana edustajia ja organisaatioita eri aloilta, esimerkiksi teollisuudesta, tutkimusorganisaatioista, valtion elimistä sekä kuluttajista. (Standards 2019a) Tietoturvallisuuden osalta tämä tarkoittaa hyvien toimintatapojen ja tietoturvallisuuden hallinnan ohjeistusta koottuna useampiin tietopaketteihin.

ISO -standardit tarkoittavat International Organization for Standardization -organisaation luomia standardeja. ISO -standardit ovat kansainvälisesti arvostettuja, ja ovatkin usein pohjana yritysten strategioihin ja toimintatapoihin paikallisen lainsäädännön lisäksi. Yritykset voivat toteuttaa sisäisiä auditointeja standardien mukaisuuden varmistamiseksi. Tieto- ja kyberturvallisuusalalla toimivat yritykset voivat hankkia auditointiluvan esimerkiksi ISO 27001 – tai muille standardeille, ja voivat yrityksen auditoituaan myöntää heille sertifikaatin, joka todistaa heidän tietoturvallisuuden hallintansa olevan standardin vaatimalla tasolla. (SFS-EN ISO/IEC 27000:2017, 26.) ISO-standardeja päivitetään niiden sisällöstä ja ajankohtaisuudesta riippuen sykleissä, aina vastaamaan ajan ja tilanteen vaatimia keinoja (All about ISO 2019b). Mitä useampi organisaatio tai yritys toteuttaa tietoturvallisuuspolitiikkaansa näiden standardien mukaan, sitä helpompi on kyseisten yritysten toimia myös yhteistyössä yhteisten toimintatapojen puitteissa, kun myös toisella organisaatiolla on todistetusti hyvin hoidettu tietoturvallisuuspolitiikka (Purser 2014). Alla on esitelty muutamia tärkeimpiä standardeja ja ohjeistuksia lyhyesti.

SFS-EN ISO/IEC 27000:2017 on tietoturvallisuusstandardien yläluokka, ja se sisältää suosituksia tietoturvallisuuden hallintaan ja riskeihin. Standardi sisältää esimerkiksi tietoturvallisuuden sanastoa, hallintajärjestelmiin kohdistuvia vaatimuksia, parhaita toimintatapoja tietoturvallisuuden hallintaan liittyvien vaatimusten toteuttamiseksi, ohjeita tietoturvallisuustason mittaamiseen, riskien hallintaa sekä auditointiin liittyviä ohjeita ja sertifiointielimiin kohdistuvia vaatimuksia. ISO 27000 pohjautuu BS7799:2 -standardiin. (SFS-EN ISO/IEC 27000:2017; Miller 2006.)

SFS-EN ISO/IEC 27001:2017 on yhtä lailla ISO 27000:n kanssa tietoturvallisuuden hallintaan liittyvä standardi. Se tarkentaa tietoturvallisuuden hallintajärjestelmän vaatimuksia, ja ohjeistaa sen luomiseen, kehittämiseen sekä jatkuvaan parantamiseen. Standardi asettaa vaatimukset myös tietoturvallisuusriskien hallintaan ja niiden hoitamiseen. Standardin asettamat

vaatimukset ovat niin sanotusti yleismaailmallisia, ja organisaatiot voivat toteuttaa sen vaatimat rajoitukset haluamallaan, yrityksen koosta ja strategian asettamista vaatimuksista riippuen parhaaksi näkemällään tavalla. (SFS-EN ISO/IEC 27001:2017)

SFS-EN ISO/IEC 27002:2017 sisältää ohjeistuksia ISO 27000- ja 27001-standardien vaatimuksien täyttämiseksi. Standardin sisältö koostuu ehdotuksista ja parhaista toimintatavoista, joiden avulla yritykset voivat käytännössä toteuttaa tietoturvallisuuspolitiikkaansa tehokkaasti ja standardien mukaisesti. Standardin sisältö koostuu kuitenkin lähinnä ehdotuksista, ja niiden tulkitseminen ja harkinta toteuttamisesta jääkin organisaation vastuulle. (SFS-EN ISO/IEC 27002:2017.)

Standardin sisältö on kuitenkin kokonaisvaltainen, ja sisältää usein hyvinkin tehokkaita toimintatapoja. Sisältöön kuuluu esimerkiksi ohjeita liittyen turvallisuusstrategian toteuttamiseen, tietoturvallisuuden organisointiin, henkilöstöhallinnon turvalliseen järjestämiseen sekä fyysiseen turvallisuuteen, mistä on tämän työn aiemmissa kappaleissa jo puhuttu. (ISO/IEC 27002:2005, 2013)

3.4 Auditointityökaluja

Katakri on puolustusministeriön julkaisema dokumentti, joka on tarkoitettu tietoturvallisuuden auditointityökaluksi viranomaiskäyttöön. Katakri pohjautuu EU:n ja kansallisiin säädöksiin ja velvoitteisiin, ja täyttää kaikki niihin liittyvät vähimmäisvaatimukset. Vaikka dokumentti on tehty viranomaiskäyttöön, toimii se helposti saatavilla olevana pohjana myös yrityksille heidän turvallisuusstrategiansa kehittämiseen, ja Katakrin johdanto-osuudessa mainitaankin mahdollisuus myös sen soveltamiseen tässä käytössä. Katakri on jaettu kolmeen osioon: turvallisuusjohtamiseen, fyysiseen turvallisuuteen sekä tekniseen tietoturvallisuuteen. Kullekin osiolle on omat vaatimuksensa, ja niiden auditointi onnistuu myös erikseen auditoinnin laajuudesta riippuen. (Katakri. 2015.) VAHTI on valtiovarainministeriön asettama julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, joka vastaa turvallisuuden kehittämisestä ja ohjauksesta yhteistoimin vastaavien organisaatioiden kanssa. VAHTI-toiminta on osa Suomen kyberturvallisuusstrategiaa ja heillä on keskeinen rooli edellä mainitun strategian toteuttamisessa. (VAHTI-toiminta.) International Security Forum julkaisee Standard of Good Practice -julkaisua, jossa kootaan standardien kuten ISO 27002:n mukaisia vaatimuksia ja ehdotetaan tehokkaita tapoja niiden saavuttamiseksi. Julkaisu on tehty juurikin yrityksiä ajatellen, ja asioita käsitellään yrityselämän näkökulmasta. (The ISF Standard of Good Practice for Information Security 2018, 2018.)

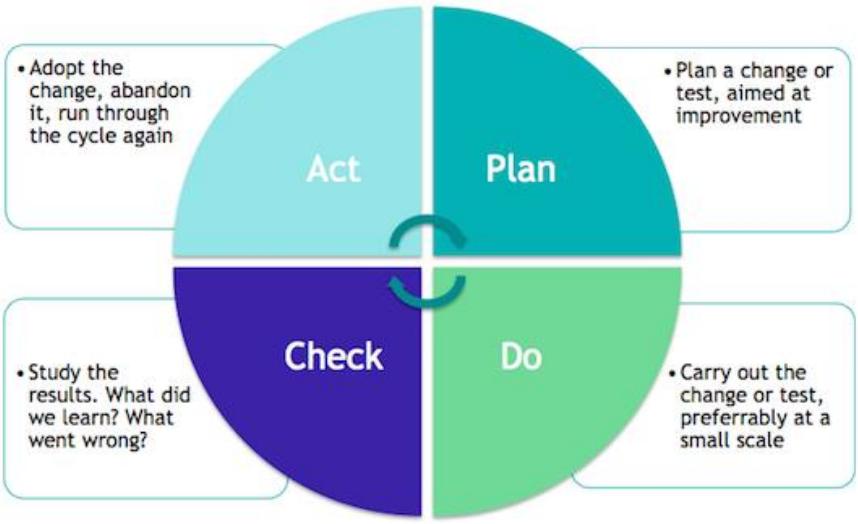
3.5 Hallinnollinen tietoturvallisuus ja tietoturvapolitiikka

Hallinnollinen osuus tietoturvallisuudesta tarkoittaa muun muassa yrityksen tietoturvallisuuspolitiikan hallintaa, linjauksia toiminnassa, johtamista, tietoturvaorganisaation määrittelyä

sekä tietoturva-asioiden sijoitusta yrityksessä. Hallinnollinen tietoturva määrittelee ja hallitsee kaikkia sen alapuolella tapahtuvia toimijia sekä muita muuttujia. Se luo tietynlaiset toimintaedellytykset tietoturvan ylläpidolle sekä kehittämiselle. (Miettinen, 2002, 131.)

