LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Henkilöstön ja johdon tietoturva-barometrin tarkentava analyysi

Linda Mellin

Laurea-ammattikorkeakoulu

Henkilöstön ja johdon tietoturvabarometrin tarkentava analyysi

Linda Mellin
Tietojenkäsittely
Opinnäytetyö
kesäkuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma (AMK)

Linda Mellin

Henkilöstön ja johdon tietoturvabarometrin tarkentava analyysi

Vuosi 2018 Sivumäärä 68

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) toteutti syksyllä 2017 Henkilöstön ja johdon tietoturvabarometrin. Tutkimukseen sai osallistua valtionhallinnon, kuntien, sairaanhoitopiirien, yliopistojen ja seurakuntayhtymien työntekijät. Kyselyyn osallistui 105 organisaatiota, 60 valtionhallinnon organisaatiota, 38 kuntaa, kolme sairaanhoitopiiriä, kolme yliopistoa ja yksi seurakuntayhtymä. Vastaajia oli yhteensä 8123.

Opinnäytetyön tarkoitus oli analysoida tuloksia esimiesten, johtoryhmän jäsenten, tietohallinnon ja tietoturvan työntekijöiden vastauksista. Tuloksien avulla pystytään arvioimaan organisaatioissa olevia kehittämiskohteita tietoturvallisuuden kehittämisen osalta. Näiden tietojen avulla Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä pystyy suunnittelemaan tulevia koulutuksia ja ohjausten sisältöjä sekä teemoja. Raportin taustana toimii syksyllä 2017 tehty Henkilöstön ja johdon tietoturvabarometri.

Lähes kaikki vastaajat kokivat tietoturvallisuuden toteutuvan hyvin organisaatiossaan ja päivittäisen työskentelyn hyvin turvalliseksi tai turvalliseksi. Kyselystä selvisi, että ohjeistuksen saaminen on huomattavasti yleisempää kuin koulutuksen saaminen. Yli puolet vastaajista ei kokenut tarvetta lisäohjeistukselle tai lisäkoulutukselle, kuitenkin sanallisen palautteen perusteella lisäkoulutuksella oli tarvetta ja se koettiin hyväksi keinoksi jakaa tietoa henkilöstölle.

Esimiehiä ja johtoryhmän jäseniä huolestutti eniten tärkeiden tietojen menetys laiterikon takia. Tietohallinnon vastaajia huolestutti eniten, että eivät saa tarpeeksi tukea johdolta tietosuojalle. Tietoturvan vastaajia huolestutti eniten, että eivät saa tarpeeksi johdon tukea tietoturvallisuudelle. Tietoturvallisuuden perusasioissa on vielä parannettavaa. Vastausten mukaan työntekijät toivovat lisää koulutusta ja ohjeistusta. Lisäksi tulisi kehittää uudenlaisia tapoja kehittää henkilöstön tietoturvaosaamista ja tietoturvatiedottamista. Tietoturvaosaamista tulisi kehittää osana henkilöstön jokapäiväistä työntekoa. Johdon ja esimiesten tukea kaivataan enemmän tietoturvasta ja tietosuojasta. Esimiesten ja johdon vastausten perusteella konkreettisille harjoituksille häiriötilanteiden hallinnassa on perusteltu tarve.

Asiasanat: tieturvabarometri, VAHTI, barometri, tietoturvallisuus

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology

Linda Mellin

Targeted Analysis of the Information Safety Barometer Concerning Public Administration Organizations and Personnel

Year 2018 Pages 68

The Public Sector Digital Security Management Board (VAHTI) completed an information safety barometer concerning public administration organizations and personnel in the Autumn of 2017. The research was open to the employees of the central governmental administration, municipalities, hospital districts, universities and congregations. 105 organizations participated in the survey of which 60 were from the central administration, 38 municipalities, three hospital districts, three universities and one congregation. There were 8123 respondents overall.

The purpose of the thesis is to analyse the findings from the point of view the manager, management, data administration and information security workers. The results help in the evaluation of what should be improved in the organization's information security. With this information, the public sector digital security management can plan future trainings. The basis for this report is the 2017 information safety barometer concerning public administration organizations and personnel.

Almost all the respondents thought that the working environment is safe and that the information security is effectively managed in the organization. The survey also shows that the employees received more instruction than education. Over half of the respondents didn't want more instruction or trainings. However, in the open questions section, the respondents though there should be more education and that would be a good way to inform the employees.

Managers and management were the most worried about losing important information due to broken devices. Data administration employees were the most worried over not receiving enough support for data protection from management. Information security employees were worried over not receiving enough support for information security from the management. Survey revealed room for improvement in the basics of information security. Employees themselves hoped for more education and instruction. Furthermore, they hoped for new ways of improved employee knowledge in information security and the way they are informed. The information security vocabulary should be part of everyday work. Employees also wished more support for data protection and information security from the management. Managers and management hoped for more concrete training exercises on the management of disturbance situations.

Keywords: Information Security Barometer, VAHTI, Barometer, Information Security

Sisällys

1 Johdanto

Tietoturvan tärkeys on digitalisaation myötä muuttunut tärkeäksi osaksi jokapäiväistä työntekoa. Johdolla, esimiehillä ja ICT-puolen työntekijöillä on suuri vastuu tietoturvan jalkauttamisessa ja ottamisesta osaksi organisaation jokapäiväistä työskentelyä. Opinnäytetyössä analysoidaan tarkemmin johtoryhmän jäsenet, esimiesten, tietohallinnon ja/tai ICT:n ja tietoturvan, tietosuojan ja kyberturvallisuuden työntekijöiden vastauksia vuoden 2017 henkilöstön ja johdon tietoturvabarometristä. Tietohallinnon ja/tai ICT:n vastaajia kutsutaan myöhemmin raportissa tietohallinnoksi. Tietoturvan, tietosuojan ja kyberturvallisuuden vastauksia kutsutaan raportissa myöhemmin tietoturvaksi. Tutkimuksen tarkoituksena on saada parempi kuva siitä, miten organisaatioiden esimiehet, johtoryhmän jäsenet, tietohallinnon sekä tietoturvallisuuden työntekijät kokevat tietoturvan toteutumisen organisaatiossa ja eroavatko heidän vastauksena merkittävästi muiden organisaatiossa vastanneiden kanssa. Raportissa käytetään kaikkien vastaajien tuloksia vertailukohteena.

1.1 Henkilöstön ja johdon tietoturvabarometri

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) on valtiovarainministeriön asettama julkisen hallinnon yhteistyöelin, valmisteluelin ja koordinaatioelin, jonka tarkoitus on kehittää digitaalista turvallisuutta ja ohjeistaa siitä. (vm.fi/vahti) Henkilöstön ja johdon tietoturvabarometri on toista kertaa julkisen hallinnon digitaalisen turvallisuuden johtoryhmän toteuttama kysely julkisen hallinnon työntekijöille. Ensimmäisen kerran se toteutettiin syksyllä 2016. Kyselyn tarkoituksena on selvittää tietoturvallisuuden kysyttyjen osa-alueiden toteutuminen organisaatiossa henkilöstön näkökulmasta.

Henkilöstön ja johdon tietoturvabarometrin tarkoitus on saada selkeä kuva valtionhallinnon, kuntien ja sairaanhoitopiirien tietoturvatasosta, tietoturvan ymmärtämisestä, henkilöstön saamasta koulutuksesta, ohjeistuksesta sekä tietosuoja-asetuksen näkyvistä muutoksista (Kuivalainen, Rousku 2016). Vuoden 2017 Henkilöstön ja johdon tietoturvabarometriin annettiin yliopistoille ja seurakuntayhtymille mahdollisuus osallistua kyselyyn (Rousku 2018).

1.2 Tutkimuksen tavoitteet

Tutkimus tulosten kautta pyritään enteilemään tulevaisuuden ongelmia. (Alapuro, Arminen 2004, 8). Tutkimuksessa selviävien tietojen avulla pystytään arvioimaan organisaatioissa olevia puutteita. Näiden tietojen avulla julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) pystyy paremmin suunnittelemaan tulevien koulutusten ja ohjausten sisältöä ja teemoja, jotta organisaatiot pystyvät kehittämään ja tekemään toimintaansa turvallisemmaksi. Edistämisellä aiotaan käytäntöjen ja toimintaperiaatteiden kehittämiseen (Toikko, Rantanen 2004, 14). Lisäksi tutkimuksen toistamisella selviää, millaisia muutoksia organisaatiossa tapahtuu tulevina vuosina.

2 Tutkimusmenetelmä

Oikeiden metodien avulla voidaan päästä tutkimuksissa totuuden mukaisiin tuloksiin (Niiniluoto 1991, 60). Jotta tutkimuksessa saadaan oikeanlaisia tuloksia, tulee tutkimusmenetelmä valita tarkasti. Tutkimusmenetelmä tulee valita sen mukaan, mikä on järkevintä tutkimuksen kannalta. Tutkimus ei voi pohjaitua tutkijan omiin mieltymyksiin vaan kohteeseen ja tutkimusongelmiin (Räsänen, Anttila, Melin 2005, 10).

2.1 Kvantitatiivinen tutkimus

Kyselyn tutkimusmenetelmäksi valitaan joko kvantitatiivinen eli määrällinen tutkimus tai kvalitatiivinen eli laadullinen tutkimus. Kvalitatiivinen tutkimuksessa aineistoa kuvaillaan ja analysoidaan muuten kuin numeraalisesti (Eskoja, Suoranta 2008,13). Kvantitatiivisen tutkimuksen tarkoitus on kerätä vastauksia niin suurelta määrältä, että yhden henkilön vastauksilla ei ole merkitystä (Ronkainen, Karjalainen 2008, 19).

Määrällisen tutkimuksen ehtona on, että tulokset on mahdollista yleistää koskemaan suurempaa joukkoa (Laaksonen, Matikainen, Tikka 2013, 32). Kyselyssä on tarkoitus saada vastauksia niin suurelta ryhmältä, että vastausten perusteella on mahdollista luoda yleiskuva tietoturvallisuuden tasosta ja saada käsitys mistä aiheista tulevat koulutukset tulisi pitää. Tutkimusmenetelmäksi valittiin kvantitatiivinen tutkimus, sillä se sopii paremmin kyselyn kokoon ja tavoitteisiin.

2.2 Kysely

Mahdollisen suuren vastaajamäärän takia sähköinen kyselylomake on ainut järkevä ratkaisu tutkimuksen toteuttamiseen. Kysely on tärkeä tapa saada tietoa vastaajien ajattelutavoista, toimintatavoista ja mielipiteistä (Vehkalahti 2008, 11). Verkossa toteutettava kysely on helppo saada jokaiselle kyselyyn osallistuvalle organisaatiolle, sillä silloin tutkija ei pysty vaikuttamaan tutkimustuloksiin omilla näkemyksillään tai mielipiteillään. Kyselyä varten laadittiin lomake, jotta kysymykset ovat samassa muodossa kaikilla vastaajilla (Ronkainen, Pehkonen, Lindblom-Ylänne, Paavilainen 2013, 113-114).

Kyselyssä käytetään kahdenlaisia kysymysmuotoja, vaihtoehdollisia kysymyksiä ja avoimia kysymyksiä. Vaihtoehdollisissa kysymyksissä vastaaja valitsee vastausvaihtoehdon, joka ovat parhaiten sopivat (Ronkainen, Karjalainen 2008, 34). Avoimien kysymysten tarkoitus on saada vastaus ristiriitaisiin kysymysiin tai asioihin, jotka ovat moniselitteisiä (Ronkainen, Karjalainen 2008, 34). Avoimia kysymyksiä on kyselyssä kahdenlaisia, tarkentavia kysymyksiä ja tiettyä asiaa kysyvät kysymykset. Tarkentavissa kysymyksissä vastaaja pääsee tarkentamaan aiemman kysymyksen vastausta. Toisissa avoimissa kysymyksissä vastaajilta kysyttiin jokin tarkka kysymys johon haluttiin vastaus.

2.3 Tutkimuksen eettisyys

Tutkimukseen valituille organisaatiolle tarjottiin mahdollisuus osallistua tutkimukseen, kuitenkin niin, että jokaisen organisaation tuli itse ilmoittautua osalliseksi. Organisaatiolle laitettiin heidän ilmoittamaan sähköpostiin esittely siitä, millaista tutkimusta ollaan tekemässä. Ilmoittautumisen jälkeen organisaatiolle lähetettiin ohjeistus siitä, mitä kysytään ja miten kysymyksiin tulee vastata. Tutkittavilla tulee olla tieto millaista tutkimusta ollaan tekemässä ennen kuin he ilmoittautuvat siihen (Tuomi 2007, 145). Halutessaan vastaaja on voinut jättää kyselyn täyttämisen kesken tai jättää vastaamatta osaan kysymyksiä. Tutkittavalla tulee olla mahdollisuus keskeyttää tutkimus halutessaan, vaikka olisi antanut jo suostumuksensa (Mäkinen 2006, 95).

2.4 Tutkimuksen anonymisointi

Kaikki kyselyn vastaukset ovat anonymisoitu niin, että niistä ei ole mahdollista tunnistaa tiettyä vastaajaa, kuitenkin vastaaja organisaatio on mahdollista tunnistaa. Tutkimuksen tarkoitus ei ole tunnistaa tai erotella tutkimuksen vastaajia toisistaan (Kuula 2006, 208). Tutkimusetiikassa on tärkeää, että yksityishenkilöillä ja organisaatiolla on oikeus säilyä anonyymeina tutkimuksessa (Mäkinen 2006, 114). Jokaiselle organisaatiolle annettiin koodi, josta pystyy tunnistamaan, kuuluuko organisaatio valtionhallintoon, kuntiin, sairaanhoitopiireihin, yliopistoihin vai seurakuntayhtymään. Tunnistusnumeroon kuuluu loppuosa, josta organisaatio on tunnistettavissa, jotta jokaisen organisaation tulokset on mahdollista lähettää oikealle organisaatiolle. Organisaatioiden numerot jaettiin sattumanvaraisesti. Kyselyssä ei kysytty yksittäisten vastaajien nimiä, koska sille ei ollut tarvetta. Tutkimuksessa on tärkeää taata osallistujien anonymisointi, jotta heille ei koidu tutkimuksesta myöhempää haittaa (Mäkinen 2006, 120).

2.5 Tutkimuksen testaaminen

Kyselystä tulee tehdä testiversio, jossa testataan kyselyn vastattavuutta. Usein testaajat ovat tutkimusryhmän jäseniä tai luottohenkilöitä (Ronkainen, Karjalainen 2008, 39). Kyselystä tehtiin testausversio, jota pääsivät kommentoimaan VAHTI-työryhmien jäsenet. Heidän antamansa palautteen perusteella kyselyyn tehtiin muutoksia, jotka helpottivat vastaamista ja selvensivät kysymyksiä. Kysely avattiin lokakuussa, jolloin kaikille ilmoittautuneille organisaatioille lähetettiin salatulla viestillä linkki. Kyselyyn pystyi ilmoittautumaan marraskuuhun asti, ja kysely sulkeutui lopullisesti joulukuussa.

2.6 Tutkimuksen ja raportin rakenne

Kysely jaettiin useammalle sivulle, jotta sen tekeminen ei olisi liian raskasta. Kysymykset jaettiin aiheiden mukaan, niin että samaan aiheeseen liittyvät kysymykset olivat samalla sivulla. Raportin rakenteessa, taulukoissa ja otsikoinnissa on otettu mallia vuoden 2016 Henki-

löstön ja johdon tietoturvabarometristä (Kuivalainen, Rousku 2016) ja vuoden 2017 Henkilöstön ja johdon tietoturvabarometristä (Rousku, 2018), jotta tulosten vertaaminen barometreihin olisi helpompaa.

3 Tutkimustulokset ja yhteenveto

Kyselyyn vastasi yhteensä 105 eri organisaatiota, joista 60 oli valtionhallinnon organisaatiota, niistä viisi (5) ministeriöitä. 38 organisaatiota oli kuntia ja sairaanhoitopiirejä oli kolme (3), Tällä kertaa mukaan oli otettu myös yliopistot, joita kyselyyn vastasi kolme (3). Kyselyyn osallistui myös yksi (1) seurakuntayhtymä. Vastauksia tuli kaiken kaikkiaan 8123 (Rousku 2018). Johtoryhmän vastauksia oli 487. Esimiesten vastauksia oli 1261. Tietohallinnossa työskentelevien vastauksia tuli 505 ja tietoturvan parissa työskentelevien vastauksia tuli 159.

Kyselyssä kysyttiin 23 erilaista kysymystä koskien työtehtäviä, koulutuksen ja ohjeistuksen saantia, huolestuneisuutta sekä tunnistautumista. Esimiehiltä ja johtoryhmän jäseniltä kysyttiin kaksi lisäkysymystä (Rousku 2018). Ensimmäisenä vastaajilta kysyttiin ovatko he esimiehiä tai kuuluvatko he johtoryhmään. Näihin vastanneille oli kaksi kysymystä, joihin ei voinut vastata jos kuului vain henkilöstöön. Kaikilla vastanneilla oli mahdollisuus valita toimenkuvakseen useampi kuin yksi vaihtoehto.

Kaikista vastanneista esimiehiä oli 1261 eli 15,5 %: heistä 220 eli 17,4 % kuului myös johtoryhmään. Esimiehistä 73 eli 5,8 % työskenteli tietohallinnossa ja 26 eli 2,1 % tietoturvan parissa. Johtoryhmään kuuluvia oli 487 eli 6,0 % kaikista vastanneista. Heistä esimiehinä toimii 220 eli 45,2 % vastanneista. Tietohallinnassa työskentelee 25 eli 5,1 % ja tietoturvan parissa 20 eli 4,1 % vastanneista. Vastanneista tietohallinnossa työskentelee 505 eli 6,2 % kaikista vastanneista. Heistä 73 eli 14,5 % toimii myös esimiehinä, ja johtoryhmässä toimii 25 eli 5,0 %. Kaikista vastanneista 159 eli 2,0 % työskentelee tietoturvan parissa. Heistä 26 eli 16,4 % vastanneista toimi myös esimies tehtävissä ja 20 eli 12,6 % johtoryhmässä.

Toimenkuva	Kaikki (8123)	%	Esimiehet (1261)	%	Johtoryhmä (487)	%	Tieto-hallinto (505)	%	Tieto-turva (159)	%
Esimies	1261	15,5 %	1261		220	45,2 %	73	14,5 %	26	16,4 %
Johtoryh-män jäsen	487	6,0 %	220	17,4 %	487		25	5,0 %	20	12,6 %
Hallinto	1585	19,5 %	353	28,0 %	201	41,3 %	0			
Tietohallin-to	505	6,2 %	73	5,8 %	25	5,1 %	505			
Tietoturva	159	2,0 %	26	2,1 %	20	4,1 %			159	
Tutkimus	282	3,5 %	26	2,1 %	6	1,2 %				
Opetus	1000	12,3 %	163	12,9 %	56	11,5 %				
Sosiaali- ja terveystoimi	1714	21,1 %	244	19,3 %	62	12,7 %				
Muu	2878	35,4 %	376	29,8 %	117	24,0 %				

Taulukko 1. Vastaajien taustatiedot.