Tietoturvallisuutta hallitaan usein yritysjohdon tai siihen perehtyneiden henkilöiden toimesta tehdyllä tietoturvallisuuspolitiikalla. Tietoturvallisuuspolitiikka määrittelee tietoturvallisuuden tavoitteet sekä vastuut ja toimintalinjat yrityksessä. Hyvin määritelty sekä dokumentoitu tietoturvallisuuspolitiikka luo pohjan hyvän turvallisuuskulttuurin kehittymiselle organisaatiossa. (VAHTI-ohje, 2007.) Turvallisuusorganisaation määrittelemiselle ei ole mitään tiettyä määritelmää, ja niin sanottua oikeata ratkaisua ei ole olemassa. Vaihtoehtoja ja mahdollisuuksia on kuitenkin useita, ja tietoturvallisuutta pitäisikin johtaa organisaation vahvuuksien mukaan. ISO 27001 -tietoturvastandardin mukaan tehtävään kannattaa kuitenkin sijoittaa ainakin joko Information Security manager, Chief Information Security officer, tai vastaavan tittelin omaava henkilö, jonka taidot riittävät tietoturvallisuuden johtamisjärjestelmän hallintaan (Who to involve).

Laaksonen, Nevasalo ja Tomula (2006, 118-119) luettelevat seikkoja, joihin yrityksen pitäisi puuttua turvallisuuspolitiikkaa luodessa. Selvitettäviä asioita on esimerkiksi: minkälaista tietoa organisaatiossa käsitellään, voiko joku hyötyä taloudellisesti tai muin keinoin yrityksen hallitsemasta tiedosta, ja kuinka joustavasti kadonnutta tai vaarantunutta tietoa voidaan tuottaa uudestaan. Asiayhteydessä täytyy myös miettiä, onko kadonneen tiedon etsimisestä tai uudestaan luomisesta enää hyötyä, mikäli puhutaan esimerkiksi liikesalaisuuksista. Ideaalitilanteessa tietoturvallisuuspolitiikkaa päivitetään ja pidetään ajan tasalla jatkuvasti alan jatkuvasti muuttuvan luonteen takia. Tähän tarkoitukseen voidaan käyttää esimerkiksi myös ISO 27001:n mukaista PDCA (Plan-Do-Check-Act) -mallia, (Kuvio 4) joka pyrkii takaamaan jatkuvan kehityksen syklin tietoturvallisuutta hoitaessa.



Kuvio 4: PDCA -malli tietoturvallisuuden kehittämisen avuksi (ICTinstitute 2017.)

Tietoturvallisuuspolitiikkaa toimeksiantajalla toteutetaan verkkokoulutuksen lisäksi myös aiemmin kerrotun tietoturvallisuusmanuaalin avulla. Verkkokoulutus pohjautuu tärkeimmiksi koettuihin kohtiin manuaalin sisällössä, joten sen avaaminen tässä asiayhteydessä on ehdottomasti olennaista. Manuaalin sisällysluettelo on seuraavanlainen: 1) Esittely, 2) Tietoisuus, 3) Tiedon suojaaminen ja luokittelu, 4) Turvalliset työskentelytavat, 5) Ohjeita sähköisessä ympäristössä toimimiseen, 6) Häiriöiden tunnistaminen ja raportointi, 7) Tietosuojalausunto.

Esittely – osiossa on kuvattu kyseisen dokumentin tarkoitukset ja tarpeet yrityksen näkökulmasta. Osiossa on kuvattu myös manuaalin kohderyhmät sekä tavoitteet, sekä yhteydet yrityksen turvallisuusstrategiaan erityisesti tietoturvallisuuden ja IT:n osalta. Tietoisuus – osio käsittelee tietoturvallisuuden osuutta yrityksen turvallisuusjohtamisjärjestelmään sekä yleisiin turvallisuusohjeisiin ja – periaatteisiin. Myös työntekijöiden roolit ja vastuut tietoturvallisuuskulttuurin ylläpitämisessä on kuvattu tässä kappaleessa. Tiedon suojaaminen ja luokittelu – alaotsikoineen käsittelee erilaisen tiedon käsittely-, säilytys- ja levitysmuotoja kaikissa muodoissa. Kappaleessa kuvataan tiedon lajittelutavat sekä periaatteet sille, miten minkäkin tietoluokituksen omaavaa tietoa käsitellään kaikissa muodoissa. Turvalliset työskentelytavat – kappaleessa opastetaan työntekijää turvallisten työtapojen ylläpitämiseksi, työskentelivät he fyysisesti missä ja miten tahansa. Ohjeita sähköisessä ympäristössä toimimiseen selvittää yleisimpiä uhkia ja ongelmia joihin verkossa sekä jokapäiväisessä työssä voi kohdata. Osiossa käsitellään esimerkiksi sähköpostin sekä internetin turvallista käyttöä, laitteisiin liittyviä ohjeita sekä omien laitteiden käyttöä työnteossa. Häiriöiden tunnistaminen ja raportointi määrittelee tietoturvallisuuspoikkeamista raportoimisen keinot ja opastaa lukijaa, mistä kaikesta ja mihin heidän tulisi ilmoittaa törmätessään sellaiseen. Tietosuojalausunto on asetettu manuaalin

loppuun ikään kuin velvoittamaan lukijan noudattamaan hänen lukemaansa materiaalia ja toimimaan niiden puitteissa töitään tehdessä. (Information security manual, 2018.)

3.6 Tiedon luokittelu

Tiedon luokittelu on prosessi, jossa jaetaan yrityksen sisällä oleva tieto eri turvallisuusluokittelun mukaan. Tiedon luokittelulle ei ole säädetty lakeja eikä se ole yritykselle millään tavoin pakollista, mutta esimerkiksi kansainvälinen tietoturvastandardi ISO 27001 määrittelee keinoja tiedon luokittelun helpottamiseksi. Tietojen luokittelulla pyritään jakamaan tieto luottamuksellisuuden mukaan niin, että pystyttäisiin mahdollisimman tehokkaasti rajaamaan ihmisten pääsyä tietylle tasolle luokiteltuun tietoon. Yleensä tieto luokitellaan sen mukaan, kuinka paljon vahinkoa se voi tuottaa yritykselle joko talouden tai maineen menetyksen saralla (SFS-EN ISO/IEC 27002:2017, 22.) Toimeksiantajalla tieto on jaettu neljään osa-alueeseen:

Secret: Salaiseksi luokiteltuun tietoon on mahdollisimman rajoitettu pääsy; Esimerkiksi kriittiset henkilötiedot, salasanat, salausavaimet, julkaisemattomat taloustiedot- ja raportit. Tämän salaustason tiedot pyritään pitämään mahdollisimman pienen piirin tiedossa, ja tieto tulee jakaa ainoastaan henkilöille, jotka sitä ehdottomasti tarvitsevat joko tiedoksi tai työnsä suorittamiseen.

Confidential: Luottamukselliseksi luokiteltuun tietoon kuuluu esimerkiksi vuosiraportit, muut henkilötiedot, markkinointisuunnitelmat, asiakastiedot sekä turvallisuusohjeet ja – suunnitelmat. Verrattuna salaiseen tietoon luottamuksellisen tiedon vuotamisen ei koeta olevan niin kriittistä yritykselle tietovuodon sattuessa.

Internal: Sisäinen tieto on tarkoitettu yrityksen sisäiseen käyttöön sekä tiettyjen raamien sisällä sidosryhmien ja yhteistyökumppaneiden käyttöön. Sisäiseen tietoon kuuluu esimerkiksi sisäiset tiedotteet, koulutukset, käyttöohjeet sekä organisaatiokaaviot. Sisäisen tiedon vuotaminen saattaa johtaa yrityksen prosessien haavoittumiseen.

Public: Julkiseen tietoon kuuluu kaikki yrityksen julkisilla verkkosivuilla ja mainonnassa jaettava tieto. Julkisen tiedon vuotaminen ei ole millään tasolla yrityksen toiminnalle vaarallista, eikä sen käsittely vaadi erityisiä suojaustoimenpiteitä. (Information Security Manual 2018.)

4 Opinnäytetyössä käytetyt menetelmät

Tämä opinnäytetyö on toiminnallinen opinnäytetyö. Sen tarkoituksena on kehityksen mittaaminen verkkokoulutuksen vaikutuksesta. Vilkan ja Airaksisen mukaan (2015, 9) toiminnallisen opinnäytetyön tavoitteena on käytännön toiminnan muotoileminen. Tutkimuksen merkitys toiminnallisessa opinnäytetyössä on suuri, sillä selvitystyö on kaiken mittaamisen pohja. Toiminnallisen opinnäytetyön lopputuotoksen toiminnallisuus on konkreettinen, esimerkiksi ohjeistus. (Vilkka & Airaksinen 2003, 9.)

Kvalitatiivisen ja kvantitatiivisen tutkimuksen erottaminen toisistaan on haastavaa. Suoraa vastakkainasettelua on vaikea tehdä, ja useammin ne nähdäänkin ennemmin toisiaan täydentävinä. (Hirsjärvi ym. 1997, 126–128.) Tässä opinnäytetyössä on käytetty osittain kvantitatiivisia menetelmiä kvalitatiivisen tutkimuksen tekemiseen. Lähtökohtana kvalitatiivisessa tutkimuksessa on todellisen elämän kuvaaminen. Kvalitatiivisen tutkimuksen tarkoituksena on tutkia kohdetta mahdollisimman kokonaisvaltaisesti. Osa kvalitatiivista tutkimusta on myös tosiasioiden paljastaminen ja löytäminen. (Hirsjärvi ym. 1997, 152–154).

Opinnäytetyössä käytettiin tiedonhankintamenetelmänä kyselytutkimusta. Kyselytutkimus on tärkeä tapa kerätä tietoa esimerkiksi mielipiteistä, asenteista ja arvoista. (Vehkalahti 2014, 11.) Kyselytutkimuksessa käytettiin suurimmaksi osaksi suljettuja osioita tulosten käsittelyn helpottamiseksi. Avoimista vastausvaihtoehdoista ilmenisi mahdollisesti moninaisempia vastauksia, mutta vastaukset tuskin toisivat lisäarvoa tutkimuksen lopputuloksen kannalta. (Vehkalahti 2014, 26.) Kysymykset olivat pitkälti monivalintakysymyksiä, sillä tarkkojen yksilöiden mielipiteiden sijaan tutkimuksessa haettiin helposti vertailtavaa dataa (Hirsjärvi ym. 1997, 190).

Aiheeseen liittyvän kirjallisuuden tunteminen on kaiken tutkimustyön perusta. Tutkimuksen alussa tulee ottaa selville miten aihetta on tutkittu aikaisemmin, miten aihe pitäisi rajata ja miten se sovitettaisiin sopimaan tutkimukseen. Tutkimuksen aikana tulee tekijän seurata tuottamaansa sisältöä, ja pitämään kiinni sen faktapohjaisuudesta. Tutkimuksen jälkeen tulee tuloksia verrata tutkimuksen sisältöön. (Hirsjärvi ym. 1997, 98–99.)

Tutkimuksesta saatujen tulosten analysointiin käytettiin niiden tarkastelua tutkimustehtävän perustaan eli tutkimuskysymyksiin, sekä tulosten vertailua taulukoina kappaleessa 6. Taulukot ovat tehokas tiivistämis- ja havainnollistamiskeino. (Hirsjärvi ym. 1997, 244.) Kyselyiden tulokset sijoitettiin taulukkoon, josta tuloksia oli helppo jaotella esimerkiksi sen mukaan, miten vastaajat olivat mihinkin kysymyksiin vastanneet. Näin saatiin selville esimerkiksi se, kuinka moni vastaajista oli tehnyt ensimmäisen kyselyn.

5 Opinnäytetyön prosessi

Opinnäytetyön prosessi käynnistyi maaliskuussa 2018, kun opinnäytetyön tekemisestä sovittiin. Verkkokoulutus oli aluksi määrä julkaista kevään/kesän aikana, mutta se siirtyi lopulta kuitenkin syksylle 2018. Kysely tehtiin yhteistyössä toimeksiantajan edustajan kanssa, jotta se sisältäisi mahdollisimman paljon heidän tärkeäksi näkemiään asioita.

Teoreettinen viitekehys koottiin painettujen, osittain julkaisemattomien sekä sähköisten lähteiden avulla. Aluksi työssä käydään läpi tietoturvallisuuteen liittyvää teoriaa, tulevaisuudennäkymiä sekä tähän työhön liittyviä muita keskeisiä tekijöitä, joilla pyrittiin tuomaan ilmi tä-

män tutkimuksen tekemisen syitä. Seuraavaksi käsiteltiin tiedon luokittelun perusteita ja periaatteita, tietoturvallisuuden hintaa yrityksille, tietoturvallisuuden johtamista sekä riskienhallintaa. Lopuksi teoriaosuudessa käytiin vielä läpi tietoisuuden lisäämisen hyötyä sekä siitä aiemmin tehtyjä tutkimuksia. Opinnäytetyö painottui sekä prosessin alku- että loppupäähän, mutta sen keskiössä oli kuitenkin eniten tapahtuneen muutoksen mittaaminen.

Tutkimuksen kohteena oli toimeksiantajan yhden toimipisteen toimistohenkilöstö, ja kyselyt lähetettiin toimeksiantajan arvioiden mukaan noin sadalle ihmiselle. Tutkimuskohteeksi valikoitui juuri tämä toimipiste, sillä suurimman osan kyselyyn vastaajista tiedettiin käsittelevän työssään korkean tietoturvallisuusluokituksen omaavia tietoja, esimerkiksi työntekijöiden henkilö- ja pankkitietoja. Tutkimus päätettiin kohdistaa tälle kohderyhmälle, sillä heidän tietoturvallisuusosaamisen tason selvittäminen koettiin olevan yritykselle tärkeintä kouluttamisen alkuvaiheessa. Molemmat kyselyt suoritettiin Google Forms -alustalla sen helppokäyttöisyyden sekä saavuttavuuden takia. Myös datan käsittely on helppoa Googlen työkaluilla. Vastaajien määrää pyrittiin kasvattamaan myös muistutusviestillä puolessa välissä vastausaikaa.

Muutamassa kohdassa käytettiin tarkentavana tekijänä myös vapaamuotoista tekstipohjaa, johon pystyi halutessaan tarkemmin perustelemaan vastaustaan. Kysymyspohja oli rakenteeltaan yksinkertainen, ja tämä helpotti tulosten tuomista taulukkomuotoon ja teki vastauksista helposti vertailtavia. Olettama kyselypohjaa tehdessä oli, että käsiteltävät asiat ovat vastaajille kohtalaisen uusia johtuen aiemman koulutusmateriaalin puutteesta suurimmalla osalla osa-alueista.

Ensimmäinen kysely toteutettiin aikavälillä 3.8.–15.8.2018, ja pohja lähetettiin noin sadalle ihmiselle, jotka työskentelevät pääasiassa henkilöstö- ja taloushallinnon puolella. Kokonaisuudessaan kysely keräsi annettuna aikana 72 vastausta. Kyselyn tarkoituksena oli selvittää tietoturvallisuusosaamisen lähtötaso ennen verkkokoulutuksen julkaisemista. Verkkokoulutusmateriaali oli tässä vaiheessa kuitenkin jo valmis, joten kysymyspohja perustettiin pitkälti sen mukaiseksi toisen kyselyn tekemisen helpottamiseksi. Kysymysvaihtoehdot pyrittiin tekemään mahdollisimman selkeiksi ja yksinkertaiseksi vastata. Vastaamiskynnystä pyrittiin myös madaltamaan pitämällä kysely kohtalaisen lyhyenä, kuitenkaan sisällön laajuuteen merkittävästi vaikuttamatta. Ensimmäisen kyselyn saateteksti sekä kysymykset ovat nähtävillä liitteissä 1 ja 2.

Toisen kyselyn vastausajankohtana oli 30.10.–16.11. Kysely lähetettiin samalle vastaajajoukolle, kun ensimmäinenkin, mutta johtuen muutoksista työpaikalla kyselyn järjestämisen ajankohtana keräsi toinen kysely vain 54 vastausta, vaikka kyselyyn vastaamisesta lähetettiin tälläkin kerralla muistutusviesti. Näistä 54 vastauksesta 44 oli tehnyt tietoturvallisuuskoulutuksen, mutta vain 35 oli vastannut myös ensimmäiseen kyselyyn. Vertailupariksi ensimmäi-

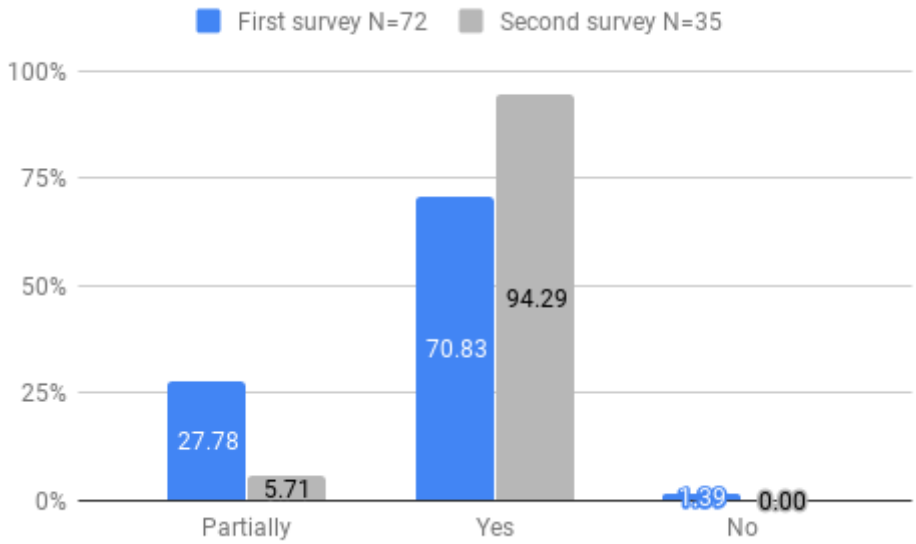
selle kyselylle valittiin siis nämä 35 henkilöä, jotka olivat sekä käyneet tietoturvallisuuskoulutuksen sekä tehneet ensimmäisen kyselyn. Vaikka vastaajien määrässä onkin suuri ero ensimmäisen ja toisen kyselyn välillä, ovat vastaajien taustamuuttujat pysyneet samana. Muutama kysymys muuttui toiseen kyselyyn. Muutokset johtuivat siitä syystä, että tämä tieto oli oikeastaan olennaista vain ensimmäisen kyselyn aikaan, ennen koulutuksen järjestämistä. Nämä kysymykset on merkitty ja mainittu seuraavassa kappaleessa olevassa tulosten analysoinnissa. Toisen kyselyn saateteksti ja kysymykset ovat nähtävillä liitteissä 3 ja 4.