3.1 Arki ja tietoturva

Vastaajilta selvitettiin, mitä laitteita he käyttävät työtehtäviensä suorittamiseen. Vastaajat pystyivät valitsemaan useamman kuin yhden vastaus vaihtoehdon. Kaikista laitteista työnantajan kannettava ja älypuhelin ovat kaikkein suosituimmat työvälineet. Eniten työnantajan kannettavaa hyödynsivät tietohallinnossa työskentelevät. Työnantajan älypuhelimen käytössä ei ollut suuria eroa verrattavien ryhmien välillä, kuitenkin niissä on huomattava ero kaikkien vastanneiden työnantajan älypuhelimen käyttöön. Muihin vastaajiin verrattaessa tietoturvan parissa työskentelevät käyttivät kaikista vähiten henkilökohtaisia laitteita. Osa vastaajista käytti jotain muuta laitetta työtehtävissä, kuten DECT-puhelinta, VOIP-puhelinta, palvelinkoneita ja TUVE-tietokonetta.

Laitteet	Kaikki (8123)	%	Esimiehet (1261)	%	Johtoryhmä (487)	%	Tietohallinto (505)	%	Tietoturva (159)	%
Työnantajan kannettava	5526	68,0 %	957	75,9 %	415	85,2 %	479	94,9 %	142	89,3 %
Työnantajan pöytätietokone	4301	52,9 %	610	48,4 %	165	33,9 %	138	27,3 %	46	28,9 %
Työnantajan tabletti	973	12,0 %	207	16,4 %	106	21,8 %	68	13,5 %	12	7,5 %
Työnantajan älypuhelin	5114	63,0 %	1011	80,2 %	392	80,5 %	423	83,8 %	133	83,6 %
Työantajan ajoneuvotietokoneella	53	0,7 %	18	1,4 %	3	0,6 %	6	1,2 %	2	1,3 %
Oma kannettava tietokone	564	6,9 %	77	6,1 %	33	6,8 %	31	6,1 %	6	3,8 %
Oma pöytätietokone	381	4,7 %	55	4,4 %	22	4,5 %	24	4,8 %	3	1,9 %
Oma tabletti	334	4,1 %	68	5,4 %	34	7,0 %	14	2,8 %	2	1,3 %
Oma älypuhelin	860	10,6 %	119	9,4 %	43	8,8 %	41	8,1 %	4	2,5 %
Jollain muulla laitteella	126	1,6 %	5	0,4 %	2	0,4 %	3	0,6 %	3	1,9 %

Taulukko 2. Vastaajien työtehtävissä käyttämät päätelaitteet.

Seuraavaksi vastaajilta kysyttiin, kuinka turvalliseksi he kokivat päivittäisen turvallisuuden työskentelyssä. Lähes kaikki vastaajista koki työskentelyn vähintään turvalliseksi niin kaikkien vastanneiden kesken kuin eritellyissä vastauksissa. Vain 17,0 % tietoturvan parissa työskentelevistä koki työskentelyn hyvin turvalliseksi, kun tietohallinnon työntekijöistä työskentelyn hyvin turvalliseksi koki 30,3 % vastanneista.

Muita merkittäviä eroa vastauksista löytyy työskentelyn jonkin verran turvalliseksi kokemisesta. Tietoturvan parissa käyskentelevistä 14,5 % koki työskentelyn jonkin verran turvattomaksi, kun johtoryhmän vastaajista vain 5,5 % koki asian näin. Tietoturvan vastanneista 3,1 % koki työskentelyn hyvin turvattomaksi. Esimiesten ja tietohallinnon työntekijöistä vain 2,0 % koki näin, ja yksikään johtoryhmän jäsenistä ei kokenut työskentelyä hyvin turvattomaksi.

Kaikkien vastanneiden kesken 1,1 % ei ollut miettinyt asiaa. Eritellyistä vastauksista esimiehistä 0,5 % ja johtoryhmän jäsenistä 0,4 % vastaajista ei ollut miettinyt asiaa ollenkaan. Tietohallinnon ja tietoturvallisuuden parissa työskentelevistä kaikki vastanneet olivat miettineet asiaa.

Koettu turvallisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Hyvin turvalliseksi	2040	25,1 %	319	25,3 %	133	27,3 %	153	30,3 %	27	17,0 %
Turvalliseksi	5430	66,8 %	868	68,8 %	325	66,7 %	328	65,0 %	104	65,4 %
Jonkin verran turvattomaksi	531	6,5 %	66	5,2 %	27	5,5 %	23	4,6 %	23	14,5 %
Hyvin turvattomaksi	29	0,4 %	2	0,2 %	0	0,0 %	1	0,2 %	5	3,1 %
En ole miettinyt asiaa	93	1,1 %	6	0,5 %	2	0,4 %	0	0,0 %	0	0,0 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Taulukko 3. Päivittäisen työskentelyn koettu turvallisuus.

3.2 Ohjeistus ja koulutus

Vastaajilta kysyttiin saavatko he tarpeeksi ohjeistusta ja koulutusta työssään. Ohjeistuksessa tarkennettiin, että kysymys koskee vain nykyistä työnantajaa. Esimiehistä 59,9 %, johtoryhmän jäsenistä 61,8 %, tietohallinnon vastaajista 65,5 % ja tietoturvallisuuden vastaajista 66,0 % sai ohjeistusta työsuhteen alkaessa. Esimiehistä 29,2 %, johtoryhmän jäsenistä 29,4 %, tietohallinnon vastaajista 35,8 % ja tietoturvan vastaajista 51,6 % sai koulutusta tietoturvallisuudesta työsuhteen alkaessa (liite 1).

Ohjeistus	Kaikki (8123)	%	Esimiehet (1261)	%	Johtoryhmä (487)	%	Tietohallinto (505)	%	Tietoturva (159)	%
Olen	4731	58,2 %	718	56,9 %	301	61,8 %	331	65,5 %	105	66,0 %
En	1905	23,5 %	305	24,2 %	102	20,9 %	94	18,6 %	23	14,5 %
En tarvitse	84	1,0 %	14	1,1 %	7	1,4 %	14	2,8 %	5	3,1 %

Taulukko 4. Tietoturvaperehdytys ohjeistusta työsuhteen alkaessa.

Esimiehistä 67,7 %, johtoryhmän jäsenistä 69,6 %, tietohallinnon vastaajista 73,5 % ja tietoturvan vastaajista 72,3 % sai ohjeistusta turvalliseen toimintaan organisaation toimitiloissa (liite 2). Esimiehistä 35,1 %, johtoryhmän jäsenistä 35,5 %, tietohallinnon vastaajista 36,0 % ja tietoturvan vastaajista 57,9 % vastaajista sai koulutusta turvalliseen toimintaan toimitiloissa (liite 3). Tietoturvan vastaajista 65,4 %, tietohallinnon vastaajista 73,7 %, johtoryhmän jäsenistä 63,0 % ja esimiehistä 55,5 % sai ohjeistusta etätyöskentelyyn tai työskentelyyn toimipaikan ulkopuolella (liite 4). Tietoturvan vastaajista 27,7 %, tietohallinnon vastaajista 20,0 %,

johtoryhmän jäsenistä 18,7 % ja esimiehistä 16,5 % sai koulutusta etätyöskentelyyn ja työskentelyyn toimipaikan ulkopuolella (liite 5).

Esimiehistä 44,4 %, johtoryhmän jäsenistä 46,4 %, tietohallinnosta 52,9 %, tietoturvasta 59,7 % sai ohjeistusta tietojen luokitteluun (liite 6). Esimiehistä 21,2 %, johtoryhmän jäsenistä 26,3 %, tietohallinnosta 28,3 % ja tietoturvasta 46,5 % sai koulutusta tietojen luokittelusta (liite 7). Esimiehistä 71,8 %, johtoryhmän jäsenistä 72,5 %, tietohallinnosta 66,5 %, tietoturvasta 63,5 % sai ohjeistusta henkilötietojen käsittelyyn ja tietosuojaan. (liite 8). Esimiehistä 41,5 %, johtoryhmän jäsenistä 40,5 %, tietohallinnosta 36,0 % ja tietoturvasta 41,5 % sai koulutusta henkilötietojen käsittelyyn ja tietosuojaan.

Koulutus	Kaikki (8123)	%	Esimiehet (1261)	%	Johtoryhmä (487)	%	Tietohallinto (505)	%	Tietoturva (159)	%
Olen	2802	34,5 %	523	41,5 %	197	40,5 %	182	36,0 %	66	41,5 %
En	1422	17,5 %	215	17,0 %	77	15,8 %	106	21,0 %	34	21,4 %
En tarvitse	251	3,1 %	11	0,9 %	10	2,1 %	24	4,8 %	6	3,8 %

Taulukko 5. Koulutus henkilötietojen käsittelyyn ja tietosuojaan.

Esimiehistä 69,2 % ja johtoryhmän jäsenistä 71,5 % sai ohjeistusta salassa pidettävän tietoaineiston käsittelyyn (liite 9). Esimiehistä 38,6 % ja johtoryhmän jäsenistä 38,4 % sai koulutusta salassa pidettävän tietoaineiston käsittelyyn (liite 10). Ohjeistusta ei saanut 10,2 % esimiehistä ja 7,8 % johtoryhmän jäsenistä. Koulutusta ei ole saanut 18,5 % esimiehistä ja 16,4 % johtoryhmän jäsenistä. Tietohallinnon vastaajista 50,5 % ja tietoturvan vastaajista 58,5 % sai ohjeistusta tietojen salaamiseen (liite 11). Tietohallinnosta 18,6 % ja tietoturvasta 26,4 % sai koulutusta tietojen salaamiseen. Tietohallinnosta 35,5 % ja 22,6 % ei ole saanut ohjeistusta. Tietohallinnosta 28,9 % ja tietoturvasta 32,1 % ei ole saanut koulutusta (liite 12).

Esimiehistä 55,4 %, johtoryhmän jäsenistä 61,0 %, tietohallinnosto 67,7 % ja tietoturvasta 64,2 % sai ohjeistusta mobiililaitteiden käyttöön (liite 13). Esimiehistä 15,3 %, johtoryhmästä 16,2 %, tietohallinnosta 17,4 % ja tietoturvasta 27,0 % sai koulutusta mobiililaitteiden käyttöön (liite 14). Esimiehistä 74,2 %, johtoryhmän jäsenistä 73,9 %, tietohallinnosta 73,7 % ja tietoturvasta 71,1 % sai ohjeistusta sähköpostin käyttöön (liite 15). Esimiehistä 29,7 %, johtoryhmän jäsenistä 28,7 %, tietohallinnosta 26,5 % ja tietoturvasta 36,5 % sai koulutusta sähköpostin käyttöön (liite 16).

Tietohallinnosta 67,1 % ja tietoturvasta 62,3 % sai ohjeistusta internetin käyttöön. Tietohallinnosta 18,8 % ja 27,0 % sai ohjeistusta. Tietohallinnosta 18,2 % ja tietoturvasta 19,5 % ei ole saanut ohjeistusta internetin käyttöön (17). Tietohallinnosta 26,3 % ja tietoturvasta 28,3 % ei ole saanut koulutusta (liite 18).

Esimiehistä 61,5 %, johtoryhmän jäsenistä 62,6 %, tietohallinnosta 54,5 % ja tietoturvasta 66,0 % sai ohjeistusta sosiaalisen median käyttöön (liite 19). Esimiehistä 19,5 %, johtoryhmän jäsenistä 23,4 %, tietohallinnosta 16,2 % ja tietoturvasta 27,0 % sai koulutusta sosiaalisen median käyttöön (liite 20). Esimiehistä 69,2 % ja johtoryhmän jäsenistä 70,4 % sai ohjeistusta salasanojen hallintaan (liite 21). Esimiehistä 24,5 % ja johtoryhmän jäsenistä 23,0 % sai koulutusta salasanojen hallintaan (liite 22).

Tietohallinnosta 62,4 %, tietoturvasta 54,7 %, esimiehistä 52,5 % ja johtoryhmän jäsenistä 56,7 % sai ohjeistusta häiriötilanteissa toimimiseen (liite 23). Tietohallinnasta 21,6 % ja tietoturvasta 28,9 %, esimiehistä 14,5 % ja johtoryhmän jäsenistä 14,2 % sai koulutusta häiriötilanteissa toimimiseen (liite 24). Esimiehistä 65,2 % ja johtoryhmän jäsenistä 67,6 % sai ohjeistusta tietoturvapoikkeamissa toimimiseen (liite 25). Esimiehistä 17,0 % ja johtoryhmän jäsenistä 17,7 % sai koulutusta tietoturvapoikkeamissa toimimiseen (liite 26). Tietohallinnosta 74,5 % ja tietoturvasta 70,4 % sai ohjeistusta yleisestä tiedosta tietoturvallisuudesta (liite 27). Tietohallinnosta 42,4 % ja tietoturvasta 57,9 % sai koulutusta yleisestä tiedosta tietoturvallisuudesta (liite 28).

Lisä kysymyksenä kysyttiin, kokivatko vastaajat tarvetta lisäohjeistukselle ja lisäkoulutukselle. Kysymys ei ollut pakollinen, joten prosentit on laskettu vastausten määrän mukaan (liite 29). Vastaajilta kysyttiin vielä tarkennusta siihen, mistä aiheista he haluaisivat lisäohjeista ja lisäkoulutusta (liite 30). Prosenttien laskemiseen käytettiin edellisen kysymykset ”kyllä” vastausmääriä. Kaikkein eniten lisäohjeistusta ja lisäkoulutusta toivottiin tietojen salaamiseen. Esimiehistä 64,0 %, johtoryhmän jäsenistä 58,3 % ja tietoturvan parissa työskentelevistä 55,2 % vastanneista toivoi sitä. Tietohallinnon työntekijät halusivat eniten lisäohjeistusta ja lisäkoulutusta tietojen luokittelusta (53,6 %) ja salassa pidettävän tietoaineiston käsittelystä (53,6 %). Vähiten lisäohjeistusta ja lisäkoulutusta haluttiin internetin käyttöön. Esimiehistä 15,9 %, tietohallinnon työntekijöistä 8,7 % ja tietoturvan parissa työskentelevistä 13,8 % toivoi sitä. Johtoryhmän jäsenet toivoivat vähiten lisäohjeistus ja lisäkoulutusta sähköpostin käyttöön (10.6 %).

3.3 Kirjautumistavat

Vastaajilta kysyttiin, mikä on heidän ensisijainen tunnistautumistapa työasemaan. Koska selvitettiin ensisijaista tunnistautumistapaa, vastaajat pystyivät valitsemaan vain yhden vaihtoehdon. Eniten virkakorttiin perustuvia kirjautumia käyttivät tietohallinnossa (26,7 %) ja tietoturvan (35,2 %) parissa työskentelevät. Kuitenkin käyttäjätunnus ja salasana ovat tunnistautumistavoista kaikkein käytetyimmät. Kaikista vastanneista käyttäjätunnusta ja salasanaa käytti 82,3 %, esimiehistä 81,8 %, johtoryhmän jäsenistä 79,5 %, tietohallinnon vastaajista 71,7 % ja tietoturvan vastaajista 64,2 %.

Vaikka biometrinen tunnistautuminen ei olekaan vielä kovin yleistä, kaikista vastanneista vain kuusi henkilöä kertoi käyttävänsä sitä, haluttiin sitä kuitenkin kysyä, jotta pystyttäisiin seuraamaan, milloin niiden käyttö alkaa yleistyä. Esimiehistä 3 henkilöä vastasi käyttävänsä biometristä tunnistautumista.

Tunnistautuminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Virkakorttiin perustuvaa kirjautumista	1394	17,2 %	225	17,8 %	94	19,3 %	135	26,7 %	56	35,2 %
Käyttäjätunnusta ja salasanaa	6688	82,3 %	1031	81,8 %	387	79,5 %	362	71,7 %	102	64,2 %
Biometristä tunnistusta (esimerkiksi sormenjälki tai kasvot)	6	0,1 %	3	0,2 %	1	0,2 %	1	0,2 %	0	0,0 %
Jotain muuta	35	0,4 %	2	0,2 %	5	1,0 %	7	1,4 %	1	0,6 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Taulukko 6. Vastaajien ensisijainen tunnistautumistapa työasemaan.

Vastaajat, jotka kertoivat käyttävänsä jotain muuta tunnistautumismenetelmää kuten Bitlocker salasanaa ja sen jälkeen Windows tunnistautuminen käyttäjätunnuksella ja salasanalla, PIN-koodia, Pulse Securea ja tekstiviestiautentikointia, Virtual Smart Cardia.Osa vastaajista kertoi, ettei käytä tunnistautumisjärjestelmää olleenkaan.

Seuraavaksi kysyttiin vastaajien tunnistautumistapaa työtehtäviin liittyvissä palveluissa. Vaihtoehdoista pystyi valitsemaan useamman kuin van yhden. Tämän takia prosenttiluvut on laskettu kysymyksenvastaaja määrien mukaan. Tietohallinnon työntekijöistä 47,3 % käyttää kertakirjautumispalvelua tunnistautumiseen työtehtäviin liittyvissä palveluissa, kun esimiehistä 22,6 % käyttää sitä.

Virkakortilla kirjautumista johtoryhmän jäsenistä käyttää 22,0 %, tietoturvan parissa työskentelevistä 47,2 % käyttää sitä kirjautumiseen. Esimiehistä 75,5 % ja tietohallinnon vastaajista 73,5 % käyttää käyttäjätunnusta ja salasanaa tunnistautumiseen. Johtoryhmästä 69,6 % ja tietoturvan parissa työskentelevistä 64,2 % vastaajista käyttää niitä (liite 31).

Vastaajilta kysyttiin salasanojen käyttöä työtehtäviin liittyvissä palveluissa. Vastaajat pystyivät valitsemaan vain yhden vaihtoehdon. Pääasiassa samaa salasanaa tietohallinnon vastaajista käytti 5,9 %, tietoturvan vastaajista samaa salasanaa käyttää 3,1 % kun kaikista vastaajista 7,6 % vastaajista käyttää pääasiassa samaa salasanaa. Muutamaa eri salasanaa käyttää johtoryhmän jäsenistä 35,5 % vastaajista, tietoturvan vastaajista 19,5 % käyttää muutamaa eri salasanaa. Tietoturvan vastaajista 39,0 % ja johtoryhmän jäsenistä 18,9 % käyttää eri salasanaa työtehtäviin liittyvissä palveluissa. Kyselyssä haluttiin kysyä myös salasanojen hallintaohjelmien käyttämisestä, jotta niiden yleistymistä voitaisiin seurata. Vastanneista esimiehistä 1,7 % ja johtoryhmän 2,7 % ilmoitti käyttävänsä salasanojen hallintaohjelmaa. Tietohallinnon

vastanneista 4,2 % ja tietoturvan parissa työskentelevistä 4,4 % ilmoitti käyttävänsä salasanojen hallinta ohjelmaa (liite 32).

3.4 Koettu huolestuneisuus

Kyselyssä haluttiin selvittää, mitkä asiat huolestuttavat organisaatioissa. Kysymykset eivät olleet pakollisia, joten kaikki vastaajat eivät ole vastanneet tähän kysymykseen. Prosenttiluvut on laskettu kysymyksen vastaaja määrän mukaan. Esimiehistä 50,2 % ja johtoryhmän jäsenistä 57,1 % ei ole huolestunut siitä, riittääkö johdon tuki turvallisuudelle. Esimiehistä 0,8 % ja johtoryhmän jäsenistä 0,4 % vastasi uhan jo tapahtuneen jo. Tietohallinnon vastaajista 48,5 % ja 39,1 % tietoturvan vastaajista ei ole huolestunut riittämättömästä johdon tuesta turvallisuudelle. Tietohallinnon vastaajista 4,8 % ja tietoturvan vastaajista 11,5 % on erittäin paljon huolestunut riittämättömästä johdon tuesta turvallisuuteen (liite 33).

Esimiehistä 46,2 % ja johtoryhmän jäsenistä 50,8 % ei ollut huolestunut johdon riittämättömästä tuesta tietoturvallisuudelle. Uhkan ilmoitti toteutuneeksi 0,5 % esimiehistä ja 0,0 % johtoryhmään kuuluvista. Tietohallinnon vastaajista 38,8 % ja tietoturvan vastaajista 36,8 % ei ole huolissaan riittämättömästä johdon tuesta tietoturvallisuudelle. Tietohallinnon vastaajista 7,9 % ja tietoturvallisuuden vastaajista 12,3 % on erittäin paljon huolestunut riittämättömästä johdon tuesta tietoturvallisuudelle. Riittämätön johdon tuki tietoturvallisuudelle huolestutti tietoturvan parissa työskenteleviä kaikkein eniten.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	4041	51,7 %	567	46,2 %	242	50,8 %	192	38,8 %	57	36,8 %
Vähän	2947	37,7 %	511	41,6 %	189	39,7 %	188	38,0 %	58	37,4 %
Paljon	526	6,7 %	108	8,8 %	33	6,9 %	69	13,9 %	15	9,7 %
Erittäin paljon	269	3,4 %	35	2,9 %	12	2,5 %	39	7,9 %	19	12,3 %
Uhka toteutunut	32	0,4 %	6	0,5 %	0	0,0 %	7	1,4 %	6	3,9 %
Yhteensä	7815	100,0 %	1227	100,0 %	476	100,0 %	495	100,0 %	155	100,0 %

Taulukko 7. Riittämätön johdon tuki tietoturvallisuudelle.

Esimiehistä 47,5 % ja johtoryhmän jäsenistä 50,1 % ei ollut huolestunut johdon riittämättömästä tuesta tietosuojalle. 0,6 % esimiehistä ja 0,0 % johtoryhmän jäsenistä koki uhkan toteutuneen. Tietohallinnon vastaajista 38,5 ja tietoturvan vastaajista 38,7 % on paljon huolestunut riittämättömästä johdon tuesta tietosuojalle. Tietohallinnon vastaajista 12,6 % ja 12,3 tietoturvallisuuden vastaajista on paljon huolestunut riittämättömästä johdon tuesta tietosuojalle. Riittämätön johdon tuki tietosuojalle huolestutti tietohallinnon vastaajia kaikista eniten.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	4050	52,0 %	581	47,5 %	237	50,1 %	196	39,8 %	52	33,5 %
Vähän	2905	37,3 %	497	40,6 %	188	39,7 %	190	38,5 %	60	38,7 %
Paljon	548	7,0 %	104	8,5 %	39	8,2 %	62	12,6 %	19	12,3 %
Erittäin paljon	254	3,3 %	35	2,9 %	9	1,9 %	41	8,3 %	18	11,6 %
Uhka toteutunut	36	0,5 %	7	0,6 %	0	0,0 %	4	0,8 %	6	3,9 %
Yhteensä	7793	100,0 %	1224	100,0 %	473	100,0 %	493	100,0 %	155	100,0 %

Taulukko 8. Riittämätön johdon tuki tietosuojalle.

Esimiehistä 38,8 %, johtoryhmän jäsenistä 40,4 %, 52,2 % tietohallinnon ja 53,9 % tietoturvan vastaajista ei ole huolestunut riittämättömästä koulutuksen määrästä tietoturvallisuudesta. Erittäin huolestunut tietoturvallisuuden riittämättömästä koulutuksesta on esimiehistä 2,7 %, johtoryhmän jäsenistä 2,3 %, tietotohallinnon vastaajista 2,8 % ja tietoturvan vastaajista 6,5 % (liite 34). Esimiehistä 45,1 %, johtoryhmän jäsenistä 42,6 %, tietohallinnosta 53,5 % ja tietoturvasta 39,5 % on vähän huolissaan, että toimipaikan tilaturvallisuus ei ole riittävällä tasolla. Esimiehistä 10,3 %, johtoryhmän jäsenistä 9,4 %, tietohallinnosta 7,8 % ja tietoturvasta 10,2 % on paljon huolissaan tilaturvallisuuden tasosta (liite 35).

Esimiehistä 46,6 %, johtoryhmän jäsenistä 48,2 %, tietohallinnosta 40,2 % ja tietoturvasta 42,3 % on vähän huolissaan, että organisaation tietoturvallisuus ei ole riittävällä tasolla. Esimiehistä 9,4 %, johtoryhmän jäsenistä 9,6 %, tietohallinnosta 12,8 % ja tietoturvasta 17,3 % on paljon huolissaan, että organisaation tietoturvallisuus ei ole riittävällä tasolla (liite 36). Esimiehistä 9,0 %, johtoryhmän jäsenistä 7,5 %, tietohallinnosta 8,0 % ja tietoturvallisuudesta 12,3 % huolettaa paljon, että työpaikalle iskee varas, joka vie sieltä laitteita tai salassa pidettäviä tietoja. Esimiehistä 2,3 %, johtoryhmän jäsenistä 2,5 %, tietohallinnosta 2,2 % ja tietoturvasta 4,5 % on erittäin paljon huolissaan, että työpaikalle iskee varas (liite 37).

Esimiehistä 68,9 %, johtoryhmän jäsenistä 67,9 %, tietohallinnosta 71,3 % ja tietoturvasta 67,5 % ei ole huolissään, että toimipisteessä ei käytetä kuvallisia henkilökortteja (liite 38). Tietoturvasta 21,9 %, tietohallinnosta 32,3 %, johtoryhmästä 38,5 % ja esimiehistä 35,4 % on vähän huolissaan, että työtehtävään liittyvä käyttäjätunnus ja salasana varastetaan (liite 39). Esimiehistä 34,3 %, johtoryhmän jäsenistä 40,0 %, tietohallinnosta 34,2 % ja tietoturvasta 44,9 % on vähän huolissaan, että heiltä yritetään urkkia tai vakoilla työtehtäviin liittyviä tietoja (liite 40).

Esimiehistä 71,7 % ja johtoryhmän jäsenistä 68,3 % ei ole huolestunut, että heidän yritetään painostaa tai heidän mielipiteisiin vaikuttaa työtehtäviin liittyen. Esimiehistä 22,2 % ja johtoryhmästä 25,4 % on vähän huolissaan (liite 41). Esimiehistä 52,3 %, johtoryhmän jäsenistä 55,9 %, tietohallinnosta 45,3 % ja tietoturvasta 54,2 % on vähän huolissaan siitä, että heidän identiteetti varastetaan ja sitä hyödynnetään väärinkäytöksiin (liite 42). Tietohallinnosta 79,4 % ja

tietoturvasta 67,3 % ei ole huolissaan, että heitä uhkaillaan nettipalveluissa. Tietohallinnosta 16,8 % ja tietoturvasta 28,1 % on vähän huolissaan. Tämä huolestutti tietohallinnon vastaajia kaikista vähiten (liite 43).

Esimiehistä 25,5 % ja johtoryhmän jäsenistä 32,6 % on vähän huolissaan, että organisaatio menettää rahaa nettihuijausten takia. Esimiehistä 3,7 % ja johtoryhmästä 2,3 % on paljon huolissaan (liite 44). Tietohallinnossa 23,6 % ja tietoturvasta 41,4 % on vähän huolissaan, että organisaatiolta käyttöön saatua luottokorttia käytetään väärin. Tietohallinnosta 3,7 % ja tietoturvasta 4,6 % on paljon huolissaan (liite 45). Esimiehistä 48,3 %, johtoryhmän jäsenistä 50,4 %, tietohallinnosta 53,5 % ja tietoturvasta 52,9 % on vähän huolissaan, että heidän päätelaitteensa varastetaan (liite 46).

Tietohallinnosta 56,0 % ja tietoturvasta 35,7 % ei ole huolissan, että päätelaitteella olevia salassa pidettäviä tietoja vuotaa ulkopuolisille. Tietohallinnosta 5,3 % ja tietoturvasta 11,7 % on paljon huolissaan (liite 47). Esimiehistä 60,4 %, johtoryhmästä 61,10 %, tietohallinnosta 58,3 % ja tietoturvasta 51,0 % on vähän huolissaan, että heidän päätelaitteeseensa iskee haittaohjelma (liite 48). Esimiehistä 2,6 %, johtoryhmän jäsenistä 2,5 %, tietohallinnosta 2,6 % ja tietoturvasta 6,5 % on erittäin paljon huolissaan, että päätelaitteen tietoturvapäivitykset eivät ole ajan tasalla (liite 49). Esimiehistä 20,1 %, johtoryhmästä 21,4 %, tietohallinnosta 11,8 % ja tietoturvasta 15,5 % on paljon huolissaan, että he menettävät tärkeitä tietoja laiterikon takia. Tämä huolestutti esimiehiä ja johtoryhmän jäseniä kaikista eniten.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	2700	34,3 %	313	25,4 %	121	25,2 %	208	41,8 %	50	32,3 %
Vähän	3370	42,8 %	561	45,5 %	214	44,5 %	200	40,2 %	67	43,2 %
Paljon	1279	16,2 %	248	20,1 %	103	21,4 %	59	11,8 %	24	15,5 %
Erittäin paljon	458	5,8 %	97	7,9 %	38	7,9 %	28	5,6 %	9	5,8 %
Uhka toteutunut	64	0,8 %	14	1,1 %	5	1,0 %	3	0,6 %	5	3,2 %
Yhteensä	7871	100,0 %	1233	100,0 %	481	100,0 %	498	100,0 %	155	100,0 %

Taulukko 9. Menetän tärkeitä tietoja laiterikon takia.

Esimiehistä 65,5 %, johtoryhmästä 67,9 %, tietohallinnosta 60,3 % ja tietoturvasta 59,2 % ei ole huolissaan, että he saavat vahingossa tietoonsa salassa pidettäviä tietoja, joihin heillä ei ole oikeutta (liite 50). Esimiehistä 66,3 %, johtoryhmän jäsenistä 70,1 %, tietohallinnosta 61,8 % ja tietoturvasta 62,6 % ei ole huolissaan, että eivät tiedä, miten henkilötietoja tulee käsitellä heidän työtehtävissä (51). Esimiehistä 27,6 %, johtoryhmän jäsenistä 24,8 %, tietohallinnosta 33,5 % ja tietoturvasta 24,7 % on vähän huolissaan, että eivät tiedä, mitkä heidän työtehtäviin liittyvät asiat ovat salassa pidettäviä (liite 52).

Esimiehistä 3,1 %, johtoryhmän jäsenistä 3,0 %, tietohallinnosta 5,1 % ja tietoturvasta 4,5 % vastanneista oli paljon huolissan, että eivät osaa käsitellä salassa pidettäviä tietoja oikeilla työvälineillä (liite 53). Esimiehistä 64,1 % ja johtoryhmästä 61,7 % ei ole huolissaan, että joutuu kuljettamaan salassa pidettäviä tietoja työpaikan ulkopuolella. Esimiehistä 30,8 % ja johtoryhmän jäsenistä 33,6 % on vähän huolissaan (liite 54). Esimiehistä 30,8 %, johtoryhmän jäsenistä 33,8 %, tietohallinnosta 22,4 % ja tietoturvasta 36,4 % ovat vähän huolissaan, että etätyöskentely ei ole turvallista työpaikan ulkopuolella (liite 55). Tietohallinnosta 61,1 % ja tietoturvasta 58,7 % ei ole huolissaan, että ei saa toimia häiriötilanteissa. Tietohallinnosta 1,2 % ja tietoturvasta 3,2 % on erittäin paljon huolissaan (liite 56).

Esimiehistä 5,4 %, johtoryhmästä 5,5 %, tietohallinnosta 4,5 % ja tietoturvasta 6,5 % on paljon huolissaan, että eivät tiedä, mitkä heidän vastuunsa ovat tietoturvallisuuden osalta. Tämä huolestutti tietoturvan parissa työskenteleviä kaikista vähiten (liite 57). Esimiehistä 47,3 %, johtoryhmän jäsenistä 47,6 %, tietohallinnosta 41,9 % ja tietoturvasta 42,0 % on vähän huolissaan, että heille tärkeä palvelu ei ole toiminnassa, silloin kun he sitä tarvitsevat. Kaikissa ryhmissä tämä uhka on toteutunut eniten (liite 58). Esimiehistä 76,8 %, johtoryhmän jäsenistä 78,4 %, tietohallinnosta 71,4 % ja tietoturvasta 60,8 % ei ole huolissaan, että heidän työtehtävänsä edellyttävät tietoturvaohjeistuksen vastaista toimintaa. Tämä huolestutti esimiehiä ja johtoryhmän jäseniä kaikista vähiten (liite 59). Esimiehistä 54,4 %, johtoryhmän jäsenistä 54,5 %, tietohallinnosta 48,2 % ja tietoturvasta 51,0 % on vähän huolissaan, että selaimesta tai muusta ohjelmistosta aiheutuu tietoturvauhka (liite 60).

3.5 Tietoaineistojen luokittelu

Kyselyssä selvitettiin, onko organisaatiossa ohjeistusta salassa pidettävien tietojen luokitteluun. Suurimmassa osassa organisaatoissa on ohjeistus tietoaineistojen luokitteluun. Tietoturvan parissa työskentelevistä 76,7 % vastasi, että organisaatiossa on ohjeistus. Kun taas heistä 5,0 % vastasi, että ei ole. Tietoturvan parissa työskentelevistä 11,9 %, vastasi että ei tiedä. Esimiehistä 52,3 % vastasi, että organisaatiolla on ohjeistus tietojen luokitteluun. Heistä 9,1 % vastasi, että ei ole. Esimiehistä 33,4 % vastasi, että ei tiedä, onko organisaatiossa ohjeistusta salassa pidettävien tietojen luokitteluun (liite 61).

Jatkokysymyksenä vastaajilta kysyttiin, osaavatko he käyttää organisaation luomia ohjeita. Tietoturvan parissa työskentelevistä 54,0 % kokee osaavan käyttää organisaation ohjeita hyvin ja 21,8 % erittäin hyvin. Johtoryhmän vastaajista 43,6 % vastasi osaavansa noudattaa ohjeita hyvin ja 36,2 % tyydyttävästi. Esimiehistä 42,7 % osaa käyttää ohjeita hyvin ja 35,3 % tyydyttävästi (liite 62). Organisaatioilta kysyttiin tietävätkö he, miten eri palveluja ja työkaluja käytetään salassa pidettävien tietojen käsittelyssä, esimerkiksi mitä salassa pidettäviä tietoja saa lähettää ja mihin niitä saa tallentaa. Esimiehistä 67,4 % vastasi tietävänsä, miten palveluja ja työkaluja käytetään ja 22,8 % vastasi että ei osaa. Johtoryhmän jäsenistä 69,8 % vastasi

osaavansa käyttää ja 19,9 % vastasi, että ei osaa käyttää palveluja ja työkaluja salassa pidettävien tietojen käsittelyssä (liite 63).

Jatkokysymyksenä kysyttiin, osaavatko vastaajat käyttää näitä palveluja ja työkaluja salassa pidettävän tiedon käsittelyssä. Tietoturvan parissa työskentelevistä 30,5 % vastasi osaavansa erittäin hyvin ja 51,5 % vastasi osaavansa käyttää erilaisia palveluja ja työkaluja hyvin. Tietohallinnon vastaajista 16,6 % vastasi osaavansa käyttää palveluja ja työkaluja erittäin hyvin ja 57,2 % vastasi osaavansa käyttää näitä hyvin. Kaikista vastanneista 0,3 % vastasi, että osaa käyttää eri palveluja ja työkaluja erittäin huonosti ja 2,4 % vastasi osaavansa käyttää niitä huonosti (liite 64).

3.6 Henkilötietojen käsittely

Kyselyssä kysyttiin, kuinka usein vastaajat käsittelevät henkilötietoja. Esimiesten vastaajista 47,7 % vastasi käsittelevänsä henkilötietoja päivittäin, 7,5 % vastasi käsittelevänsä henkilötietoja harvemmin kuin kuukausittain ja 2,4 % vastasi, että ei käsittele henkilötietoja. Tietoturvan parissa työskentelevistä 17.0 % vastasi käsittelevänsä henkilötietoja useamman kerran viikossa ja 5,7 % vastasi käsittelevänsä henkilötietoja kerran viikossa. Tietohallinnon vastaajista 18,4 % vastasi, että ei käsittele henkilötietoja ollenkaan (liite 65).

Kyselyssä haluttiin myös selvittää, kokevatko vastaajat, että heidän organisaatiossaan käsitellään vain tarpeellisia henkilötietoja. Tietohallinnon vastaajista 53,3 % vastasi, että heidän organisaationsa käsittelee vain tarpeellisia henkilötietoja. 11,7 % vastaajista vastasi, että heidän organisaatiossa käsitellään muitakin kuin vain tarpeellisia henkilötietoja ja 27,5 % ei osannut sanoa. Esimiesten vastaajista 79,9 % vastasi, että heidän organisaatiossa käsitellään vain tarpeellisia henkilötietoja. Vastaajista 6,7 % koki, että organisaatiossa käsitellään muitakin kuin tarpeellisia henkilötietoja ja 11,9 % ei osannut sanoa (liite 66). Vastaajilta haluttiin selvittää, onko tietosuoja-asetukseen alettu valmistautumaan.

Esimiesten vastaajista 24,7 % vastasi, että organisaatiossa on ryhdytty toimenpiteisiin, 22,8 % ei ollut havainnut mitään ja 17,4 % ei ollut tietoisia mikä on tietosuoja-asetus. Johtoryhmän vastaajista 25,9 % vastasi, että organisaatiossa on ryhdytty toimenpiteisiin, 16,8 % ei ollut havainnut mitään ja 14,0 % ei tiennyt mikä tietosuoja-asetus on (liite 67). Lisäksi vastaajilta haluttiin kysyä, tiesivätkö he keneltä he voivat organisaatiossaan kysyä tietosuoja-asioista. Tietoturvan parissa työskentelevistä 22,0 % vastasi olevansa tämä henkilö. Suurin osa vastaajista tiesi keneltä he voivat kysyä asiasta esimiehistä 71,8 %, johtoryhmän jäsenistä 74,3 %, tietohallinnosta 72,1 % ja tietoturvasta 61,0 %.

Kysyminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen se henkilö	244	3,0 %	92	7,3 %	32	6,6 %	40	7,9 %	35	22,0 %
Tiedän keneltä kysyä	4768	58,7 %	906	71,8 %	362	74,3 %	364	72,1 %	97	61,0 %
En ole varma	2248	27,7 %	208	16,5 %	65	13,3 %	73	14,5 %	17	10,7 %
En tiedä keneltä kysyä	863	10,6 %	55	4,4 %	28	5,7 %	28	5,5 %	10	6,3 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Taulukko 10. Keneltä kysyä tietosuoja-asioista.