Kahden eri tilanteen väliseen eroon koettiin kvalitatiivisen tutkimuksen olevan ainoa oikea vaihtoehto. Vertailukelpoisia vastauksia kyselyihin tuli 72 ja 35. Vastausmääristä odotettiin hieman suurempia, mikä saattaa vaikuttaa tutkimuksen reliabiliteettiin negatiivisesti. Tutkimuksen oli kuitenkin tarkoitus olla suuntaa antava, ja selkeää kehitystä oli joka tapauksessa nähtävissä.

6 Kyselyn tulokset

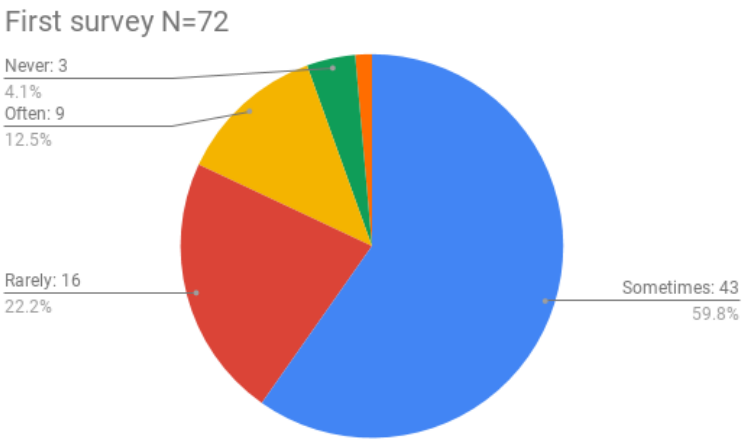
Kyselyn tuloksista on kuvattuna kuvioissa tärkeimmät löydökset sekä suurimmat muutokset. Vähäisemmän merkityksen kohdat sekä lähes muuttumattomana pysyneet seikat on kuvattu lyhyemmin tämän kappaleen lopussa.

Taustamuuttujia kysymällä pyrittiin lähinnä selvittämään, onko vastaajissa kyselyiden välillä eroja. Vastaajista suurin osa, 71 % ja 69 % oli naisia, ja loput 29 % ja 26 % miehiä. Toisessa kyselyssä noin 6 % ei halunnut tuoda ilmi sukupuoltaan. Myös ikäjakauma pysyi hyvin pitkälti samana, pieniä luonnollisia eroja lukuun ottamatta johtuen eri vastaajamääristä kyselyiden välillä. Vastaajista yli puolet kummassakin kyselyssä on yli 45-vuotiaita, noin 20 % oli 35–45 -vuotiaita, sekä noin 15 % oli 25–35 -vuotiaita. Kumpaankin kyselyyn vastasi myös alle 25 -vuotiaita, sekä muutamat eivät halunneet tuoda ikäänsä ilmi. Vastaajien keskuudessa myös yrityksessä työskentelyaika oli hyvin pitkälti pysynyt samana. Noin puolet kumpaankin kyselyyn vastanneista on työskennellyt yrityksessä yli 10 vuotta. Noin 35 % on työskennellyt 1-5 vuotta. Lyhemmän aikaa työskennelleitä oli myös molempiin kyselyihin vastanneiden joukossa. Kuviossa 5 on esiteltynä ensimmäinen tietoturvakoulutuksen sisältöön liittyvän kysymyksen tulokset.



Kuvio 5: Tiedätkö kyber- ja tietoturvallisuuden väliset erot?

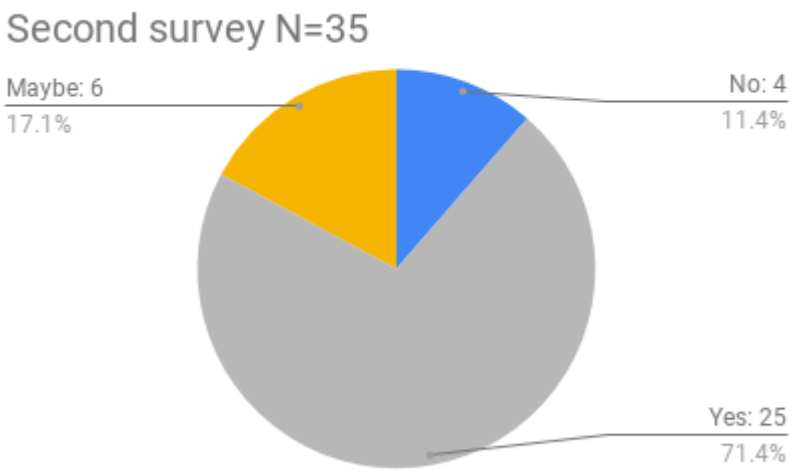
Tieto- ja kyberturvallisuuden ymmärtämisen taso kehittyi verkkokoulutuksen jälkeen parempaan suuntaan. Ensimmäisessä kyselyssä kyllä-vastausvaihtoehdon prosentti oli noin 71 %, kun toisessa kyselyssä taas se oli noussut jopa 94 %:iin. Prosentuaalinen muutos kyllä -vastauksessa oli noin +33 %. Ensimmäisen kyselyn aikaan pyrittiin selvittämään myös, kuinka paljon tietoturvallisuudesta ylipäätään puhuttiin työympäristössä ennen verkkokoulutuksen järjestämisestä tiedottamista (Kuvio 6).



Kuvio 6: Kuinka usein tietoturvallisuudesta puhutaan työympäristössäsi?

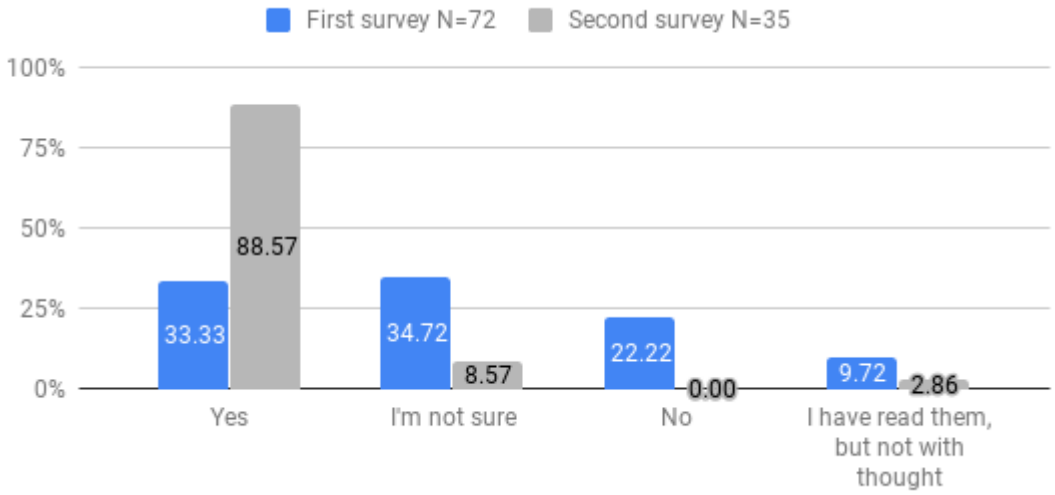
Kysymyksellä pyrittiin selvittämään, kuinka usein tietoturvallisuusasiat tulivat puheeksi yrityksessä ennen tietoturvakoulutuksen julkaisemista tai siitä ilmoittamista. 59 % vastaajista vastasi joskus, 22 % vastasi harvoin, noin 12 %:n mielestä usein, ja muutaman vastaajan mielestä ei ikinä. Erot todennäköisesti johtuvat joko vaihtelevista työtehtävistä vastaajien joukossa,

tai siitä miten yksilöt kokevat keskustelun määrän. Toisessa kyselyssä pyrittiin selvittämään kokevatko vastaajat keskustelun aiheesta lisääntyvän tulevaisuudessa (Kuvio 7).



Kuvio 7: Koetko, että tietoturvallisuudesta tullaan tulevaisuudessa puhumaan enemmän työympäristössäsi?