3.7 Työskentely toimipaikan ulkopuolella

Vastaajilta kysyttiin, salliiko heidän organisaationsa työskentelyn toimipaikan ulkopuolella. Lähes kaikkien vastaajien organisaatiot sallivat työskentelyn toimipaikan ulkopuolella. Esimiesten vastaajista 9,7 %, johtoryhmien vastaajista 93,4 %, tietohallinnon vastaajista 3,0 % ja tietoturvan vastaajista 91,2 % vastasi, että organisaatio ei salli työskentelyä toimipaikan ulkopuolella (liite 68). Seuraavaksi kysyttiin hyödyntävätkö, vastaajat mahdollisuutta työskennellä toimipaikan ulkopuolella. Vastaus ei ollut pakollinen, joten prosentit on laskettu vastanneiden määrän mukaan. Johtoryhmän jäsenistä 25,0 % ja tietoturvan vastaajista 14,4 % vastasi työskentelevänsä useana päivänä viikossa toimipaikan ulkopuolella. Eniten vastaajat, esimiehet 29,4 %, johtoryhmän jäsenet 29,4 %, tietohallinnosta 26,6 % ja tietoturvallisuudesta 34,9 %, vastasi työskentelevänsä työpaikan ulkopuolella epäsäännöllisesti, kuitenkin kuukausittain (liite 69).

Kyselyssä kysyttiin, onko työskentelyyn toimipaikan ulkopuolella ohjeistettu tarpeeksi. Esimiehistä 47,6 %, johtoryhmän jäsenistä 57,3 %, tietohallinnosta 65,9 % ja tietoturvasta 66,7 % vastasi saaneensa tarpeeksi ohjeistusta työskentelyyn toimipaikan ulkopuolella (liite 70). Vastaajilta kysyttiin, pystyvätkö he toimimaan saamiensa ohjeiden mukaisesti. Vastaus ei ollut pakollinen, joten prosentit on laskettu kysymykseen vastanneiden määrän mukaan. Suurin osa vastanneista vastasi pystyvänsä toimimaan erittäin hyvin, hyvin tai tyydyttävästi ohjeistuksen mukaisesti (liite 71).

3.8 Työsähköpostin lukeminen

Vastaajilta kysyttiin, kuinka usein he käyttävät työnantajan tarjoamaa laitetta organisaation sähköpostin lukemiseen ja kuinka usein he käyttävät henkilökohtaista laitetta. Kysymyksessä sai valita useamman kuin yhden vaihtoehdon, joten prosentit on laskettu vastaaja ryhmien kokonaismäärien mukaan. Esimiehistä (51,9 %), johtoryhmän jäsenistä (58,9 %) ja tietoturvallisuuden parissa työskentelevistä (50,3 %) lukee työnantajan laitteella organisaation sähköpostia päivittäin. Tietohallinnon vastaajista 36,0 % lukee työnantajan laitteella sähköpostia päivittäin, ja heistä 61,8 % lukee sähköpostia arkipäivisin (liite 72). Tietoturvan parissa työskentelevistä 83,6 %, tietohallinnosta 72,9 %, johtoryhmän jäsenistä 67,8 % ja esimiehistä 59,9 %

ei käytä henkilökohtaisia laitteita organisaation sähköpostin lukemiseen. Esimiehistä 64,6 % käyttää henkilökohtaista laitetta organisaation sähköpostin lukemiseen muutaman kerran vuodessa (liite 73).

3.9 Tietoturvallisuuden merkitys ja toteutuminen

Vastaajilta kysyttiin, millaisessa merkityksessä he näkevät tietoturvallisuuden omassa organisaatiossaan. Esimiehistä 59,9 %, johtoryhmän jäsenistä 60,8 %, tietohallinnosta 70,9 % ja tietoturvasta 71,1 % kokee tietoturvallisuuden lisäävän laatua ja luotettavuutta. Tietoturvallisuuden merkityksen organisaatiossa ymmärtää esimiehistä 5,9 %, johtoryhmän jäsenistä 4,7 %, tietohallinnosta 7,3 % ja tietoturvallisuuden 3,8 % vastaajista (liite 74).

Perustelut

> ”Edellytys sille, että viranomainen voi toimia tehtävänsä mukaisesti kaikissa olosuhteissa. Olennainen osa myös maineenhallintaa ja sitä kautta luotettavuutta ja uskottavuutta.”
>
> ”Jos ei ole tietoa, en voi tehdä työtäni. En voi työskennellä jatkuvasti samassa työpisteessäni ja silloinkin tiedon on oltava saatavilla.”
>
> ”Koska tämä ICT-keskittämisen virhe on jo tehty, on tietoturvallisuus pidettävä siellä korkealla tasolla.”
>
> ”Tietoturvallisuus mahdollistaa esim. etätyöskentelyn, joka olisi täysin mahdotonta ilman tietoturvallisia ja toimivia ratkaisuja.”
>
> ”Yritysten kanssa, kun toimii niin luotettavuus on yksi tärkeimmistä asioista.”

Jatkokysymyksenä kysyttiin, miten tietoturvallisuus toteutuu organisaatiossa. Esimiehistä 16,6 % ja 17,2 % tietohallinnon vastaajista kokee tietoturvallisuuden toteutuvan erittäin hyvin. Johtoryhmän jäsenistä 75,6 % ja tietoturvan vastaajista 64,2 % kokee tietoturvallisuuden toteutuvan hyvin. Tietoturvan vastaajista 14,5 % ja johtoryhmän vastaajista 7, 0 % kokee tietoturvallisuuden toteutuvan huonosti organisaatiossa (liite 75).

Perustelut.

> ”Ei ole mitään hirveän hälyttävää päässyt käymään ja kaikki rullaa ainakin toistaiseksi”
>
> ”Epätietoisuutta on liikaa. Laitteita ja ohjelmia tulee koko ajan lisää ja uusia, mutta kukaan ei anna perehdytystä.”

”Kaikki ymmärtänevät perusteet, mutta olemattoman koulutuksen vuoksi asiasta ei voi olla varma.”

”Lipsumista on tapahtunut ja tapahtuu koulutuksesta ja tiedottamisesta huolimatta. Itse puutun välittömästi poikkeaman havaittuani”

”On naivia uskoa, ettei tietoturva on täysin varmaa.”

”vanhentuneet tietoturva-ohjeet, välinpitämättömyys tietoturvan osalta, puutteelliset tekniset suojaukset ja puuttuva tietoturvakulttuuri”

”Vastuuhenkilöt on määritelty, ohjeistusta olemassa, koulutusta annettu ja saatavilla tarpeen mukaan.”

3.10 Esimiesten ja johtoryhmään kuuluvien lisäkysymykset

Esimiehille ja johtoryhmän jäseniltä kysyttiin kaksi lisäkysymystä. Heitä pyydettiin arvioimaan, kuinka he kokivat esitettyjen asioiden tärkeyden, haasteellisuuden ja toteutumisen organisaatiossaan. Vastaajat pääsivät arvioimaan esimerkiksi johdon sitoutumista, riskienhallintaa ja resursseja. Asioita arvioitiin asteikolla 0-4.

Tärkeys

4. Erittäin tärkeä
3. Tärkeä
2. Ei niin tärkeä
1. Ei lainkaan tärkeä
0. En osaa sanoa

Vaikeus

4. Erittäin vaikea
3. Vaikea
2. Kohtalaisen vaikea
1. Erittäin helppo
0. En osaa sanoa

Toteutuminen

4. Erittäin hyvin
3. Hyvin

2. Huonosti

1. Erittäin huonosti

0. En osaa sanoa

Johdon sitoutuminen tietoturvallisuuden toteutumiseen nähtiin erittäin tärkeänä, ja se koettiin onnistuneen hyvin. Asia koettiin kohtalaisen vaikeaksi. Esimiehet kokivat johdon sitoutumisen tietoturvallisuuden toteutumiseen johtoryhmän jäseniä vaikeammaksi.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,73	2,41	3,05
Esimiehet	3,74	2,49	3,03
Johtoryhmä	3,74	2,41	3,05
Ero	0	0,08	-0,02

Taulukko 11. Johto on sitoutunut tietoturvallisuuden toteuttamiseen.

Johdon sitoutuminen tietosuojan toteutumiseen koettiin myös erittäin tärkeäksi ja toteutuminen onnistuneeksi. Esimiehet kokivat johdon sitoutumisen tietosuojan toteutumiseen vaikeammaksi kuin johtoryhmän jäsenet.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,73	2,43	3,04
Esimiehet	3,74	2,52	3,03
Johtoryhmä	3,73	2,43	3,04
Ero	0,01	0,09	-0,01

Taulukko 12. Johto on sitoutunut tietosuojan toteuttamiseen.

Johdon tietämys mistä toimintaa koskevat tietoturvavaatimukset tulevat koettiin molemmissa ryhmissä tärkeäksi ja toteutuneen hyvin. Esimiehet kokivat tämän vaikeammaksi kuin johtoryhmän jäsenet.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,58	2,36	3,09
Esimiehet	3,56	2,43	3,06
Johtoryhmä	3,58	2,36	3,09
Ero	-0,02	0,07	-0,03

Taulukko 13. Johto tietää mistä toimintaa koskevat tietoturvavaatimukset tulevat.

Esimiehet kokivat vaikeammaksi itselleen ja organisaation muulle johdolle omata tarvittava tietoturvallisuuden osaaminen kuin johtoryhmän jäsenet. Molemmat ryhmät pitivät asiaa tärkeänä ja sen onnistuneen hyvin. (liite 76). Esimiehet kokivat, että tietoturvallisuuteen tarvittavat henkilöstöresurssit ja talousresurssit ovat kunnossa johtoryhmän jäseniä tärkeämmäksi. Esimiehet kokivat asian myös toteutuneen huonommin kuin esimiehet. Johtoryhmän jäsenet kokivat tämän parhaiten toteutuneeksi.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,78	2,69	2,73
Esimiehet	3,90	2,70	2,71
Johtoryhmä	3,78	2,69	3,73
Ero	0,12	0,01	-1,02

Taulukko 14. Organisaationi käytössä ovat tietoturvallisuuteen tarvittavat henkilöstöresurssit ja talousresurssit.

Johtoryhmän jäsenet kokevat tietotehtävien organisoinnin ja vastauiden jakamisen helpommaksi kuin esimiehet. Molemmat ryhmät pitivät asiaa tärkeänä ja asian toteutuneen hyvin (liite 77). Johtoryhmän jäsenet kokevat henkilöstön noudattavan tietoturvallisuutta koskevia ohjeita paremmin kuin esimiehet. Esimiehet ja johtoryhmän jäsenet kokivat tämän kaikkein tärkeimmäksi.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,8	2,72	2,86
Esimiehet	3,83	2,75	2,79
Johtoryhmä	3,80	2,72	2,86
Ero	0,03	0,03	-0,07

Taulukko 15. Henkilöstö noudattaa tietoturvallisuutta koskevia ohjeita.

Esimiehet kokevat tiedonkulun organisaation sisällä tärkeämmäksi kuin johtoryhmän jäsenet. Johtoryhmän jäsenet kokevat, että tehtävä on helpompi toteuttaa kuin esimiehet. Toteutumisessa ei näytä olevan eroja (liite 78).

Johtoryhmän jäsenet kokevat organisaatiossa olevan tietoturvaosaamisen tason tärkeämmäksi kuin esimiehet. Johtoryhmän jäsenet kokevat sen myös toteutuneen paremmin. Asian vaikeudessa ei ollut mitään eroja (liite 79). Esimiehet ja johtoryhmän jäsenet kokevat vaikeaksi saada riittävästi tietoa tietoturvallisuudesta johtamisen tueksi. Asia kuitenkin koettiin tärkeäksi ja toteutuneen hyvin (liite 80).

Esimiehet kokivat vaikeammaksi määritellä tietoturvapoikkeamien ja häiriötilanteiden toimintamallit (liite 81). Molemmat ryhmät kokivat, että häiriötilanteiden hallintaa ei harjoitella riittävästi. Esimiehet ja johtoryhmän jäsenet kokivat tämän kaikista vaikeimmaksi ja huonointen toteutuneeksi.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,39	2,76	2,21
Esimiehet	3,38	2,81	2,18
Johtoryhmä	3,39	2,76	2,21
Ero	-0,01	0,05	-0,03

Taulukko 16. Häiriötilanteiden hallintaa harjoitellaan riittävästi.

Molemmissa ryhmissä riskienhallinnan toimiminen koettiin tärkeäksi, mutta se ei ole toteutunut hyvin (liite 82). Molemmissa ryhmissä sopimuksissa tietoturvallisuuden huomioiminen ei ollut toteutunut hyvällä tasolla. Asia koettiin tärkeäksi, mutta myös vaikeaksi (liite 83). Molemmissa ryhmissä tietoturvapoikkeamien ilmoittaminen Viestintävirastossa toimivalle Kyberturvallisuuskeskukselle koettiin vaikeaksi ja toteutuneen melko hyvin. Johtoryhmän jäsenet kuitenkin kokivat asian helpommaksi ja toteutuneen paremmin kuin esimiehet. (liite 84).

Tietoturvapoikkeamista viestimisen suunnittelu ja vastuuttaminen nähtiin molemmissa ryhmissä vaikeana ja toteutuneen melko hyvin (liite 85). Organisaation riittävästi toteuttamat tietoturva-auditoinnit ja muut tarkastukset nähdään tärkeänä molemmissa ryhmissä. Se koetaan myös vaikeaksi ja toteutuneen vain melko hyvin (liite 86). Esimiehet kokivat teknisen tietoturvallisuuden tason, jotta sillä pystytään estämään keskeisimmät tietoturvauhan toteutumasta toteutuneen paremmin kuin johtoryhmän jäsenet. Molemmissa ryhmissä asia koettiin tärkeäksi (liite 87).

3.11 Tietoturvallisuuden kehittäminen

Johtoryhmän jäseniltä ja esimiehiltä kysyttiin, miten organisaation tietoturvallisuutta voitaisiin kehittää. Useat vastaajista kertoivat koulutusten olevan hyvä keino tietoturvallisuuden kehittämisessä.

> ”Antamalla hyvää koulutusta ja opastusta tiedostojen suojaamiseen.”
>
> ”Henkilökohtaisella ja osallistuvalla koulutuksella. Henkilöstö tarvitsee muitakin tapoja opiskella ja oppia kuin verkkokurssit.”
>
> ” Henkilökunnan koulutuksella ja asennekasvatuksella.”
>
> ”Järjestämällä koulutusta”

Osa vastaajista toivoi, että pitäisi olla selvempää kenelle vastuut kuuluvat

> ”Määrittelemällä selkeät vastuualueet ja toimintamallit miten ja kenen vastuulla tietoturvallisuus on”

> ” Määrittämällä vastuuhenkilö”

Vastaajat halusivat myös, että tietoturva saataisiin osaksi jokapäiväistä työntekoa.

> ”Nostamalla näitä asioita esiin säännöllisesti”

> ”puhumalla siitä ns. tavallisena toimintana, ei pelkästään kriisitoimintana”

> ”Säännöllistä positiivista puhetta asian tiimoilta.”

4 Tietoturvallisuuden kehittäminen

Kaikilta vastaajilta kysyttiin avoimien kysymysten avulla, miten heidän organisaationsa tietoturvallisuutta voitaisiin kehittää ja miten he ovat parantaneet organisaationsa tietoturvallisuutta.

4.1 Miten toivoisit tietoturvallisuutta kehitettävän

Näistäkin vastauksista huomasi, että vastaajat selvästi toivovat lisää koulutusta.

> ”Enemmän koulutusta koko henkilökunnalle. Ohjeet ja asetukset on vietävä nimenomaan käytäntöön.”

> ”Enemmän koulutusta.”

> ”Esimiesten kouluttaminen - henkilöstön kouluttaminen ja AIKAA”

Lisäksi toivottiin enemmän ohjeistusta.

> ”Antamalla lisää selkeitä ohjeita työntekijöille.”

> ”En koskaan löytänyt intrasta sitä tietoturvaopasta, joka olisi pitänyt lukea työsuhteen alkaessa ilmeisesti.”

> ”Enemmän puhetta, koulutusta ja selkeää ohjeistusta talon sisällä liittyen tietoturvaan. Selkeäksi jokaiselle se että tietoturva on tärkeä osa työpaikan kult-

> tuuria, riippumatta työtehtävästä. Selkeäksi mikä on kenenkin rooli ja osuus huolehdittaessa tietoturvasta.”

Jotkut tosin totesivat, että asioita pitäisi tuoda erilaisilla tavoilla esille.

> ”Asiaa voisi pitää enemmän esillä -- toisaalta henkilöstö uupuu jo nyt liiallisesta ohjeistuksesta; kaikkea ei kyetä omaksumaan.”

> ”Avoimuutta pitäisi lisätä ja tiedotusta. Pitäisi perustella, miksi asioita tehdään niin kuin tehdään. On oltava moderni.”

> ”Enemmän aikaa ajankohtaisiin tietoturva-asioihin perehtymiseksi. Auditoinnit tai vähintään sisäiset itsearvioinnit säännöllisiksi ja vakavasti otettaviksi kehittämisaihioiksi”

> ”Infoja häiriötilanteisiin valmistautumisesta.”

> ”Käytännön läheistä ja esimerkein tapahtuvaa ohjeistusta. Ei vain kirjettä sähköpostissa vaan käytäisiin ohjeet yhdessä läpi, vaikka pienryhmätöinä.”

Tukea kaivattiin lisää johdolta ja esimiehiltä.

> ”Johdon ja esimiesten tulee sitoutua tietotuvalliseen toimintaan. Tietoturvallisten työvälineiden saatavuuteen ja toimivuuteen tulee panostaa huomattavasti lisää resursseja.”

> ”Johdon otettava vastuu periaatteiden lisäksi myös tietoturvallisten toimintamallien käytännön toteuttamisesta”

> ”Johdon tuki ja ymmärrys tietoturva-asioihin olisi hyvä asia.”

> ”Jokainen esimies pitää huolen, että työntekijät käyvät tietoturvatestin läpi ja yhä uudelleen toistettava palavereissa salassapitovelvoitetta.”

Jotkut vastaajista kaipasivat selvyyttä tietosuojaan.

> ”Tietosuoja asioiden kehittämistä tulee jatkaa nimetyn henkilön toimesta. Hyvä keino on tietoturvakoulutus henkilöstölle.”

> ”Tietosuoja-asioihin kaipaisin linjausta ja käytännön ohjeistusta. Ettei tehtäisi turhia ja kalliita nykyisiin tietojärjestelmiin kohdistuvia uudistuksia sen takia, ettei tiedetä, mitä oikeasti lain tulkinta vaatii. ”

> ”Tietosuojauksesta vastaava henkilö on jäänyt vähän pimentoon", enemmän tietoa yleensäkin tietoturvallisuudesta, koska paljon käsitellään henkilötietoja myös kannettavilla laitteilla työyksiköiden ulkopuolella. Haluan tietää, miten voin minimoida risti, jottei tietovuotoja tapahdu omalta osaltani."

4.2 Tietoturvallisuuden parantaminen

Vastaajilta kysyttiin, miten he ovat parantaneet organisaationsa tietoturvallisuutta. Moni vastasi auttavansa tai tukevansa toiminnallaan muita.

> ”Antamalla työntekijöille ohjeita siitä, miten asioihin tulisi kiinnittää vieläkin tarkemmin huomiota.”

> ”Ehdottanut esim. turvatulostuksen käyttöönottamista.”

> ”Kiinnittänyt henkilöstön huomiota somessa esiintymiseen työasioissa ja painottanut tietoturvan merkitystä erityisesti etätyössä.”

> ”Ohjeistus henkilöstölle. Lukittavat kaapit.”

> ”Pidän asiaa säännöllisesti esillä esim. henkilöstön tapaamisissa, esimerkkiä näyttämällä mm. kulkukorttien käyttö.”

> ”Välittänyt tietoa, kouluttanut henkilöstöä tietoturvallisuuden osalta.”

Toiset keskittyivät toiminnastaan huolehtimiseen.

> ”Huolehdin oman toimintani tietoturvallisuudesta ja neuvon parhaani mukaan, jos yksikössäni jollain on kysyttävää esim. lomakkeiden käsittelystä ja hävittämisestä.”

> ”Itse noudatan mahdollisimman hyvin ja käytän maalaisjärkeä.”

> ”Kirjaudun ulos ohjelmasta, kun lopetan työskentelyn. Käytän vain työantajan laitteita mm. spostia lukiessani.”

> ”Olen käynyt VAHTI ja JUHTA työpajoissa”

> ”Siirtynyt käyttämään varmennekorttia sekavien salasanojen sijaan”

> ”Tietosuojattujen sähköpostikäytäntöjen käyttöönotto, oman tietovarannon lisääminen (itseopiskelu).”

> ”Yritän vähentää omassa toiminnassani olevia riskejä”

5 Palaute kyselystä

Osa piti kyselyä tarpeellisena.

> ”Asia on niin tärkeä, että pitää seurata koko ajan. Pitäisi myös seurata, että näihin vastataan ja jos tulokset huonot, edellyttää johdolta toimintaa.”
>
> ”Asiallinen, joskin hyvin yleisellä tasolla käsittelevä.”
>
> ”Erittäin tarpeellinen kysely ja tällaisen pitäisi olla pakollinen kaikille valtion virastojen työntekijöille. Kysely pitäisi uusia säännöllisesti ja siitä pitää tulla viraston johdolle palaute ja selvityspyyntö mihin toimenpiteisiin on ryhdytty.”
>
> ”Erittäin hyvä, että tietoturva-asioihin puututaan. Etsitään epäkohdat ja pyritään vaikuttamaan niihin.”
>
> ”Hieno homma, että näitä tehdään. Vahti -ryhmä tekee todella tärkeää työtä (ja on tehnyt jo vuosia). Mielestäni näillä kyselyillä on merkittävä vaikutus tietoturvan kehittymiseen, se nähtiin jo viime vuoden kyselystä, johon valitettavasti ajan puutteen vuoksi oma organisaatiomme ei vielä ehtinyt mukaan. Nyt ehdittiin...”
>
> ”Hyvä ja ajankohtainen kysely. Toivottavasti tulokset konkretisoituvat ja johtavat toimenpiteisiin omassa organisaatiossani - mieluummin ennen kuin mikään uhka toteutuu.”
>
> ”Ok ja aika ymmärrettävät kysymyksetkin. Ei pelkkää ITC jargonia, jota muut eivät ymmärrä.”

Toisten mielestä se oli liian pitkä tai haastava.

> ”Aika epäoleellisia asioita kyselyssä. Mistään teknisestä toteutuksesta ei ollut kysymyksiä (ei uskallettu?). Olisin voinut niihin antaa jopa positiivista palautetta, että virtuaalikoneet ja kertakirjautumiset tulivat hallintoon ~10 vuotta myöhemmin kuin mitä yksityiselle sektorille, mutta sentään tulivat ja jopa kohtuullisen toimivina!”
>
> ”Hankala täyttää kun vastausvaihtoehdot olivat sivun yläosassa. Joutui aika-ajoin palaamaan sivun yläosaan.”

> ”Joissakin kysymyksissä ei ollut oikeaa vastauskohtaa ja jos jätti vastaamatta, ohjelma ei päästänyt eteenpäin. Joihinkin kysymyksiin olisi voinut laittaa 2 täpin useaankin kohteeseen.”
>
> ”Jokin väittämä olisi piristänyt tylsiä kysymyksiä :)”
>
> ”Liian pitkä, vaihtoehtovastauksissa liian karkea jaottelu, parempi numeraalinen skaala 1-10 kuin hyvin/huonosti. ”
>
> ”Tosi vaikeaa ja hieman turhauttavaakin oli vastata, kun ei ole koulutuspohjaa tällaiselle. Digitiimiläisille se voi ollakin helppoa. Kun ei oikein ymmärrä sitäkään, miksi koneet kesäisten päivitysten jälkeen jatkuvasti herjaavat jotain One Driveä tai pitää sulkea ilmoituksia näytöltä. Tuntuu aika heikoilta nuo Windows10:n ohjelmistot. ”
>
> ”Välillä jäin miettimään ja oli epäselvää, mitä sanalla organisaatio" pitäisi ymmärtää - omaa yksikköä vai laajempaa yhteisöä, "osastoa". Vaikutti vastaamiseen, sekoitti. "”

Jotkut vastaajat eivät kokeneet, että kysely koskee heitä.

> ”Ei ihan osu omaan yksikkööni”
>
> ”En ymmärtänyt edes kaikkia kysymyksiä - ilmeisesti ei koske meitä, jotka työskentelevät todella vähän koneella. (tehdään enemmän fyysistä työtä)”

6 Tulosten yhteenveto ja kehittämisideat

6.1 Tulosten yhteenveto

Suurin osa vastaajista käyttää työtehtäviensä tekemiseen vain työnantajan laitteita, mikä on hyvä, sillä henkilökohtaisten laitteiden tietoturvallisuudesta ei voi olla täyttä varmuutta. lähes kaikki vastaajista kokee päivittäisen työskentelyn hyvin turvalliseksi tai turvalliseksi. Vain muutama vastaaja ei ollut miettinyt asiaa ollenkaan.

Kuten henkilöstön ja johdon tietoturvabarometristä (Rousku, 2018) jo huomattiin, yleisesti organisaatiossa saadaan hyvin ohjeistusta, mutta koulutuksen toteuttaminen jää huomattavasti pienemmäksi. Yli puolet vastaajista ei kokenut tarvetta lisäohjeistukselle tai lisäkoulutukselle, kuitenkin sanallisessa palautteessa etenkin koulutusta toivottiin lisää ja se nähtiin hyvänä tapa saada tietoa henkilöstölle. Eniten lisäohjeistusta ja lisäkoulutusta kaivattiin tietojen salaamisessa, tietojen luokittelussa ja salassa pidettävän tiedon käsittelyssä.

Vastaajien suosituin kirjatumistapa työasemaan ja työtehtäviin liittyvissä palveluissa on käyttäjätunnus ja salasana. Vastaajat käyttävät palveluissa pääsääntöisesti eri salasanoja. Esimiehiä ja johtoryhmän jäseniä huoletti kaikkein vähiten se, että heidän työtehtävänsä edellyttäisivät tietoturvaohjeiden vastaista toimintaa. Heitä huolestutti eniten se, että he menettävät tärkeitä tietoja laiterikon takia. Tietohallinnon vastaajia huolestutti vähiten se, että heitä uhkaillaan nettipalvelussa. Eniten heitä huolestutti se, että eivät saa riittävää tukea johdolta tietosuojalle. Tietoturvan vastaajia huolestutti vähiten se, että eivät tiedä mikä heidän vastuu tietoturvallisuuden osalta on. Suurin huoli heillä oli, että eivät saa riittävästi tukea johdolta tietoturvallisuudelle.

Vastaajat kokivat saavansa ohjeistusta salassa pidettävien tietojen luokitteluun. Vastaajat kokivat osaavansa käyttää luokittelua hyvin tai tyydyttävästi. Yli 60% vastaajista tietää, miten eri palveluja ja työkaluja käytetään salassa pidettävien tietojen luokittelussa. Osa kehitysehdotuksista on koottu vastaajilta tulleesta palautteesta ja osa on tekijän huomioihin perustuvia parannusehdotuksia. Vastaajat kokivat osaavansa käyttää näitä työkaluja ja palveluja hyvin.

Esimiehet ja johtoryhmän jäsenet kertoivat käsittelevänsä henkilötietoja päivittäin tai useamman kerran viikossa. Tietohallinnon vastaajat käsittelevät henkilötietoja päivittäin, useamman kerran viikossa tai eivät käsittele ollenkaan. Tietoturvan vastaajat käsittelevät henkilötietoja selvästi jo muita harvemmin, kuitenkin päivittäin, useamman kerran viikossa tai harvemmin kuin kuukausittain. Yli puolet vastaajista koki, että heidän organisaatiossaan käsitellään vain tarpeellisia henkilötietoja. Tietohallinnon vastaajista hieman yli neljäs osa ei osannut sanoa.

Tietohallinnon ja tietoturvan vastaajat kokivat, että organisaatiossa on ryhdytty toimiin, on käynnistetty tai ollaan käynnistämässä hanke tietosuoja-asetuksen osalta. Esimiesten ja johtoryhmän vastaajien osalta oli suurempaa hajontaa. Esimiehistä suurin osa kertoi että, joko ollaan ryhdytty toimiin tai että he eivät ole havainneet mitään. Johtoryhmän jäsenissä joko oltiin tietoisia tai oltiin ryhdytty toimiin. Kun kysyttiin, tiesivätkö vastaajat, kuka heidän organisaatiossa on se henkilö, jolta voi kysyä tietosuoja asioista yli puolet vastasi tietävänsä, keneltä asiasta kuuluu kysyä.

Vastaajista suurin osa kertoi, että heidän organisaationsa sallii työskentelyn toimipaikan ulkopuolella. Vastaajat hyödyntävät tätä mahdollisuutta epäsäännöllisesti, kuitenkin kuukausittain. Hieman alle puolet vastaajista sai tarpeeksi ohjeistusta työskentelyyn toimipaikan ulkopuolella. Lähes kaikki vastaajat pystyivät toimimaan ohjeiden mukaisesti joko erittäin hyvin tai hyvin.

Esimiesten, johtoryhmän jäsenten ja tietoturvan vastaajat lukevat sähköpostia työnantajan laitteella päivittäin. Tietohallinnon vastaajat lukevat sähköpostia arkipäivisin. Esimiehet lukevat muutaman kerran vuodessa henkilökohtaisilla laitteilla tai eivät lue niillä ollenkaan.

Johtoryhmän jäsenet, tietohallinnon ja tietoturvan vastaajat eivät lue sähköpostia ollenkaan henkilökohtaisilla laitteillaan.

Vastaajista suurin osa kokee, että tietoturvallisuus lisää työskentelyn laatua ja luotettavuutta. Melkein kaikki vastaajista kokee, että tietoturvallisuus toteutuu hyvin organisaatiossa.

Esimiesten ja johtoryhmän kysymyksistä molemmat kokivat tärkeimmäksi, että henkilöstö noudattaa tietoturvallisuutta koskevia ohjeita. Vaikeimmaksi asiaksi molemmat ryhmät kokivat riittävän häiriötilanteiden hallinnan harjoittelun. Tämä oli myös koettu toteutuneen huonoiten. Esimiehet kokivat parhaiten toteutuneen sen, että johto tietää mistä toimintaa koskevat tietoturvavaatimukset tulevat. Johtoryhmän jäsenet kokivat parhaiten toteutuneen sen, että heillä on tarvittavat henkilöstöresurssit ja talousresurssit tietoturvallisuuteen.

6.2 Kehitysehdotuksia

Osa kehitysehdotuksista on koottu vastaajilta tulleesta palautteesta ja osa on tekijän huomioihin perustuvia parannusehdotuksia.

6.2.1 Vastaajaksi kyselyyn ilmoittautuminen

Ilmoittautuminen oli syksyn kyselyssä mahdollista vain suomeksi. Se aiheutti vastaajissa huolta siitä, että myös kysely on mahdollista tehdä vain suomeksi. Tasavertaisuuden ja selvyyden takia olisi hyvä, että ilmoittautumislomake olisi mahdollista saada myös ruotsiksi.

Ilmoittautumisen yhteydessä olisi hyvä kysyä organisaation kokoa. Vastaaminen voisi olla vapaaehtoista, jos edes osa ilmoittautujista ilmoittaisi organisaation koon, se vähentäisi analysoijan työmäärää, sillä hänen ei tarvitsisi erikseen kysyä organisaation kokoa niin monelta ilmoittautuneelta. Tämä myös nopeuttaisi tilastojen tekemistä.

Ilmoittautumisen ja ohjeistuksen avulla on koetettava tehdä ilmoittautujalle selvemmäksi, että kysely koskee koko henkilöstöä eikä vain esimerkiksi tietoturvavastaavia. Syksyn kyselyssä kaikki vastaajat eivät olleet tätä ymmärtäneet.

6.2.2 Kysely

Kyselyn alussa olisi hyvä olla alkuteksti, mikä olisi kaikkien vastaajien luettavissa. Siinä tulisi kertoa, mihin tarkoitukseen kysely on tehty, mitä sen tuloksilla tehdään ja missä tulokset julkaistaan. Tekstissä kannattaisi myös mainita, miksi kysely teetetään koko henkilöstölle eikä vain tietoturvan kanssa päivittäin työskenteleviltä. Lisäksi tulisi mainita, että jokainen organisaatio saa käyttöönsä oman organisaationsa tulokset. Saadessaan linkin kyselyyn organisaatiot ovat saaneet myös ohjeistuksen vastaajille, mutta ilmeisesti se ei ole tavoittanut kaikkia vastaajia ja sen takia monet aiemmin mainitsemistani asioita olivat jääneet usealle vastaajalle epäselväksi. Olisi siis parempi laittaa vastausohjeistus alkutekstistä ennen kyselyä, jotta jo-

kaisella vastaajalla olisi mahdollisuus saada kaikki tarpeellinen tieto. Kyselyn eettisyyttä voitaisiin parantaa lisäämällä alkutekstiin osio, missä kerrotaan vastaajan oikeudesta jättää kysely osittain tai kokonaan täyttämättä. Lisäksi kyselyn tekijöiden tulisi miettiä, mikä kysymykset kyselyssä pidetään pakollisina ja millä perustein.

Osa vastaajista koko kyselyssä käytetyn termistön oudoksi. Kyselyn lopussa voisi olla kohta, missä vastaajilta ensin kysyttäisiin, oliko jotkin kyselyn termeistä vieraita. Jos vieraita termejä esiintyy, olisi vastaajilla tämä jälkeen mahdollisuus kirjata vieraat termit. Silloin jokainen organisaatio saisi tiedon, mitkä tietoturvallisuuteen liittyvät termit ovat epäselviä heidän työntekijöilleen. Vastaajat kokivat osan kysymyksistä todella raskaiksi, etenkin koulutusta ja ohjeistusta selvittävät kysymykset. Kyselyä tulisi pyrkiä keventää. Osalle vastaajista oli epäselvää, mikä on ohjeistuksen ja koulutuksen ero. Tämä tulisi selventää kysymyksen alussa, vaikka pienellä tekstillä.

Kyselyssä kysyttiin, onko työntekijä saanut töidensä alussa ohjeistusta tai koulutusta tietoturvaan liittyvissä asioissa. Kuitenkin jotkut vastaajat ovat aloittaneet työnsä silloin, kun töissä ei ole käytetty tietokoneita, jolloin he voivat vain vastata, etteivät ole saaneet ohjeistusta tai koulutusta. Nämä vastaajat väärentävät hiukan tilastoa, joten heille tulisi luoda oma vastausvaihtoehto. Osa vastaajista pohti miten vastata tilanteessa, jossa vastaaja on itse opiskellut aihetta tai sai koulutusta siihen edellisessä työpaikassa. Näitä asioita tulisi selventää vastaajille joko antamalla enemmän vastausvaihtoehtoja tai mainitsemalla alkutekstissä, että itse opiskeltua tai aikaisemmassa työssä saatua ohjeistusta tai koulutusta ei huomioida, sillä halutaan saada tietoa, miten asiat on hoidettu vastaajan sen hetkisen työnantajan toimesta.

Koulutuksen ja ohjeistuksen saannin lisäksi olisi mielenkiintoista tietää, osaavatko vastaajat oikeasti noudattaa tai soveltaa saamaansa tietoa. Useat vastanneista olisivat toivoneet ”en tiedä” vastausvaihtoehdoksi. Tämä kuitenkin luo riskin siihen, että vastaajat valitsisivat liian helposti ”en tiedä” -vaihtoehdon. Etenkin kun moni vastanneista ilmaisi palautteessa, että ei ollut välttämättä ymmärtänyt kaikkia termejä, joita käytettiin kyselyssä.

6.2.3 Tulokset

Tulosten perusteella voi päätellä, että tietoturvan perusasioissa on vielä parannettavaa. Vastausten mukaan työntekijät eivät saa riittävästi koulutusta tietoturva-asioista. Avoimien vastausten perusteella vastaajat toivovat lisää koulutusta, mutta myös ohjeistusta. Koulutuksen ja ohjeistuksen lisäksi kaivattiin tiedottamista ajankohtaisista asioista ja uudenlaisia tapoja kehittää henkilöstön tietoturvaosaamista.

Avoimien vastausten perusteella vastaajat haluaisivat enemmän yhteistyötä eri toimijoiden välillä. Lisäksi termistö vaikutti tuottavan joillekin vastaajille ongelmia. Ne tulisi saada osaksi työntekijöiden jokapäiväistä työntekoa. Tulosten perusteella esimiehiltä ja johtoryhmän jä-

seniltä toivotaan konkreettista tuen osoittamista eri organisaation ryhmille etenkin tietoturvan ja tietosuojan osalta. Avoimien kysymysten perusteella johdon ja esimiesten tukea kaivataan enemmän tietoturvan parissa. Johdon ja esimiesten vastausten perusteella olisi tarvetta harjoitella häiriötilanteiden hallintaa.

Lähteet

Painetut

Alapuro, R. Arminen, I. 2004. Vertailevan tutkimuksen ulottuvuuksia. WSOY. Werner Söderström. Vantaa.

Eskola, J. Suoranta J. 2008. Johdatus laadulliseen tutkimukseen. 8. painos. Gummerus kirjapaino. Jyväskylä.

Kuula, A. 2006. Tutkimusetiikka aineistojen hankinta, käyttö ja säilytys. Gummerus kirjapaino. Jyväskylä.

Laaksonen, S-M. Matikainen J. Tikka, M. 2013. Otteita verkosta, verkon ja sosiaalisen median tutkimusmenetelmät. Bookwell. Jyväskylä

Mäkinen, O. 2006. Tutkimusetiikan ABC. Tammi. Helsinki

Niiniluoto, I. 1999. Johdatus tieteenfilosofiaan, käsitteen- ja teorianmuodostus. 2. painos. Otava. Keuruu.

Ronkainen, S. Pehkonen L. Lindblom-Ylänne, S. Paavilainen, E. 2013. Tutkimuksen voimasanat. 1-2. painos. Sanoma Pro. Helsinki.

Ronkainen, S. Karjalainen, A. 2008. Sähköä kyselyyn! Web-kysely tutkimuksessa ja tiedonkeruussa. Lapin yliopistopaino. Rovaniemi.

Räsänen, P. Anttila, A-H. Melin, H. 2005. Tutkimus menetelmien pyörteissä; Sosiaalitutkimuksen lähtökohdat ja valinnat. WS Bookwell. Juva.

Toikko, T. Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta. Tampereen Yliopistopaino. Tampere.