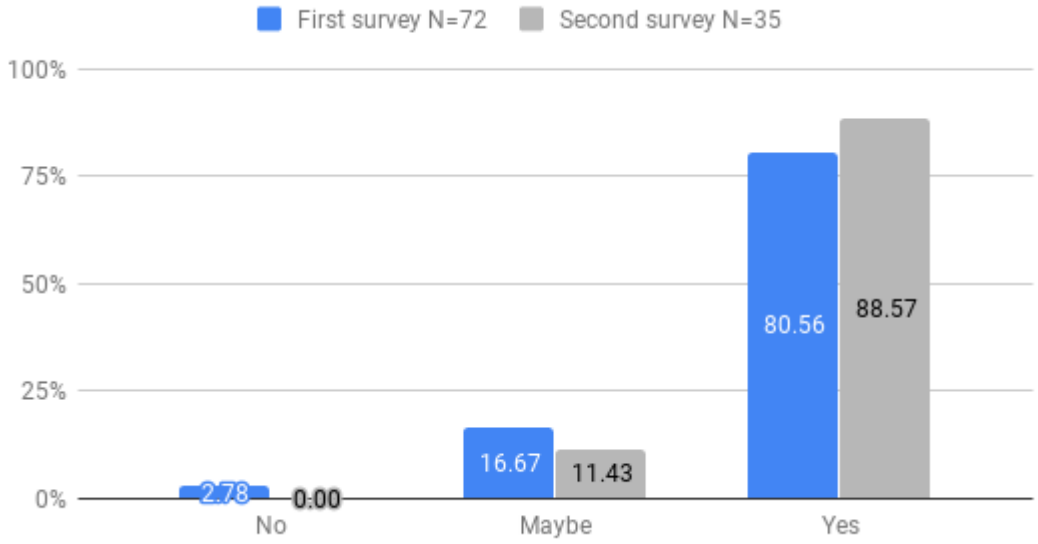
Toisessa kyselyssä kysymys oli muutettu kuvastamaan paremmin tulevaisuudennäkymiä. 71 % vastaajista oli sitä mieltä, että tietoturvallisuuskeskustelun määrä tulee kasvamaan tulevaisuudessa. Seuraava kysymys liittyi tiedon luokittelun periaatteisiin yrityksessä (Kuvio 8).



Kuvio 8: Olen lukenut ja ymmärrän yrityksen tietoturvaluokittelun periaatteet.

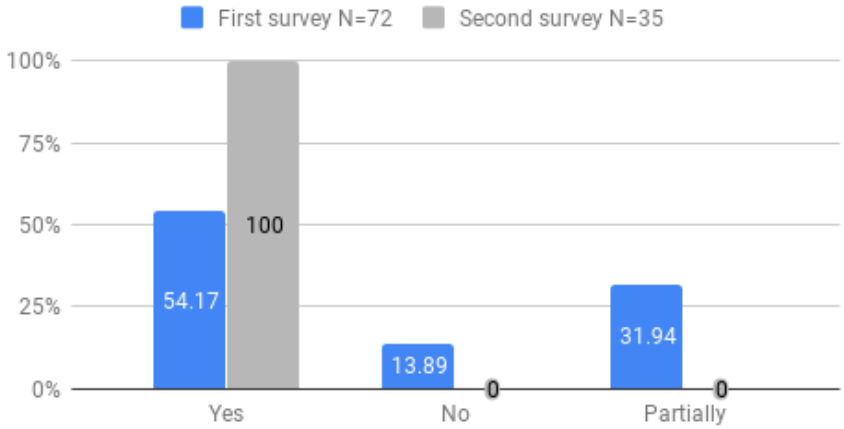
Tiedon suojaluokittelun periaatteet olivat ensimmäisen kyselyn aikaan vastaajille kohtalaisen tuntemattomia, vain 33 % kertoi tietäneensä niiden sisällöstä. Suurin osa kertoi, ettei tiedä

tai on vain silmäillyt ne läpi. Verkkokoulutuksen jälkeen kuitenkin jopa 88 % kertoi tietäneensä sisällön, sillä niihin tutustuminen oli osa verkkokoulutuksen sisältöä. Seuraavassa kuviossa on eroteltu myös tietojen luokitteluun liittyvä seikka, kun kysyttiin sisäisen ja luottamuksellisen tiedon eroja (Kuvio 9).



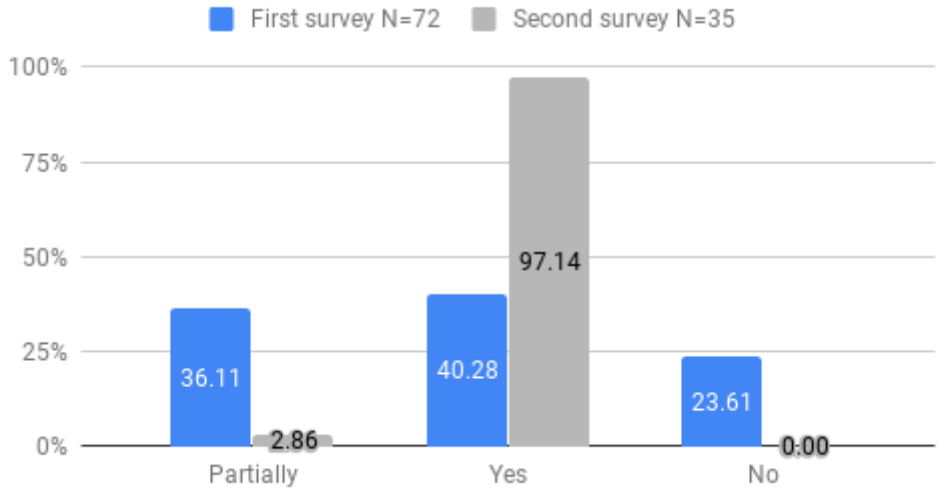
Kuvio 9: Tiedän sisäisen ja luottamuksellisen tiedon erot.

Ensimmäisen kyselyn aikaan noin 81 % tiesi yrityksen tiedon luokittelun mukaisen eron sisäisen ja luottamuksellisen tiedon eroissa. Noin 17 % kertoi ehkä tietävänsä erot. Vastaavat prosentit toisen kyselyn aikaan oli 89 % ja 11 %. Seuraavassa kohdassa on esiteltynä turvallisten työtapojen tietämys toimistolla työskenneltäessä (Kuvio 10).



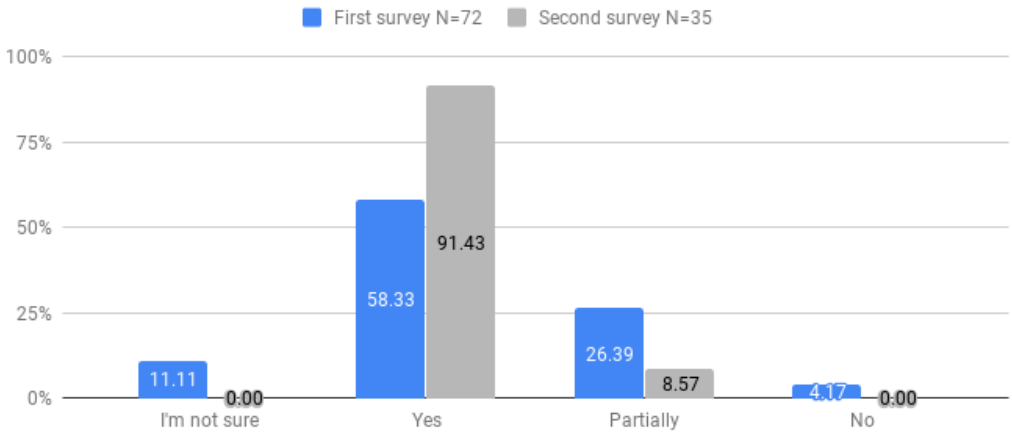
Kuvio 10: Tiedän toimistolla työskentelemiseen liittyvät tietoturvallisuusohjeet.

Tietoturvallisuusohjeet toimistolla työskentelyyn vaikutti olleen hyvinkin pimennossa ennen koulutuksen käymistä. Ohjeita oli aiemminkin olemassa, mutta ne eivät olleet laajassa jaossa henkilöstölle, vaan lähinnä muistutuslappuina ja -viesteinä ympäri toimipisteitä. Koulutuksen jälkeen kuitenkin 100 % vastaajista tiesi turvalliset toimintatavat. Kuviossa 11 on esiteltynä vastaava kysymys mutta liittyen etätyöskentelyyn.



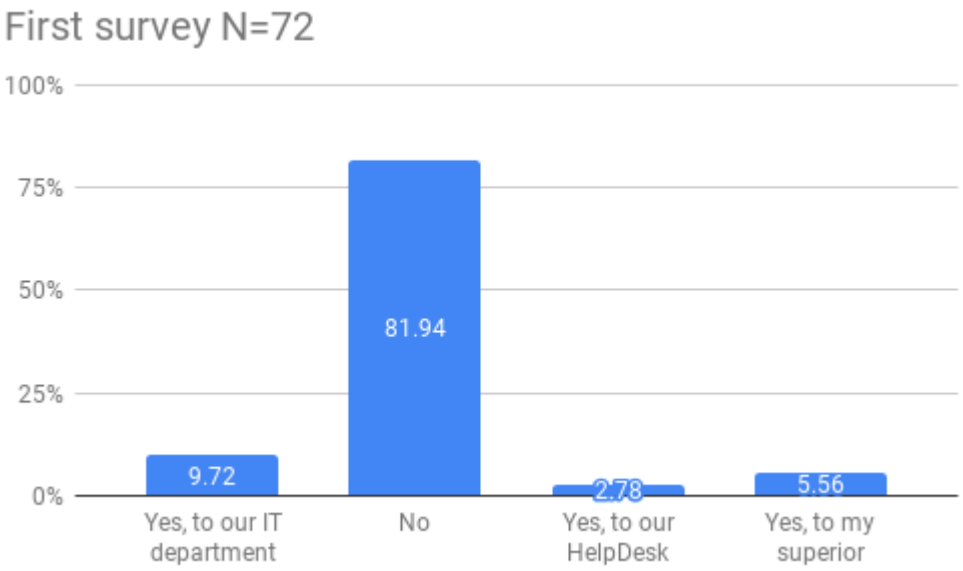
Kuvio 11: Tiedän etätyöhön liittyvät tietoturvallisuusohjeet.