Tuomi, J. 2007. Tutki ja lue, johdatus tieteellisen tekstin ymmärtämiseen. Tammi.

Uusitalo, H. 1991. Tiede, tutkimus ja tutkielma, johdatus tutkielman maailmaan. Werner Söderström. Juva.

Vehkalahti, K. 2008. Kyselytutkimuksen mittarit ja menetelmät. Vammalan kirjapaino. Vammala.

Sähköiset

Kuivalainen, M. Rousku, K. 2016. Henkilöstön ja johdon tietoturvabarometri. Viitattu 23.5.2018.
http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79060/VAHTI3_henkiloston_ja_johdon_tietoturvabarometri.pdf?sequence=1&isAllowed=y

Rousku, K. 2018. Henkilöstön ja johdon tietoturvabarometri. Viitattu 23.5.2018.
http://julkaisut.valtioneuvosto.fi/

Valtiovarainministeriö. VAHTI-toiminta. Viitattu 29.5.2018. http://vm.fi/vahti

Taulukot

Liitteet

Liite 1: Ensimmäinen liite

Tietoturvaperehdytys koulutus työsuhteen alkaessa.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	2158	26,6 %	368	29,2 %	143	29,4 %	181	35,8 %	82	51,6 %
En	2001	24,6 %	328	26,0 %	112	23,0 %	111	22,0 %	22	13,8 %
En tarvitse	122	1,5 %	12	1,0 %	6	1,2 %	15	3,0 %	10	6,3 %

Liite 2: Toinen liite

Koulutus turvalliseen toimintaan organisaation toimililoissa.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	2451	30,2 %	442	35,1 %	173	35,5 %	182	36,0 %	92	57,9 %
En	1620	19,9 %	254	20,1 %	84	17,2 %	105	20,8 %	18	11,3 %
En tarvitse	133	1,6 %	9	0,7 %	8	1,6 %	11	2,2 %	5	3,1 %

Liite 3: Kolmas liite

Ohjeistus turvalliseen toimintaan organisaation toimitiloissa.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	5508	67,8 %	854	67,7 %	339	69,6 %	371	73,5 %	115	72,3 %
En	1092	13,4 %	157	12,5 %	55	11,3 %	63	12,5 %	10	6,3 %
En tarvitse	120	1,5 %	16	1,3 %	9	1,8 %	8	1,6 %	4	2,5 %

Liite 4: Neljäs liite

Ohjeistus etätyöskentelyyn tai työskentelyyn toimipaikan ulkopuolella.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	3750	46,2 %	700	55,5 %	307	63,0 %	372	73,7 %	104	65,4 %
En	1873	23,1 %	270	21,4 %	87	17,9 %	67	13,3 %	23	14,5 %
En tarvitse	1227	15,1 %	99	7,9 %	28	5,7 %	27	5,3 %	9	5,7 %

Liite 5: Viides liite

Koulutus etätyöskentelyyn tai työskentelyyn toimipaikan ulkopuolella.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	952	11,7 %	208	16,5 %	91	18,7 %	101	20,0 %	44	27,7 %
En	1934	23,8 %	346	27,4 %	116	23,8 %	127	25,1 %	42	26,4 %
En tarvitse	1139	14,0 %	94	7,5 %	24	4,9 %	36	7,1 %	13	8,2 %

Liite 6: Kuudes liite

Ohjeistus tietojen luokitteluun.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	3284	40,4 %	560	44,4 %	226	46,4 %	267	52,9 %	95	59,7 %
En	2849	35,1 %	446	35,4 %	115	23,6 %	147	29,1 %	27	17,0 %
En tarvitse	577	7,1 %	32	2,5 %	14	2,9 %	22	4,4 %	7	4,4 %

Liite 7: Seitsemäs liite

Koulutus tietojen luokitteluun.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	1501	18,5 %	267	21,2 %	128	26,3 %	143	28,3 %	74	46,5 %
En	2222	27,4 %	403	32,0 %	127	26,1 %	139	27,5 %	32	20,1 %
En tarvitse	500	6,2 %	24	1,9 %	15	3,1 %	23	4,6 %	8	5,0 %

Liite 8: Kahdeksas liite

Ohjeistus henkilötietojen käsittelyyn ja tietosuojan.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	5445	67,0 %	905	71,8 %	353	72,5 %	336	66,5 %	101	63,5 %
En	903	11,1 %	108	8,6 %	37	7,6 %	79	15,6 %	26	16,4 %
En tarvitse	250	3,1 %	13	1,0 %	9	1,8 %	20	4,0 %	4	2,5 %

Liite 9: Yhdeksäs liite

Ohjeistus salassa pidettävän tietoaineiston käsittelyyn.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	2802	34,5 %	523	41,5 %	197	40,5 %	182	36,0 %	66	41,5 %
En	1422	17,5 %	215	17,0 %	77	15,8 %	106	21,0 %	34	21,4 %
En tarvitse	251	3,1 %	11	0,9 %	10	2,1 %	24	4,8 %	6	3,8 %

Liite 10: Kymmenes liite

Koulutus salassa pidettävän tietoaineiston käsittelyyn.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	2649	32,6 %	487	38,6 %	187	38,4 %	183	36,2 %	86	54,1 %
En	1510	18,6 %	233	18,5 %	80	16,4 %	109	21,6 %	20	12,6 %
En tarvitse	232	2,9 %	12	1,0 %	12	2,5 %	17	3,4 %	6	3,8 %

Liite 11: Yhdestoista liite

Ohjeistus tietojen salaamiseen.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	3069	37,8 %	5527	41,8 %	218	44,8 %	255	50,5 %	93	58,5 %
En	3242	39,9 %	498	39,5 %	173	35,5 %	169	33,5 %	36	22,6 %
En tarvitse	529	6,5 %	25	2,0 %	15	3,1 %	37	39,4 %	8	5,0 %

Liite 12: Kahdestoista liite

Koulutus tietojen salaamiseen.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	1159	14,3 %	218	17,3 %	86	17,7 %	94	18,6 %	42	26,4 %
En	2558	31,5 %	456	36,2 %	159	32,6 %	146	28,9 %	51	32,1 %
En tarvitse	447	5,5 %	20	1,6 %	10	2,1 %	34	6,7 %	9	5,7 %

Liite 13: Kolmastoista liite

Ohje mobiililaitteiden käyttöön.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	4021	49,5 %	699	55,4 %	297	61,0 %	342	67,7 %	102	64,2 %
En	2477	30,5 %	348	27,6 %	115	23,6 %	99	19,6 %	30	18,9 %
En tarvitse	433	5,3 %	34	2,7 %	9	1,8 %	28	5,5 %	3	1,9 %

Liite 14: Neljästoista liite

Koulutus mobiililaitteiden käyttöön.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	1166	14,4 %	193	15,3 %	79	16,2 %	88	17,4 %	43	27,0 %
En	2433	30,0 %	428	33,9 %	148	30,4 %	144	28,5 %	57	35,8 %
En tarvitse	428	5,3 %	31	2,5 %	10	2,1 %	36	7,1 %	5	3,1 %

Liite 15: Viidestoista liite

Ohjeistus sähköpostin käyttöön.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	5764	71,0 %	936	74,2 %	360	73,9 %	372	73,7 %	113	71,1 %
En	1074	13,2 %	125	9,9 %	50	10,3 %	56	11,1 %	16	10,1 %
En tarvitse	87	1,1 %	10	0,8 %	4	0,8 %	33	6,5 %	5	3,1 %

Liite 16: Kuudestoista liite

Koulutus sähköpostin käyttöön.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	2165	26,7 %	375	29,7 %	140	28,7 %	134	26,5 %	58	36,5 %
En	1768	21,8 %	286	22,7 %	100	20,5 %	109	21,6 %	40	25,2 %
En tarvitse	128	1,6 %	15	1,2 %	6	1,2 %	37	7,3 %	6	3,8 %

Liite 17: Seitsemästoista liite

Ohjeistus internetin käyttöön.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	4979	61,3 %	846	67,1 %	328	67,4 %	339	67,1 %	99	62,3 %
En	1872	23,0 %	222	17,6 %	84	17,2 %	92	18,2 %	31	19,5 %
En tarvitse	144	1,8 %	14	1,1 %	8	1,6 %	37	7,3 %	7	4,4 %

Liite 18: Kahdeksastoista liite

Koulutus internetin käyttöön.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	1638	20,2 %	299	23,7 %	114	23,4 %	95	18,8 %	43	27,0 %
En	2105	25,9 %	331	26,2 %	115	23,6 %	133	26,3 %	45	28,3 %
En tarvitse	188	2,3 %	19	1,5 %	7	1,4 %	36	7,1 %	9	5,7 %

Liite 19: Yhdeksästoista liite

Ohjeistus sosiaalisen median käyttöön.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	4273	52,6 %	776	61,5 %	305	62,6 %	275	54,5 %	105	66,0 %
En	2222	27,4 %	266	21,1 %	103	21,1 %	139	27,5 %	29	18,2 %
En tarvitse	524	6,5 %	50	4,0 %	15	3,1 %	49	9,7 %	5	3,1 %

Liite 20: Kahdeskymmenes liite

Koulutus sosiaalisen median käyttöön

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	1231	15,2 %	246	19,5 %	114	23,4 %	82	16,2 %	43	27,0 %
En	2184	26,9 %	366	29,0 %	109	22,4 %	137	27,1 %	44	27,7 %
En tarvitse	522	6,4 %	37	2,9 %	15	3,08 %	52	10,3 %	11	6,9 %

Liite 21: Kahdeskymmenesensimmäinen liite

Ohjeistus tietoturvalliseen salasanojen hallintaan.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	5397	66,4 %	873	69,2 %	343	70,4 %	339	67,1 %	101	63,5 %
En	1516	18,7 %	186	14,8 %	72	14,8 %	100	19,8 %	27	17,0 %
En tarvitse	104	1,3 %	12	1,0 %	4	0,8 %	26	5,1 %	9	5,7 %

Liite 22: Kahdeskymmenestoinen liite

Koulutus tietoturvalliseen salasanojen hallintaan.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	1763	21,7 %	309	24,5 %	112	23,0 %	111	22,0 %	48	30,2 %
En	2020	24,9 %	338	26,8 %	123	25,3 %	134	26,5 %	43	27,0 %
En tarvitse	115	1,4 %	13	1,0 %	4	0,8 %	24	4,8 %	8	5,0 %

Liite 23: Kahdeskymmeneskolmas liite

Ohjeistus häiriötilanteissa toimimiseen, esimerkiksi palveluiden käyttökatko.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	3917	48,2 %	662	52,5 %	276	56,7 %	315	62,4 %	87	54,7 %
En	3113	38,3 %	429	34,0 %	150	30,8 %	120	23,8 %	42	26,4 %
En tarvitse	151	1,9 %	15	1,2 %	5	1,0 %	28	5,5 %	6	3,8 %

Liite 24: kahdeskymmenesneljäs liite

Koulutus häiriötilanteissa toimimiseen, esimerkiksi palveluiden käyttökatko.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	945	11,6 %	183	14,5 %	69	14,2 %	109	21,6 %	46	28,9 %
En	2584	31,8 %	411	32,6 %	152	31,2 %	137	27,1 %	49	30,8 %
En tarvitse	198	2,4 %	21	1,7 %	10	2,1 %	29	5,7 %	6	3,8 %

Liite 25: Kahdeskymmenesviides liite

Ohjeistus tietoturvallisuuspoikkeamissa toimimiseen, esimerkiksi haittaohjelmaepäily.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	4734	58,3 %	822	65,2 %	329	67,6 %	368	72,9 %	107	67,3 %
En	2355	29,0 %	277	22,0 %	96	19,7 %	72	14,3 %	22	13,8 %
En tarvitse	109	1,3 %	8	0,6 %	4	0,8 %	21	4,2 %	8	5,0 %

Liite 26: Kahdeskymmeneskuudes liite

Koulutus tietoturvapoikkeamissa toimimiseen, esimerkiksi haittaohjelmaepäily.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	1125	13,8 %	215	17,0 %	86	17,7 %	128	25,3 %	60	37,7 %
En	2454	30,2 %	393	31,2 %	132	27,1 %	134	26,5 %	28	17,6 %
En tarvitse	148	1,8 %	15	1,2 %	7	1,4 %	23	4,6 %	10	6,3 %

Liite 27: Kahdeskymmenesseitsemäs liite

Ohjeistus yleisestä tietoturvasta.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	5761	70,9 %	912	72,3 %	353	72,5 %	376	74,5 %	112	70,4 %
En	1002	12,3 %	111	8,8 %	42	8,6 %	48	9,5 %	9	5,7 %
En tarvitse	74	0,9 %	6	0,5 %	5	1,0 %	17	3,4 %	7	4,4 %

Liite 28: Kahdeskymmeneskahdeksas liite

Koulutus yleisestä tietoturvasta.

Koulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Olen	2512	30,9 %	452	35,8 %	190	39,0 %	214	42,4 %	92	57,9 %
En	1520	18,7 %	229	18,2 %	73	15,0 %	84	16,6 %	11	6,9 %
En tarvitse	105	1,3 %	11	0,9 %	5	1,0 %	19	3,8 %	10	6,3 %

Liite 29: Kahdeskymmenesyhdeksäs liite

Tarve lisäohjeistukselle ja lisäkoulutukselle.

Tarve	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Kyllä	3364	42,1 %	605	48,8 %	218	45,4 %	183	36,5 %	58	36,7 %
Ei	4635	57,9 %	635	51,2 %	262	54,6 %	318	63,5 %	100	63,3 %
Yhteensä	7999	100,0 %	1240	100,0 %	480	100,0 %	501	100,0 %	158	100,0 %

Liite 30: Kolmaskymmenes liite

Lisäohjeistus ja lisäkoulutus.

Lisäohjeistus ja lisäkoulutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Tietoturvaperehdytys työsuhteeni alkaessa	637	18,9 %	119	19,7 %	34	15,6 %	38	20,8 %	15	25,9 %
Turvallinen toiminta organisaation toimitiloissa	798	23,7 %	147	24,3 %	39	17,9 %	43	23,5 %	12	20,7 %
Etätyöskentely tai työskentely toimipaikan ulkopuolella	1192	35,4 %	228	37,7 %	84	38,5 %	51	27,9 %	20	34,5 %
Tietojen luokittelu	1509	44,9 %	296	48,9 %	105	48,2 %	98	53,6 %	28	48,3 %
Henkilötietojen käsittely ja tietosuoja	1275	37,9 %	231	38,2 %	72	33,0 %	91	49,7 %	23	39,7 %
Salassa pidettävän tietoaineiston käsittely	1460	43,4 %	272	45,0 %	90	41,3 %	98	53,6 %	29	50,0 %
Tiedostojen salaaminen	1901	56,5 %	387	64,0 %	127	58,3 %	77	42,1 %	32	55,2 %
Mobiililaitteiden käyttö	1141	33,9 %	201	33,2 %	69	31,7 %	39	21,3 %	24	41,4 %
Sähköpostin käyttö	620	18,4 %	97	16,0 %	23	10,6 %	20	10,9 %	9	15,5 %
Internetin käyttö	611	18,2 %	96	15,9 %	31	14,2 %	16	8,7 %	8	13,8 %
Sosiaalisen median käyttö	921	27,4 %	182	30,1 %	60	27,5 %	49	26,8 %	14	24,1 %
Tietoturvallinen salasanojen hallinta	957	28,4 %	170	28,1 %	60	27,5 %	53	29,0 %	22	37,9 %
Häiriötilanteissa toimiminen, esimerkiksi palveluiden käyttökatko	1775	52,8 %	302	49,9 %	116	53,2 %	83	45,4 %	29	50,0 %
Tietoturvapoikkeamissa toimiminen, esimerkiksi haittaohjelmaepäily	1814	53,9 %	319	52,7 %	118	54,1 %	91	49,7 %	25	43,1 %
Yleinen tieto tietoturvallisuudesta	1293	38,4 %	197	32,6 %	68	31,2 %	70	38,3 %	21	36,2 %
Yhteensä	3364		605		218		183		58	

Liite 31: Kolmaskymmenesensimmäinen liite

Tunnistautuminen työtehtäviin liittyvissä palveluissa.

Tunnistautuminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Kertakirjautumispalvelu	2356	29,0 %	285	22,6 %	160	32,9 %	239	47,3 %	75	47,2 %
Virkakortti	1633	20,1 %	252	20,0 %	107	22,0 %	157	31,1 %	75	47,2 %
Käyttäjätunnus ja salasana	6031	74,2 %	952	75,5 %	339	69,6 %	371	73,5 %	102	64,2 %

Liite 32: Kolmaskymmenestoinen liite

Salasanojen käyttö työtehtäviin liittyvissä palveluissa.