Tilanne oli etätyöskentelyn osalta sama kuin esitetty kuviossa 16. Ohjeet olivat olemassa, mutta eivät laajassa jaossa. Koulutuksen jälkeen vastaajien mielestä kuitenkin 97 % koki tietävänsä ohjeet myös etätyöskentelyyn. Kyselyihin vastaajista kaikki käyttivät työnantajan tarjoamia mobiililaitteita tai tietokoneita. Seuraavassa kohdassa kysyttiin, tietävätkö vastaajat niihin liittyvät turvallisuusohjeet (Kuvio 12).



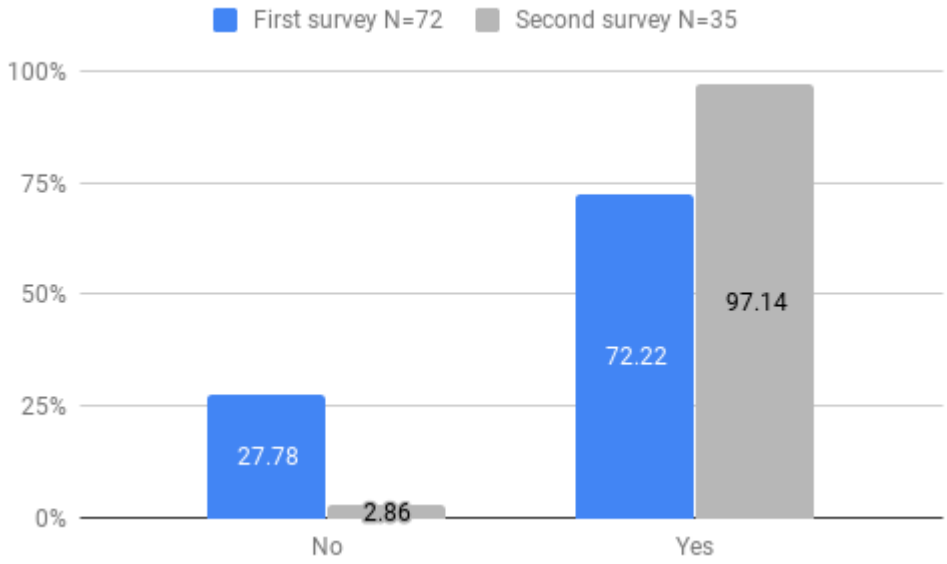
Kuvio 12: Tiedän työnantajan mobiililaitteisiin ja tietokoneisiin liittyvät tietoturvallisuusohjeistukset.

Tietoturvallisuusohjeet työnantajan tarjoamille laitteille oli ensimmäisessä kyselyssä tiedossa vain 58 %:lla, ja 26 % vastaajista koki tiedon olevan osittain hallussa. Toisen kyselyn aikaan 91 % kuitenkin koki jo tietävänsä ohjeet. Ohjeet olivat osana verkkokoulutusta. Seuraavaksi kyselyssä oli salasanoihin ja tunnustenhallintaan liittyvä aihealue (Kuvio 13).



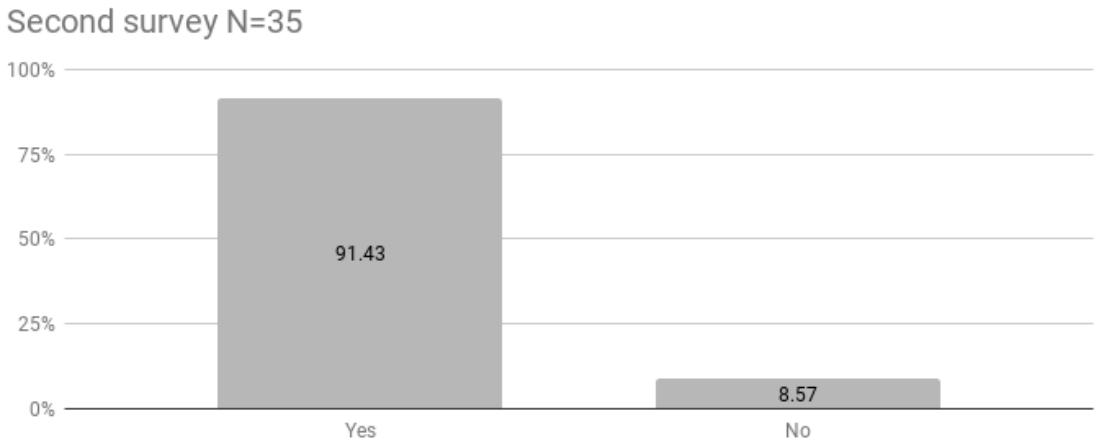
Kuvio 13: Oletko ikinä antanut kenellekään salasanaasi tai muita kirjautumistietojasi?

Ensimmäisessä kyselyssä selvitettiin avoimen kysymyksen avulla, kenelle on mahdollisesti antanut aiemmin salasanojaan tai muita kirjautumistietojaan. Osa sanoi antaneensa tietoja esimiehille, IT-osastolle tai Helpdeskiin. IT-osasto mahdollisesti tarvitsi tunnuksia ennen töidensä hoitamiseen pidemmän aikaan sitten, joka selittäisi tämän. Uuden ohjeistuksen ja teknologian mahdollistamana IT-osasto ei enää kuitenkaan salasanoja pyydä tai tarvitse. Verkkokoulutuksen käymisen jälkeen vastasivat kaikki kyselyyn vastanneet, etteivät aio jatkossa jakaa salasanaansa missään olosuhteissa. Tietoturvapoikkeamien tunnistaminen ja niistä raportointi oli suuri osa verkkokoulutuksen sisältöä, ja seuraavassa kohdassa on esiteltynä siihen liittyvää dataa (Kuvio 14).



Kuvio 14: Tiedän, mihin tietoturvapoikkeamista tulee raportoida.

Tietoturvatapahtumista raportointi oli tiedossa 72 %:lla. kun 28 % ei siitä tiennyt. Koulutuksen jälkeen raportointi oli hallussa jo 97 %:lla. Viimeisenä kysymyksenä toisessa kyselyssä oli vastaajien henkilökohtainen suhtautuminen verkkokoulutukseen (Kuvio 15).



Kuvio 15: Koetko tietoturvallisuusosaamisesi parantuneen verkkokoulutuksen käymisen myötä?

Viimeisenä kysymyksenä toisessa kyselyssä oli vielä kokemukset tietoturvallisuuskoulutuksen hyödyllisyydestä. Vastaajista 91 % koki, että koulutuksesta oli hyötyä heidän osaamiselleen, ja se myös näkyi positiivisena muutoksena kyselyn tuloksissa.

Kumpaankin kyselyyn vastanneista yli 94 % kummassakin kyselyssä koki tietoturvallisuuden olevan jokaisen työntekijän vastuulla. Myös henkilökohtaisen vastuun kohdalla prosentit olivat

samanlaisia. Ensimmäisessä kyselyssä noin 83 % tiedosti käsittelevänsä salausluokiteltuja tietoja työnkuvassaan, kun toisen kyselyn aikaan vastaava prosentti oli jo noin 91 %. Ensimmäisen kyselyn aikaan noin 69 % myönsi avaavansa sähköposteissa olevat liitteet ja tiedostot varmistamatta, kuka sen lähettäjä on. Toisen kyselyn aikaan vastaava prosentti oli jo noin 89 %.

7 Johtopäätökset ja oman työn arviointi

Tutkimuksen tarkoituksena oli selvittää, minkälainen pohja henkilöstöllä on ollut tietoturvallisuusasioissa ennen verkkokoulutuksen julkaisemista, ja miten se mahdollisesti kehittyi sen jälkeen. Tutkimuksen alussa tiedettiin, että todennäköistä kehitystä tulee tapahtumaan johtuen tietoturvaohjeiden puuttumisesta ylipäätään. Tutkimuksen kysymyksillä pyrittiin aluksi selvittämään lähtötaso, ja sen jälkeen pyrittiin selvittämään, eri onko aihealueilla tapahtunut kehitystä tietoturvallisuuskoulutuksen julkaisemisen myötä.

Taustamuuttujissa ei ollut suuria eroja kyselyiden välillä. Tällä ei varsinaisesti ole vaikutusta kyselyn tuloksiin sillä yrityksessä ei ollut aiemmin ollut käytössä laajamittaista tietoturvallisuuskoulutusta. Tästä voidaan kuitenkin päätellä, että vastaajakunta molemmissa kyselyissä on pysynyt tilastoiden puitteissa suurin piirtein samana.

Vastauksista kävi ilmi, että tietoturvallisuusosaaminen on todella kasvanut yrityksessä huomattavasti. Suurimmassa osassa kysymyksistä ”oikean” vastauksen vastausmäärä oli kasvanut keskimäärin 56 %. Epävarmat ehkä ja osittain -vastaukset poistuivat toisen kyselyn kohdalla lähes kokonaan, ja tuntui että vastaajat olivat saaneet varmuutta koulutuksen sisällön sisäistettyään. Erityisen positiivista muutosta tapahtui kehitykselle liittyen eri paikoissa työskentelyyn, jossa ohjeet eivät olleet lähelläkään haluttua tasoa ensimmäisen kyselyn aikaan.

Vastaajat tiesivät jo ensimmäisen kyselyn aikaan, että tietoturvallisuus kuuluu jokaisen työntekijän vastuulle. Tämä on positiivinen asia tulevaisuuden kannalta, sillä se on perusta kaikelle tietoturvatyölle. Tietoturvallisuuskulttuuri pohjautuu yksilöiden osallistamiseen, ja työntekijöiden positiivinen suhtautuminen tietoturvatyöhön on ehdotonta sen menestykselle. Tämä helpottaa myös tietoturvallisuuteen liittyvän kuukausittaisen uutiskirjeen menestystä, sillä kiinnostusta tietoturvallisuustyölle selvästi on. Tätä tukee myös se seikka, että vastaajat kokivat myös henkilökohtaisesti tietoturvallisuusosaamisensa kasvaneen verkkokoulutuksen myötä. Tietoturvallisuustyö tulee yrityksessä jatkumaan positiivisten tutkimustulosten takia, ja päivityksiä tietoturvallisuusosaamiseen tullaan varmasti tekemään alan kehittyessä.

Tutkimuksen lopputulokset viittaisivat erityisen positiiviseen muutokseen. Täytyy kuitenkin muistaa, että vastaajamäärät kyselyiden välillä vaihtelivat paljon. Tämä johtuu osittain kyselyn järjestämisen lyhyestä aikavälistä, jolloin kaikki vastaajat eivät välttämättä olleet kerenneet suorittamaan verkkokoulutusta, ja osittain työympäristössä tapahtuneista muutoksista,

joihin ei kellään ollut vaikutusvaltaa. Mikäli jälkimmäiseen kyselyyn olisi saatu enemmän vastaajia olisivat tulokset olleet varmasti osittain erilaisia, mutta saadun tiedon valossa suunta on kuitenkin parempaan. Lähinnä koulutuksen positiivinen vaikutus luo työntekijöille luonnollista kiinnostusta aihealueeseen, jolloin he mahdollisesti miettivät tekemisiään ja päätöksiään työympäristössä nykyään myös tietoturvallisuuden kannalta.

7.1 Tutkimuskysymykset

Ensimmäinen tutkimuskysymys ”Onko tietoturvallisuuskoulutuksesta hyötyä yrityksen henkilöstön osaamisen kannalta?” voidaan vahvistaa tämän opinnäytetyön tulosten valossa. Kuten kappaleessa 6 ja 7 on esitetty, on tietoturvallisuusosaamisessa tapahtunut selvää muutosta, keskimäärin 56 % positiivisempaan suuntaan. Vastaajista useimmat ovat siis kyselyiden välillä selvästi saaneet lisää osaamista, ja suurin osa vastaajistakin koki tietoturvallisuuskoulutuksen kehittäneen heitä.

Vastaus toiseen tutkimuskysymykseen ”Onko tietoturvallisuuskoulutus tehokas keino tietoturvaosaamisen lisäämiseksi?” on myös kyllä. Saatujen positiivisten tulosten valossa voidaan kokea, että ulkoisen palveluntarjoajan verkkokoulutuspohja on hyvinkin kustannustehokas keino koulutuksen levittämiseen. Käytännössä ainoat kulut verkkokoulutuksen päivityksen lisäksi tulee pohjan käyttämisen lisenssistä ja verkkokoulutuksen käymiseen menetetystä työajasta. Tiedon saavutettavuus on myös hyvä, ja koulutukseen on helppo lisätä päivityksiä. Myös uudelleen jakaminen on helppoa, kun pohjaa voidaan jakaa esimerkiksi linkin välityksellä sisäisissä sähköposti- ja muissa viestintäkanavissa.

7.2 Oman työn arviointi

Opinnäytetyö voitaisiin samoilla kysymyksillä toteuttaa helposti, ja vertailla vastauksia samoihin kysymyksiin esimerkiksi vuoden päästä, ja verrata tästä työstä saatuihin tuloksiin. Tilanne toimeksiantajalla on mahdollisesti tätä tutkimusta parempi jatkuvan tietoturvallisuustyön vuoksi. Kysymyksiä on myös mahdollista muokata tai lisätä riippuen siitä, minkälaisiin asioihin toimeksiantaja päättää tietoturvallisuustyössä keskittyä esimerkiksi tästä tutkimuksesta saatujen löydösten perusteella, tai sen pohjalta minkälaisia tietoturvallisuusuhkia pidetään milläkin hetkellä kaikkein tärkeimpinä.

Tutkimuksen validiteettia eli pätevyyttä voi pitää riittävänä, sillä kysymysten avulla saatiin vastattua kumpaankin tutkimuskysymykseen eli ”Onko tietoturvallisuuskoulutuksesta hyötyä työntekijöiden tietoturvaosaamisen kannalta?” ja ”Onko tietoturvallisuuskoulutus tehokas keino (tietoturva)tietoisuuden lisäämiseksi?”.

Opinnäytetyön rajaus auttoi teoriapohjan ja tutkimuksen pääkohtien rakentamisessa. Työn aihe oli sikäli opinnäytetyön tekijälle tuttu, että hän oli ollut mukana koulutuksen ja tietotur-

vallisuusmanuaalin kehittämisessä. Tästä oli apua esimerkiksi tutkimuskysymysten muodostamisessa' sekä kyselyä järjestäessä. Opinnäytetyön tekeminen oli pitkä prosessi, mutta auttoi tekijää selvästi oman roolinsa ymmärtämisessä sekä ammatillisen kehityksen kasvussa. Opinnäytetyön teon ja tutkimuksen pohjalta tekijä sai paljon oppia alalta ja työtehtävistä, jotka häntä tulevaisuudessa kiinnostavat.

Lähteet

Painetut

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. 12. painos. Jyväskylä: Tammi.

Laaksonen, M., Nevasalo, T. & Tomula, H. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Miettinen, J. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media.

SFS-EN ISO/IEC 27000:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen Standardoimisliitto. Viitattu 15.5.2019.

SFS-EN ISO/IEC 27001:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto. Viitattu 15.5.2019.

SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen Standardoimisliitto. Viitattu 15.5.2019.

Vehkalahti, K. 2014. Kyselytutkimuksen mittarit ja menetelmät. Finn Lectura.

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Sähköiset

BSIGroup. 2019. How are standards made? Viitattu 29.4.2019. https://www.bsigroup.com/en-GB/standards/Information-about-standards/how-are-standards-made/

Bureau of Labor Statistic. 2019. Information Security Analysts. Viitattu 27.4.2019 https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Burgess, M. 2016. TalkTalk hack toll: 100k customers and £60m. Viitattu 30.4.2019 https://www.wired.co.uk/article/talktalk-hack-customers-lost

Conrad, E. Feldman & J. Misenar, S. 2016. Chapter 2 - Domain 1: Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity). Viitattu 13.4.2019. https://www.sciencedirect.com/science/article/pii/B9780128024379000023

Constantin, L. 2019. Data breaches exposed 5 billion records in 2018. Viitattu 1.5.2019. https://www.csoonline.com/article/3341317/data-breaches-exposed-5-billion-records-in-2018.html

Euroopan Unioni. 2016. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Viitattu 11.4.2019. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI#d1e3363-1-1

GDPREU. 2018. Fines and penalties. Viitattu 11.4.2019. https://www.gdpreu.org/compliance/fines-and-penalties/

Gartner. 2018. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Viitattu 31.4.2019. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

IBM, 2018. 2018 Cost of a Data Breach Study: Global Overview. Viitattu 22.4.2019. https://www.ibm.com/downloads/cas/861MNWN2

ICT Institute. 2017. Information security and PDCA (Plan-Do-Check-Act). Viitattu 3.5.2019. https://ictinstitute.nl/pdca-plan-do-check-act/

Information Security Forum. 2018. The ISF Standard of Good Practice for Information Security 2018. Viitattu 4.3.2019. https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/

Infradata. 2018. Top Five Cyber Security Threats in 2019. Viitattu 30.3.2019. https://www.infradata.nl/en/news-blog/top-5-cyber-security-threats-in-2019/

ISO. 2019a. Standards. Viitattu 30.4.2019. https://www.iso.org/standards.html

ISO. 2019b. All about ISO. Viitattu 15.5.2019. https://www.iso.org/about-us.html

ISO. ISO/IEC 27000 family - Information security management systems. Viitattu 30.4.2019. https://www.iso.org/isoiec-27001-information-security.html

ISO. ISO/IEC 27002:2005. Information technology -- Security techniques -- Code of practice for information security management. Viitattu 11.4.2019. https://www.iso.org/standard/50297.html

ISO. ISO/IEC 27002:2013. Information technology -- Security techniques -- Code of practice for information security controls. Viitattu 30.3.2019. https://www.iso.org/standard/54533.html

Kaspersky Lab. 2018. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Viitattu 25.2.2019. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kosutic, D. 2014. How to perform training & awareness for ISO 27001 and ISO 22301. Viitattu 22.1.2019 https://advisera.com/27001academy/blog/2014/05/19/how-to-perform-training-awareness-for-iso-27001-and-iso-22301/

Kovacs, E. 2019. Data Breach Cost Marriott $28 Million So Far.Viitattu 22.2.2019 https://www.securityweek.com/data-breach-cost-marriott-28-million-so-far

Martin, J. 2018. What is access control? A key component of data security. Viitattu 11.1.2019. https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html

Martin, M. 2014. Cybersecurity Awareness Is About Both 'Knowing' and 'Doing'. Viitattu 25.3.2019. https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/

Maurer, R. 2015. Human Error Cited as Top Cause of Data Breaches. Viitattu 29.1.2019. https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/human-error-top-cause-data-breaches.aspx

Miller, M. 2006. ISO 17799 and 27001: Setting the Standards for Information Security. Viitattu 21.4.2019. https://www.bankinfosecurity.com/iso-17799-27001-setting-standards-for-information-security-a-165

Nobles, C. 2018. Shifting the Human Factors Paradigm in Cybersecurity. Viitattu 23.3.2019. https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/17.pdf

Positive Technologies. 2018. Cybersecurity threatscape 2018 Q2. Viitattu 21.1.2019. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018-q2/#id2

Puolustusministeriö, 2015. Katakri 2015 – tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 25.3.2019. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Researchgate. Placing IDS in a normal network. Viitattu 30.4.2019. https://www.researchgate.net/figure/placing-IDS-in-a-normal-network_fig3_311312293

SANS. Information Security Resources. Viitattu 3.5.2019. https://www.sans.org/information-security/

Shepard, S. 2018. The Average Cost of a Data Breach. Viitattu 3.5.2019. https://security-today.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx

Suomen Standardoimisliitto. ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä. Viitattu 30.3.2019. https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta

Tietosuojalaki 1050/2018. Viitattu 11.4.2019. https://www.finlex.fi/fi/laki/alkup/2018/20181050

VAHTI-toiminta. Valtiovarainministeriö. Viitattu 21.1.2019. https://vm.fi/vahti

Valtionhallinnon tietoturvasanasto. 2008. Valtiovarainministeriö. Viitattu 14.5.2019. https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229

Venable, D. 2017. Information security is not information technology. Viitattu 15.5.2019. https://www.csoonline.com/article/3225344/information-security-is-not-information-technology.html

Wainstein, L. 2018. 6 Top Information Security Risks to Know About as You Prepare for 2019. Viitattu 29.4.2019. https://www.getastra.com/blog/cms/information-security-risks-to-know-about-as-you-prepare-for-2019/

Zacks, A. 2018. Can an Antivirus Protect your IoT Devices in 2019? Viitattu 3.5.2019. https://www.safetydetective.com/blog/can-antivirus-protect-your-iot-devices/

Julkaisemattomat

Information security manual. 2018.

Kuviot

Liitteet

Liite 1: Kyselyn 1 kysymykset

1) What is your gender?
    a) Female
    b) Male
    c) Prefer not to say
    d) Other:
2) How old are you?
    a) Under 25
    b) 25-35
    c) 35-45
    d) 45 or older
    e) I prefer not to say
3) How long have you worked at (name changed)?
    a) 0-1 years
    b) 1-5 years
    c) 5-10 years
    d) More than 10 years
4) Do you know what information- and cyber security are?
    a) Yes
    b) No
    c) Maybe
5) Have you received information security training at (name changed)?
    a) Yes, I have
    b) I don't remember
    c) No, I haven't
6) Information security is every employees' responsibility.
    a) Disagree
    b) Maybe
    c) Agree
7) My personal choices play a significant role in protecting information.
    a) Agree
    b) Disagree
    c) Partially
8) How often is information security discussed in your work environment?
    a) Often
    b) Sometimes
    c) Rarely
    d) Never
    e) I'm not sure
9) I'm familiar with (name changed) Information Classification Guidelines.
    a) Yes
    b) No
    c) Maybe
    d) I have read them, but not with thought
10) I handle classified information in my job assignment.
    a) True
    b) False

c) Maybe

11) I know the difference between internal and confidential information.

a) Yes
b) No
c) Maybe

12) Do you know the information security guidance when working at the office?

a) Yes
b) No
c) Maybe

13) Do you know the information security related rules for remote working?

a) Yes
b) No
c) Maybe

14) When traveling, I can talk about work related matters if I'm being careful.

a) Yes
b) No
c) Maybe

15) Are you using (name changed) provided computer/mobile devices?

a) Yes
b) No

16) I am aware from the information security perspective what I am allowed to do with my employer provided computer or mobile devices.

a) Yes
b) No
c) Partially
d) I'm not sure

17) Have you ever given anyone your password or other login information?

a) Yes
b) No
c) Other:

18) If someone you don't know sends you an attachment or link via e-mail, how likely are you to open it?

a) I always open links and attachments without thinking about it
b) Depends: if they seem trustworthy
c) I never open links or attachments from people I don't know without making sure who they are first.
d) I'm not sure

19) I know where to report all information security related incidents.

a) Yes
b) No

Liite 2: Kyselyn 1 saateteksti

Information security awareness survey for (name changed) personnel.

Please answer the following questions with thought. Answering this survey should take you under 5 minutes. This survey is part of a bachelor's thesis, and all your answers are highly appreciated. The purpose of this survey is to find out the level of information security awareness at (name changed) site at this time. All the data will be handled confidentially, and no personal information will be recorded.

Liite 3: Kyselyn 2 kysymykset

1) What is your gender?
    c) Female
    d) Male
    e) Prefer not to say
    f) Other:
2) How old are you?
    a) Under 25
    b) 25-35
    c) 35-45
    d) 45 or older
    e) I prefer not to say
3) How long have you worked at (name changed)?
    a) 0-1 years
    b) 1-5 years
    c) 5-10 years
    d) More than 10 years
4) Did you complete the first part of the survey back in August?
    a) Yes
    b) No
    c)
5) Do you know what information- and cyber security are?
    a) Yes
    b) No
    c) Maybe
6) Have you received information security training at (name changed)?
    a) Yes, I have
    b) I don't remember
    c) No, I haven't
7) Information security is every employees' responsibility.
    a) Disagree
    b) Maybe
    c) Agree
8) My personal choices play a significant role in protecting information.
    a) Agree
    b) Disagree
    c) Partially

9) Do you think information security will be discussed more in your work environment in the future? *
   a) Yes
   b) No
   c) Maybe

10) I'm familiar with (name changed) Information Classification Guidelines.
   a) Yes
   b) No
   c) Maybe
   d) I have read them, but not with thought

11) I handle classified information in my job assignment.
   a) True
   b) False
   c) Maybe

12) I know the difference between internal and confidential information.
   a) Yes
   b) No
   c) Maybe

13) Do you know the information security guidance when working at the office?
   a) Yes
   b) No
   c) Maybe

14) Do you know the information security related rules for remote working?
   a) Yes
   b) No
   c) Maybe

15) When traveling, I can talk about work related matters if I'm being careful.
   a) Yes
   b) No
   c) Maybe

16) Are you using (name changed) provided computer/mobile devices?
   a) Yes
   b) No

17) I am aware from the information security perspective what I am allowed to do with my employer provided computer or mobile devices.
   a) Yes
   b) No
   c) Partially
   d) I'm not sure

18) How likely are you to give other people your passwords or other login information in the future?
   a) I will not share my passwords with anyone
   b) Depends: if they seem trustworthy

19) Have you ever given anyone your password or other login information?

a) Yes
b) No
c) Other:

20) If someone you don't know sends you an attachment or link via e-mail, how likely are you to open it?

a) I always open links and attachments without thinking about it
b) Depends: if they seem trustworthy
c) I never open links or attachments from people I don't know without making sure who they are first.
d) I'm not sure

21) I know where to report all information security related incidents.

a) Yes
b) No

Liite 4: Kyselyn 2 saateteksti

Information security awareness survey for (name changed) personnel

Please answer the following questions with thought. Answering this survey should take you under 5 minutes. This survey is part of a bachelors thesis, and all your answers are highly appreciated. The purpose of this survey is to find out the level of information security awareness at HKScan Turku site at this time. All the data will be handled confidentially, and no personal information will be recorded.