Salasanat	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Pääasiassa sama salasana	614	7,6 %	55	4,4 %	17	3,5 %	30	5,9 %	5	3,1 %
Muutama eri salasana	2680	33,0 %	438	34,7 %	173	35,5 %	151	29,9 %	31	19,5 %
Pääsääntöisesti eri salasana	2974	36,6 %	501	39,7 %	192	39,4 %	199	39,4 %	54	34,0 %
Eri salasana	1698	20,9 %	246	19,5 %	92	18,9 %	104	20,6 %	62	39,0 %
Salasanojen hallintaohjelma	157	1,9 %	21	1,7 %	13	2,7 %	21	4,2 %	7	4,4 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 33: Kolmaskymmeneskolmas liite

Riittämätön johdon tuki turvallisuudelle.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	4262	54,3 %	619	50,2 %	273	57,1 %	241	48,5 %	61	39,1 %
Vähän	2825	36,0 %	494	40,0 %	171	35,8 %	180	36,2 %	55	35,3 %
Paljon	491	6,3 %	78	6,3 %	18	3,8 %	44	8,9 %	17	10,9 %
Erittäin paljon	243	3,1 %	33	2,7 %	14	2,9 %	24	4,8 %	18	11,5 %
Uhka toteutunut	35	0,4 %	10	0,8 %	2	0,4 %	8	1,6 %	5	3,2 %
Yhteensä	7856	100,0 %	1234	100,0 %	478	100,0 %	497	100,0 %	156	100,0 %

Liite 34: Kolmaskymmenesneljäs liite

Minua ei ole koulutettu tietoturvallisuuteen riittävästi.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3319	42,3 %	475	38,8 %	191	40,4 %	258	52,2 %	83	53,9 %
Vähän	3567	45,5 %	593	48,4 %	225	47,6 %	188	38,1 %	45	29,2 %
Paljon	717	9,1 %	122	10,0 %	45	9,5 %	31	6,3 %	15	9,7 %
Erittäin paljon	220	2,8 %	33	2,7 %	11	2,3 %	14	2,8 %	10	6,5 %
Uhka toteutunut	21	0,3 %	1	0,1 %	1	0,2 %	3	0,6 %	1	0,6 %
Yhteensä	7844	100,0 %	1224	100,0 %	473	100,0 %	494	100,0 %	154	100,0 %

Liite 35: Kolmaskymmenesviides liite

Tilaturvallisuus ei ole riittävällä tasolla.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3812	48,5 %	500	40,7 %	213	44,7 %	266	53,5 %	62	39,5 %
Vähän	3004	38,2 %	555	45,1 %	203	42,6 %	171	34,4 %	59	37,6 %
Paljon	692	8,8 %	127	10,3 %	45	9,4 %	39	7,8 %	16	10,2 %
Erittäin paljon	297	3,8 %	38	3,1 %	11	2,3 %	12	2,4 %	15	9,6 %
Uhka toteutunut	62	0,8 %	10	0,8 %	5	1,0 %	9	1,8 %	5	3,2 %
Yhteensä	7867	100,0 %	1230	100,0 %	477	100,0 %	497	100,0 %	157	100,0 %

Liite 36: Kolmaskymmeneskuudes liite

Organisaationi tietoturvallisuus ei ole riittävällä tasolla.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3847	49,2 %	504	40,9 %	186	39,0 %	205	41,0 %	46	29,5 %
Vähän	3128	40,0 %	574	46,6 %	230	48,2 %	201	40,2 %	66	42,3 %
Paljon	586	7,5 %	116	9,4 %	46	9,6 %	64	12,8 %	27	17,3 %
Erittäin paljon	220	2,8 %	29	2,4 %	12	2,5 %	24	4,8 %	10	6,4 %
Uhka toteutunut	42	0,5 %	8	0,6 %	3	0,6 %	6	1,2 %	7	4,5 %
Yhteensä	7823	100,0 %	1231	100,0 %	477	100,0 %	500	100,0 %	156	100,0 %

Liite 37: Kolmaskymmenesseitsemäs liite

Työpaikalleni iskee varas, joka vie sieltä laitteita tai salassa pidettäviä tietoja.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3738	47,3 %	487	39,3 %	188	39,2 %	260	52,3 %	63	40,9 %
Vähän	3209	40,6 %	590	47,7 %	235	49,1 %	174	35,0 %	65	42,2 %
Paljon	594	7,5 %	112	9,0 %	36	7,5 %	40	8,0 %	19	12,3 %
Erittäin paljon	222	2,8 %	29	2,3 %	12	2,5 %	11	2,2 %	7	4,5 %
Uhka toteutunut	139	1,8 %	20	1,6 %	8	1,7 %	12	2,4 %	0	0,0 %
Yhteensä	7902	100,0 %	1238	100,0 %	479	100,0 %	497	100,0 %	154	100,0 %

Liite 38: Kolmaskymmeneskahdeksas liite

Työpisteessäni ei käytetä kuvallisia henkilökortteja.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5718	73,7 %	834	68,9 %	319	67,9 %	352	71,3 %	102	67,5 %
Vähän	1481	19,1 %	279	23,1 %	111	23,6 %	90	18,2 %	33	21,9 %
Paljon	314	4,0 %	62	5,1 %	30	6,4 %	32	6,5 %	4	2,6 %
Erittäin paljon	156	2,0 %	24	2,0 %	6	1,3 %	13	2,6 %	9	6,0 %
Uhka toteutunut	85	1,1 %	11	0,9 %	4	0,9 %	7	1,4 %	3	2,0 %
Yhteensä	7754	100,0 %	1210	100,0 %	470	100,0 %	494	100,0 %	151	100,0 %

Liite 39: Kolmaskymmenesyhdeksäs liite

Työtehtäviini liittyvä käyttäjätunnus ja salasana varastetaan.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	4845	61,5 %	722	58,4 %	271	56,5 %	301	60,3 %	102	67,5 %
Vähän	2548	32,3 %	437	35,4 %	185	38,5 %	161	32,3 %	33	21,9 %
Paljon	344	4,4 %	55	4,4 %	17	3,5 %	24	4,8 %	4	2,6 %
Erittäin paljon	141	1,8 %	22	1,8 %	7	1,5 %	11	2,2 %	9	6,0 %
Uhka toteutunut	4	0,1 %	0	0,0 %	0	0,0 %	2	0,4 %	3	2,0 %
Yhteensä	7882	100,0 %	1236	100,0 %	480	100,0 %	499	100,0 %	151	100,0 %

Liite 40: Neljäskymmenes liite

Minulta yritetään urkkia tai vakoilla työtehtäviini liittyviä tietoja.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5233	66,5 %	725	58,9 %	260	54,5 %	281	56,9 %	55	35,3 %
Vähän	2189	27,8 %	422	34,3 %	191	40,0 %	169	34,2 %	70	44,9 %
Paljon	312	4,0 %	57	4,6 %	19	4,0 %	32	6,5 %	22	14,1 %
Erittäin paljon	112	1,4 %	23	1,9 %	7	1,5 %	9	1,8 %	8	5,1 %
Uhka toteutunut	18	0,2 %	4	0,3 %	0	0,0 %	3	0,6 %	1	0,6 %
Yhteensä	7864	100,0 %	1231	100,0 %	477	100,0 %	494	100,0 %	156	100,0 %

Liite 41: Neljäskymmenesensimmäinen liite

Minua yritetään painostaa tai mielipiteisiini vaikuttaa työtehtäviini liittyen.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	6027	77,0 %	883	71,7 %	326	68,3 %	368	75,1 %	81	51,9 %
Vähän	1418	18,1 %	273	22,2 %	121	25,4 %	96	19,6 %	52	33,3 %
Paljon	237	3,0 %	47	3,8 %	21	4,4 %	11	2,2 %	16	10,3 %
Erittäin paljon	95	1,2 %	19	1,5 %	6	1,3 %	10	2,0 %	4	2,6 %
Uhka toteutunut	50	0,6 %	10	0,8 %	3	0,6 %	5	1,0 %	3	1,9 %
Yhteensä	7827	100,0 %	1232	100,0 %	477	100,0 %	490	100,0 %	156	100,0 %

Liite 42: Neljäskymmenestoinen liite

Identiteettini varastetaan ja sitä hyödynnetään väärinkäytöksiin.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3516	44,5 %	432	35,1 %	155	32,4 %	203	40,8 %	51	32,9 %
Vähän	3549	44,9 %	644	52,3 %	268	55,9 %	225	45,3 %	84	54,2 %
Paljon	598	7,6 %	115	9,3 %	45	9,4 %	54	10,9 %	15	9,7 %
Erittäin paljon	227	2,9 %	38	3,1 %	11	2,3 %	15	3,0 %	5	3,2 %
Uhka toteutunut	10	0,1 %	3	0,2 %	0	0,0 %	0	0,0 %	0	0,0 %
Yhteensä	7900	100,0 %	1232	100,0 %	479	100,0 %	497	100,0 %	155	100,0 %

Liite 43: Neljäskymmeneskolmas liite

Minua uhkaillaan nettipalvelussa.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5786	74,1 %	827	67,7 %	301	63,5 %	393	79,4 %	103	67,3 %
Vähän	1660	21,3 %	323	26,5 %	140	29,5 %	83	16,8 %	43	28,1 %
Paljon	252	3,2 %	54	4,4 %	27	5,7 %	14	2,8 %	5	3,3 %
Erittäin paljon	85	1,1 %	14	1,1 %	3	0,6 %	5	1,0 %	1	0,7 %
Uhka toteutunut	21	0,3 %	3	0,2 %	3	0,6 %	0	0,0 %	1	0,7 %
Yhteensä	7804	100,0 %	1221	100,0 %	474	100,0 %	495	100,0 %	153	100,0 %

Liite 44: Neljäskymmenesneljäs liite

Organisaationi menettää rahaa nettihuijausten tai kiristysten takia.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5988	77,5 %	841	69,8 %	305	64,6 %	317	64,6 %	91	59,9 %
Vähän	1479	19,1 %	307	25,5 %	154	32,6 %	139	28,3 %	53	34,9 %
Paljon	172	2,2 %	44	3,7 %	11	2,3 %	27	5,5 %	6	3,9 %
Erittäin paljon	84	1,1 %	12	1,0 %	2	0,4 %	8	1,6 %	1	0,7 %
Uhka toteutunut	2	0,0 %	1	0,1 %	0	0,0 %	0	0,0 %	1	0,7 %
Yhteensä	7725	100,0 %	1205	100,0 %	472	100,0 %	491	100,0 %	152	100,0 %

Liite 45: Neljäskymmenesviides liite

Organisaationi käyttööni antamaa luottokorttia käytetään väärin.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5845	76,0 %	859	71,4 %	281	60,2 %	352	72,1 %	82	53,9 %
Vähän	1558	20,3 %	296	24,6 %	166	35,5 %	115	23,6 %	63	41,4 %
Paljon	181	2,4 %	36	3,0 %	16	3,4 %	18	3,7 %	7	4,6 %
Erittäin paljon	92	1,2 %	9	0,7 %	3	0,6 %	3	0,6 %	0	0,0 %
Uhka toteutunut	12	0,2 %	3	0,2 %	1	0,2 %	0	0,0 %	0	0,0 %
Yhteensä	7688	100,0 %	1203	100,0 %	467	100,0 %	488	100,0 %	152	100,0 %

Liite 46: Neljäskymmeneskuudes liite

Päätelaitteeni varastetaan.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	4323	55,3 %	540	44,1 %	191	40,0 %	184	37,2 %	49	31,6 %
Vähän	2974	38,0 %	592	48,3 %	241	50,4 %	265	53,5 %	82	52,9 %
Paljon	384	4,9 %	71	5,8 %	38	7,9 %	37	7,5 %	18	11,6 %
Erittäin paljon	126	1,6 %	20	1,6 %	7	1,5 %	9	1,8 %	6	3,9 %
Uhka toteutunut	10	0,1 %	2	0,2 %	1	0,2 %	0	0,0 %	0	0,0 %
Yhteensä	7817	100,0 %	1225	100,0 %	478	100,0 %	495	100,0 %	155	100,0 %

Liite 47: Neljäskymmenesseitsemäs liite

Päätelaitteessani olevia salassa pidettäviä tietoja vuotaa ulkopuoliselle.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	4303	55,3 %	586	48,2 %	232	48,9 %	274	56,0 %	55	35,7 %
Vähän	2906	37,4 %	519	42,7 %	199	42,0 %	181	37,0 %	68	44,2 %
Paljon	399	5,1 %	80	6,6 %	36	7,6 %	26	5,3 %	18	11,7 %
Erittäin paljon	165	2,1 %	30	2,5 %	7	1,5 %	8	1,6 %	13	8,4 %
Uhka toteutunut	6	0,1 %	0	0,0 %	0	0,0 %	0	0,0 %	0	0,0 %
Yhteensä	7779	100,0 %	1215	100,0 %	474	100,0 %	489	100,0 %	154	100,0 %

Liite 48: Neljäskymmeneskahdeksas liite

Päätelaitteeseeni iskee haittaohjelma (virus tai vastaava).

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	1907	24,1 %	211	17,1 %	76	15,7 %	133	26,7 %	29	18,7 %
Vähän	4572	57,8 %	745	60,4 %	295	61,0 %	291	58,3 %	79	51,0 %
Paljon	1109	14,0 %	215	17,4 %	89	18,4 %	56	11,2 %	30	19,4 %
Erittäin paljon	305	3,9 %	57	4,6 %	23	4,8 %	17	3,4 %	16	10,3 %
Uhka toteutunut	21	0,3 %	5	0,4 %	1	0,2 %	2	0,4 %	1	0,6 %
Yhteensä	7914	100,0 %	1233	100,0 %	484	100,0 %	499	100,0 %	155	100,0 %

Liite 49: Neljäskymmenesyhdeksäs liite

Päätelaitteeni tietoturvapäivitykset eivät ole ajan tasalla.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	4434	56,8 %	630	51,4 %	230	48,3 %	303	61,0 %	69	45,1 %
Vähän	2720	34,8 %	482	39,3 %	205	43,1 %	159	32,0 %	60	39,2 %
Paljon	466	6,0 %	79	6,4 %	27	5,7 %	21	4,2 %	13	8,5 %
Erittäin paljon	171	2,2 %	32	2,6 %	12	2,5 %	13	2,6 %	10	6,5 %
Uhka toteutunut	15	0,2 %	2	0,2 %	2	0,4 %	1	0,2 %	1	0,7 %
Yhteensä	7806	100,0 %	1225	100,0 %	476	100,0 %	497	100,0 %	153	100,0 %

Liite 50: Viideskymmenes liite

Saan vahingossa tietooni salassa pidettäviä tietoja, joihin minulla ei ole oikeutta.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5281	68,0 %	799	65,5 %	322	67,9 %	296	60,3 %	90	59,2 %
Vähän	2045	26,3 %	353	28,9 %	131	27,6 %	158	32,2 %	46	30,3 %
Paljon	291	3,7 %	43	3,5 %	19	4,0 %	32	6,5 %	6	3,9 %
Erittäin paljon	97	1,2 %	12	1,0 %	1	0,2 %	5	1,0 %	4	2,6 %
Uhka toteutunut	54	0,7 %	13	1,1 %	1	0,2 %	0	0,0 %	6	3,9 %
Yhteensä	7768	100,0 %	1220	100,0 %	474	100,0 %	491	100,0 %	152	100,0 %

Liite 51: Viideskymmenesensimmäinen liite

En tiedä, kuinka henkilötietoja tulee käsitellä työtehtävissäni.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5371	69,1 %	803	66,3 %	330	70,1 %	306	61,8 %	97	62,6 %
Vähän	2138	27,5 %	370	30,5 %	130	27,6 %	164	33,1 %	47	30,3 %
Paljon	199	2,6 %	29	2,4 %	10	2,1 %	19	3,8 %	6	3,9 %
Erittäin paljon	56	0,7 %	9	0,7 %	1	0,2 %	6	1,2 %	5	3,2 %
Uhka toteutunut	6	0,1 %	1	0,1 %	0	0,0 %	0	0,0 %	0	0,0 %
Yhteensä	7770	100,0 %	1212	100,0 %	471	100,0 %	495	100,0 %	155	100,0 %

Liite 52: Viideskymmenestoinen liite

En tiedä, mitkä työtehtäviini liittyvät asiat ovat salassa pidettäviä.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5448	70,4 %	833	68,9 %	345	73,1 %	293	59,6 %	105	68,2 %
Vähän	1975	25,5 %	334	27,6 %	117	24,8 %	165	33,5 %	38	24,7 %
Paljon	246	3,2 %	34	2,8 %	8	1,7 %	26	5,3 %	7	4,5 %
Erittäin paljon	67	0,9 %	8	0,7 %	2	0,4 %	8	1,6 %	4	2,6 %
Uhka toteutunut	5	0,1 %	0	0,0 %	0	0,0 %	0	0,0 %	0	0,0 %
Yhteensä	7741	100,0 %	1209	100,0 %	472	100,0 %	492	100,0 %	154	100,0 %

Liite 53: Viideskymmeneskolmas liite

En osaa käsitellä salassa pidettäviä tietoja oikeilla työvälineillä.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5301	68,8 %	749	62,5 %	322	68,5 %	312	63,7 %	104	67,1 %
Vähän	2095	27,2 %	407	34,0 %	133	28,3 %	147	30,0 %	41	26,5 %
Paljon	253	3,3 %	37	3,1 %	14	3,0 %	25	5,1 %	7	4,5 %
Erittäin paljon	52	0,7 %	5	0,4 %	1	0,2 %	6	1,2 %	3	1,9 %
Uhka toteutunut	4	0,1 %	0	0,0 %	0	0,0 %	0	0,0 %	0	0,0 %
Yhteensä	7705	100,0 %	1198	100,0 %	470	100,0 %	490	100,0 %	155	100,0 %

Liite 54: Viideskymmenesneljäs liite

Joudun kuljettamaan ja käsittelemään salassa pidettäviä tietoja työpaikkani ulkopuolella.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5375	70,0 %	771	64,1 %	290	61,7 %	366	74,4 %	78	50,6 %
Vähän	1931	25,1 %	370	30,8 %	158	33,6 %	105	21,3 %	58	37,7 %
Paljon	290	3,8 %	47	3,9 %	15	3,2 %	19	3,9 %	14	9,1 %
Erittäin paljon	68	0,9 %	8	0,7 %	4	0,9 %	2	0,4 %	3	1,9 %
Uhka toteutunut	16	0,2 %	6	0,5 %	3	0,6 %	0	0,0 %	1	0,6 %
Yhteensä	7680	100,0 %	1202	100,0 %	470	100,0 %	492	100,0 %	154	100,0 %

Liite 55: Viideskymmenesviides liite

Etätyöskentely ei ole turvallista työpaikan ulkopuolella.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5582	72,9 %	779	64,9 %	292	62,0 %	363	73,8 %	80	51,9 %
Vähän	1776	23,2 %	370	30,8 %	159	33,8 %	110	22,4 %	56	36,4 %
Paljon	224	2,9 %	43	3,6 %	17	3,6 %	13	2,6 %	11	7,1 %
Erittäin paljon	68	0,9 %	8	0,7 %	3	0,6 %	4	0,8 %	7	4,5 %
Uhka toteutunut	7	0,1 %	1	0,1 %	0	0,0 %	2	0,4 %	0	0,0 %
Yhteensä	7657	100,0 %	1201	100,0 %	471	100,0 %	492	100,0 %	154	100,0 %

Liite 56: Viideskymmeneskuudes liite

En tiedä, miten tulee toimia häiriötilanteissa.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3927	50,7 %	575	47,7 %	248	52,3 %	299	61,1 %	91	58,7 %
Vähän	3237	41,8 %	548	45,4 %	194	40,9 %	163	33,3 %	51	32,9 %
Paljon	462	6,0 %	67	5,6 %	28	5,9 %	20	4,1 %	8	5,2 %
Erittäin paljon	107	1,4 %	14	1,2 %	4	0,8 %	6	1,2 %	5	3,2 %
Uhka toteutunut	15	0,2 %	2	0,2 %	0	0,0 %	1	0,2 %	0	0,0 %
Yhteensä	7748	100,0 %	1206	100,0 %	474	100,0 %	489	100,0 %	155	100,0 %

Liite 57: Viideskymmenesseitsemäs liite

En tiedä, mitkä ovat vastuullani tietoturvallisuuden osalta.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3927	50,7 %	701	58,3 %	283	60,0 %	317	64,4 %	107	69,9 %
Vähän	3237	41,8 %	422	35,1 %	159	33,7 %	143	29,1 %	29	19,0 %
Paljon	462	6,0 %	65	5,4 %	26	5,5 %	22	4,5 %	10	6,5 %
Erittäin paljon	107	1,4 %	12	1,0 %	3	0,6 %	9	1,8 %	5	3,3 %
Uhka toteutunut	15	0,2 %	2	0,2 %	1	0,2 %	1	0,2 %	2	1,3 %
Yhteensä	7748	100,0 %	1202	100,0 %	472	100,0 %	492	100,0 %	153	100,0 %

Liite 58: Viideskymmeneskahdeksas liite

Minulle tärkeä palvelu ei ole toiminnassa silloin kun tarvitsen sitä.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	2501	32,0 %	317	26,0 %	118	24,7 %	150	30,2 %	38	24,2 %
Vähän	3341	42,8 %	576	47,3 %	227	47,6 %	208	41,9 %	66	42,0 %
Paljon	1296	16,6 %	227	18,7 %	84	17,6 %	84	16,9 %	31	19,7 %
Erittäin paljon	381	4,9 %	58	4,8 %	31	6,5 %	34	6,8 %	14	8,9 %
Uhka toteutunut	293	3,8 %	39	3,2 %	17	3,6 %	21	4,2 %	8	5,1 %
Yhteensä	7812	100,0 %	1217	100,0 %	477	100,0 %	497	100,0 %	157	100,0 %

Liite 59: Viideskymmenesyhdeksäs liite

Työtehtäväni edellyttävät tietoturvaohjeen vastaista toimintaa.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	5995	78,5 %	916	76,8 %	367	78,4 %	352	71,4 %	93	60,8 %
Vähän	1290	16,9 %	226	18,9 %	85	18,2 %	110	22,3 %	37	24,2 %
Paljon	228	3,0 %	34	2,8 %	11	2,4 %	21	4,3 %	15	9,8 %
Erittäin paljon	71	0,9 %	11	0,9 %	2	0,4 %	6	1,2 %	6	3,9 %
Uhka toteutunut	49	0,6 %	6	0,5 %	3	0,6 %	4	0,8 %	2	1,3 %
Yhteensä	7633	100,0 %	1193	100,0 %	468	100,0 %	493	100,0 %	153	100,0 %

Liite 60: Kuudeskymmenes liite

Selaimesta tai jostain muusta ohjelmistosta aiheutuu tietoturvauhka.

Huolestuneisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Ei huolestuta	3146	40,5 %	395	32,6 %	151	31,8 %	187	37,9 %	43	27,4 %
Vähän	3674	47,3 %	660	54,4 %	259	54,5 %	238	48,2 %	80	51,0 %
Paljon	724	9,3 %	121	10,0 %	52	10,9 %	51	10,3 %	24	15,3 %
Erittäin paljon	202	2,6 %	34	2,8 %	12	2,5 %	14	2,8 %	7	4,5 %
Uhka toteutunut	25	0,3 %	3	0,2 %	1	0,2 %	4	0,8 %	3	1,9 %
Yhteensä	7771	100,0 %	1213	100,0 %	475	100,0 %	494	100,0 %	157	100,0 %

Liite 61: Kuudeskymmenesensimmäinen liite

Salassa pidettäväien tietojen luokittelu.

Luokittelu	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Kyllä	3928	48,4 %	660	52,3 %	281	57,7 %	289	57,2 %	122	76,7 %
Ei	558	6,9 %	115	9,1 %	49	10,1 %	34	6,7 %	8	5,0 %
Valmisteilla	202	2,5 %	65	5,2 %	26	5,3 %	45	8,9 %	10	6,3 %
En tiedä	3435	42,3 %	421	33,4 %	131	26,9 %	137	27,1 %	19	11,9 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 62: Kuudeskymmenestoinen liite

Osaamiseen käyttää luokittelua

Osaaminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Erittäin hyvin	440	10,9 %	63	9,3 %	27	9,4 %	25	8,5 %	27	21,8 %
Hyvin	1678	41,7 %	288	42,7 %	125	43,6 %	117	39,8 %	67	54,0 %
Tyydyttävästi	1226	30,4 %	238	35,3 %	104	36,2 %	92	31,3 %	24	19,4 %
Huonosti	327	8,1 %	58	8,6 %	16	5,6 %	31	10,5 %	5	4,0 %
Erittäin huonosti	71	1,8 %	11	1,6 %	3	1,0 %	6	2,0 %	0	0,0 %
En käsittele	285	7,1 %	16	2,4 %	12	4,2 %	23	7,8 %	1	0,8 %
Yhteensä	4027	100,0 %	674	100,0 %	287	100,0 %	294	100,0 %	124	100,0 %

Liite 63: Kuudeskymmeneskolmas liite

Palveluiden ja työkalujen käyttö salassa pidettäviin tietojen luokitteluun.

Palvelut ja työkalut	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Kyllä	4716	58,1 %	850	67,4 %	340	69,8 %	318	63,0 %	139	87,4 %
En	2027	25,0 %	288	22,8 %	97	19,9 %	81	16,0 %	16	10,1 %
En käsittele	1380	17,0 %	123	9,8 %	50	10,3 %	106	21,0 %	4	2,5 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 64: Kuudeskymmenesneljäs liite

Osaaminen.

Osaaminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Erittäin hyvin	583	12,3 %	85	10,0 %	36	10,6 %	53	16,6 %	43	30,5 %
Hyvin	2638	55,7 %	448	52,7 %	192	56,5 %	183	57,2 %	72	51,1 %
Tyydyttävästi	1384	29,2 %	285	33,5 %	104	30,6 %	80	25,0 %	22	15,6 %
Huonosti	114	2,4 %	30	3,5 %	8	2,4 %	3	0,9 %	4	2,8 %
Erittäin huonosti	15	0,3 %	2	0,2 %	0	0,0 %	1	0,3 %	0	0,0 %
Yhteensä	4734	100,0 %	850	100,0 %	340	100,0 %	320	100,0 %	141	100,0 %

Liite 65: Kuudeskymmenesviides liite

Henkilötietojen käsittely määrä.

Käsittely	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Päivittäin	4093	50,4 %	601	47,7 %	172	35,3 %	98	19,4 %	55	34,6 %
Useamman kerran viikossa	1196	14,7 %	293	23,2 %	123	25,3 %	93	18,4 %	27	17,0 %
Kerran viikossa	383	4,7 %	119	9,4 %	41	8,4 %	43	8,5 %	9	5,7 %
Kuukausittain	579	7,1 %	124	9,8 %	63	12,9 %	56	11,1 %	20	12,6 %
Harvemmin	992	12,2 %	94	7,5 %	58	11,9 %	122	24,2 %	33	20,8 %
En käsittele	880	10,8 %	30	2,4 %	30	6,2 %	93	18,4 %	15	9,4 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 66: Kuudeskymmeneskuudes liite

Tarpeellinen henkilötietojen käsittely.

Tarpeellisuus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Kyllä	5763	70,9 %	1008	79,9 %	379	77,8 %	269	53,3 %	112	70,4 %
Ei	422	5,2 %	85	6,7 %	25	5,1 %	59	11,7 %	14	8,8 %
En osaa sanoa	1403	17,3 %	150	11,9 %	71	14,6 %	139	27,5 %	31	19,5 %
En käsittele	535	6,6 %	18	1,4 %	12	2,5 %	38	7,5 %	2	1,3 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 67: Kuudeskymmenesseitsemäs liite

Soveltaminen

Soveltaminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
On ryhdytty toimenpiteisiin	1406	17,3 %	311	24,7 %	126	25,9 %	185	36,6 %	63	39,6 %
On käynnistetty/käynnistämässä hanke	857	10,6 %	178	14,1 %	91	18,7 %	107	21,2 %	35	22,0 %
Ollaan tietoisia	1239	15,3 %	264	20,9 %	120	24,6 %	75	14,9 %	20	12,6 %
En ole havainnut	2126	26,2 %	288	22,8 %	82	16,8 %	72	14,3 %	31	19,5 %
Mikä on tietosuoja-asetus	2495	30,7 %	220	17,4 %	68	14,0 %	66	13,1 %	10	6,3 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 68: Kuudeskymmeneskahdeksas liite

Työskentely toimipaikan ulkopuolella.

Salliminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Kyllä	6230	76,7 %	1068	84,7 %	455	93,4 %	481	95,2 %	145	91,2 %
Ei	1199	14,8 %	122	9,7 %	19	3,9 %	15	3,0 %	7	4,4 %
En tiedä	694	8,5 %	71	5,6 %	13	2,7 %	9	1,8 %	7	4,4 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 69: Kuudeskymmenesyhdeksäs liite

Hyödyntäminen.

Hyödyntäminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Useana päivänä viikossa	1314	20,8 %	202	18,7 %	114	25,0 %	105	21,8 %	21	14,4 %
Keskimäärin päivän viikossa	752	11,9 %	106	9,8 %	47	10,3 %	79	16,4 %	27	18,5 %
Epäsäännöllisesti, kuitenkin kuukausittain	1358	21,5 %	318	29,4 %	134	29,4 %	126	26,2 %	51	34,9 %
Harvoin, muutaman kerran vuodessa	1183	18,7 %	251	23,2 %	101	22,1 %	89	18,5 %	26	17,8 %
En hyödynnä	1711	27,1 %	204	18,9 %	60	13,2 %	82	17,0 %	21	14,4 %
Yhteensä	6318	100,0 %	1081	100,0 %	456	100,0 %	481	100,0 %	146	100,0 %

Liite 70: Seitsemäskymmenes liite

Ohjeistus työskentelyyn toimipaikan ulkopuolella.

Ohjeistus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Kyllä	3153	38,8 %	600	47,6 %	279	57,3 %	333	65,9 %	106	66,7 %
Ei	1372	16,9 %	251	19,9 %	99	20,3 %	74	14,7 %	25	15,7 %
En työskentele työpaikan ulkopuolella	2017	24,8 %	203	16,1 %	49	10,1 %	45	8,9 %	17	10,7 %
En osaa sanoa	1581	19,5 %	207	16,4 %	60	12,3 %	53	10,5 %	11	6,9 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 71: Seitsemäskymmenesensimmäinen liite

Toimiminen ohjeistuksen mukaisesti

Toimiminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Erittäin hyvin	1557	49,0 %	258	42,9 %	126	45,2 %	184	54,6 %	56	52,3 %
Hyvin	1490	46,9 %	313	52,0 %	137	49,1 %	142	42,1 %	50	46,7 %
Tyydyttävästi	127	4,0 %	31	5,1 %	16	5,7 %	10	3,0 %	1	0,9 %
Huonosti	4	0,1 %	0	0,0 %	0	0,0 %	1	0,3 %	0	0,0 %
Erittäin huonosti	0	0,0 %	0	0,0 %	0	0,0 %	0	0,0 %	0	0,0 %
Yhteensä	3178	100,0 %	602	100,0 %	279	100,0 %	337	100,0 %	107	100,0 %

Liite 72: Seitsemäskymmenestoinen liite

Työnantajan laitteella lukeminen.

Lukeminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Päivittäin	2377	29,3 %	654	51,9 %	287	58,9 %	182	36,0 %	80	50,3 %
Arkipäivisin	5024	61,8 %	573	45,4 %	185	38,0 %	312	61,8 %	75	47,2 %
Muutaman kerran viikossa	390	4,8 %	15	1,2 %	7	1,4 %	5	1,0 %	2	1,3 %
Muutaman kerran kuukaudessa	94	1,2 %	4	0,3 %	2	0,4 %	2	0,4 %	0	0,0 %
Muutaman kerran vuodessa	198	2,4 %	3	0,2 %	1	0,2 %	1	0,2 %	0	0,0 %
En lue	722	8,9 %	131	10,4 %	5	1,0 %	3	0,6 %	2	1,3 %

Liite 73: Seitsemäskymmeneskolmas liite

Henkilökotaisella laitteella lukeminen.

Lukeminen	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Päivittäin	722	8,9 %	11	0,9 %	51	10,5 %	32	6,3 %	5	3,1 %
Arkipäivisin	155	1,9 %	69	5,5 %	6	1,2 %	9	1,8 %	3	1,9 %
Muutaman kerran viikossa	464	5,7 %	124	9,8 %	25	5,1 %	20	4,0 %	4	2,5 %
Muutaman kerran kuukaudessa	548	6,7 %	111	8,8 %	33	6,8 %	25	5,0 %	4	2,5 %
Muutaman kerran vuodessa	805	9,9 %	815	64,6 %	42	8,6 %	51	10,1 %	10	6,3 %
En lue	5429	66,8 %	755	59,9 %	330	67,8 %	368	72,9 %	133	83,6 %

Liite 74: Seitsemäskymmenesneljäs liite

Tietoturvallisuuden merkityksen kokeminen.

Merkitys	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Lisää laatua ja luotettavuutta	4731	58,2 %	755	59,9 %	296	60,8 %	358	70,9 %	113	71,1 %
Tarpeellinen	2892	35,6 %	430	34,1 %	167	34,3 %	109	21,6 %	40	25,2 %
Ymmärrän	484	6,0 %	75	5,9 %	23	4,7 %	37	7,3 %	6	3,8 %
Riesa	16	0,2 %	1	0,1 %	1	0,2 %	1	0,2 %	0	0,0 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 75: Seitsemäskymmenesseitsemäs liite

Tietoturvallisuuden toteutuminen.

Toteutus	Kaikki	%	Esimiehet	%	Johtoryhmä	%	Tietohallinto	%	Tietoturva	%
Erittäin hyvin	1528	18,8 %	209	16,6 %	84	17,2 %	109	21,6 %	30	18,9 %
Hyvin	5852	72,0 %	946	75,0 %	368	75,6 %	339	67,1 %	102	64,2 %
Huonosti	698	8,6 %	102	8,1 %	34	7,0 %	53	10,5 %	23	14,5 %
Erittäin huonosti	45	0,6 %	4	0,3 %	1	0,2 %	4	0,8 %	4	2,5 %
Yhteensä	8123	100,0 %	1261	100,0 %	487	100,0 %	505	100,0 %	159	100,0 %

Liite 76: Seitsemäskymmeneskuudes liite

Itselläni ja organisaationi muulla johdolla on tietoturvallisuuteen tarvittava osaaminen.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,65	2,53	2,91
Esimiehet	3,67	2,60	2,89
Johtoryhmä	3,65	2,53	2,91
Ero	0,02	0,07	-0,02

Liite 77: Seitsemäskymmenesseitsemäs liite

Organisaation tietoturvatehtävät on organisoitu ja vastuut määritetty.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,64	2,42	2,83
Esimiehet	3,70	2,49	2,89
Johtoryhmä	3,64	2,42	2,86
Ero	0,06	0,07	0,03

Liite 78: Seitsemäskymmeneskahdeksas liite

Tiedonkulku organisaation sisällä toimii.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,58	2,64	2,72
Esimiehet	3,65	2,71	2,72
Johtoryhmä	3,58	2,64	2,72
Ero	0,07	0,07	0

Liite 79: Seitsemäskymmenesyhdeksäs liite

Organisaation käytettävissä oleva tietoturvaosaaminen on riittävän korkeatasoista.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,77	2,73	2,9
Esimiehet	3,72	2,73	2,83
Johtoryhmä	3,77	2,73	2,90
Ero	-0,05	0	-0,07

Liite 80: Kahdeksaskymmenes liite

Organisaatio saa johtamisen tueksi riittävästi tietoa tietoturvallisuuden osalta.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,57	2,55	2,77
Esimiehet	3,62	2,63	2,85
Johtoryhmä	3,57	2,55	2,77
Ero	0,05	0,08	0,08

Liite 81: Kahdeksaskymmenesensimmäinen liite

Tietoturvapoikkeamien ja häiriötilanteiden toimintamalli on määritelty ja toiminnassa.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,67	2,55	2,74
Esimiehet	3,66	2,67	2,67
Johtoryhmä	3,67	2,55	2,74
Ero	-0,01	0,12	-0,07

Liite 82: Kahdeksaskymmenestoinen liite

Riskienhallinta organisaation eri tasoilla on toimivaa.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,58	2,68	2,62
Esimiehet	3,61	2,74	2,63
Johtoryhmä	3,58	2,68	2,62
Ero	0,03	0,06	0,01

Liite 83: Kahdeksaskymmeneskolmas liite

Organisaation sopimuksissa on tietoturvallisuus huomioitu vaadittavalla tasolla.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,62	2,58	2,79
Esimiehet	3,65	2,65	2,81
Johtoryhmä	3,62	2,58	2,79
Ero	0,03	0,07	0,02

Liite 84: Kahdeksaskymmenesneljäs liite

Organisaatio ilmoittaa tietoturvapoikkeamista Viestintävirastossa toimivalle Kyberturvallisuuskeskukselle.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,48	2,33	2,69
Esimiehet	3,55	2,42	2,61
Johtoryhmä	3,48	2,33	2,69
Ero	0,07	0,09	-0,08

Liite 85: Kahdeksaskymmenesviides liite

Tietoturvapoikkeamista viestiminen on suunniteltu ja vastuutettu.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,56	2,41	2,76
Esimiehet	3,61	2,49	2,74
Johtoryhmä	3,56	2,41	2,76
Ero	0,05	0,08	-0,02

Liite 86: Kahdeksaskymmeneskuudes liite

Organisaatio toteuttaa riittävän määrän tietoturva-auditointeja ja muita tarkastuksia

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,44	2,59	2,55
Esimiehet	3,46	2,60	2,50
Johtoryhmä	3,44	2,59	2,55
Ero	0,02	0,01	-0,05

Liite 87: Kahdeksaskymmenesseitsemäs liite

Tekninen tietoturvallisuus on riittävän hyvällä tasolla estämään keskeisimpien tietoturvauhkien toteutumisen.

Sektori	Tärkeys	Vaikeus	Toteutuminen
Kaikki	3,79	2,63	2,99
Esimiehet	3,76	2,67	3,02
Johtoryhmä	3,79	2,63	2,99
Ero	-0,03	0,04	0,03

Liite 88: Kahdeksaskymmeneskahdeksas liite

Henkilöstön ja johdon tietoturvabarometrin kysymykset

1.1 Toimenkuvani: Henkilöstö

Valitse, jos kuulut lisäksi seuraaviin ryhmiin

- Esimies
- johtoryhmän jäsen

1.2 Ensisijainen työtehtäväni liittyy seuraaviin asioihin

- hallinto
- tietohallinto ja/tai ICT
- tietoturva, tietosuoja, kyberturvallisuus tai vastaava turvallisuusalan tehtävä
- tutkimus
- opetus
- sosiaali- ja terveystoimi
- jokin muu

2.1 Millä laitteilla hoidat työtehtäviäsi – valitse kaikki käyttämäsi päätelaitteet

- työnantajan kannettavalla tietokoneella
- työnantajan pöytätietokoneella
- työnantajan tabletilla
- työnantajan älypuhelimella
- työnantajan ajoneuvotietokoneella
- omalla kannettavalla tietokoneella
- omalla pöytätietokoneella
- omalla tabletilla
- omalla älypuhelimella
- jollain muulla laitteella
    - millä?

2.2 Miten turvalliseksi koet päivittäisen työskentelysi?

- hyvin turvalliseksi
- turvalliseksi
- jonkin verran turvattomaksi
- hyvin turvattomaksi
- en ole miettinyt asiaa

2.3 Mihin seuraavista olet saanut omasta mielestäsi riittävästi ohjeita ja koulutusta? Valitse yksi rasti ohjeistusta koskien ja yksi rasti koulusta koskien.
vastaus vaihtoehdot: olen saanut ohjeita, en ole saanut ohjeita, työtehtävistäni johtuen en tarvitse ohjeita. Olen saanut koulutusta, en ole saanut koulutusta, työtehtävistäni johtuen en tarvitse koulutusta.

- tietoturvaperehdytys työsuhteeni alkaessa
- turvallinen toiminta organisaation toimitiloissa
- etätyöskentely tai työskentely toimipaikan ulkopuolella
- tietojen luokittelu
- henkilötietojen käsittely ja tietosuoja
- salassa pidettävän tietoaineiston käsittely
- tiedostojen salaaminen

- mobiililaitteiden käyttö
- sähköpostin käyttö
- internetin käyttö
- sosiaalisen median käyttö
- tietoturvallinen salasanojen hallinta
- häiriötilanteissa toimiminen, esimerkiksi palveluiden käyttökatko
- tietoturvapoikkeamissa toimiminen, esimerkiksi haittaohjelmaepäily
- yleinen tieto tietoturvallisuudesta

    - Tarvitsetko lisäohjeistus tai -koulutusta?

        - kyllä
        - en

    - Mihin seuraavista tarvitset lisäkoulutusta tai ohjeistusta

        - tietoturvaperehdytys työsuhteeni alkaessa
        - turvallinen toiminta organisaation toimitiloissa
        - etätyöskentely tai työskentely toimipaikan ulkopuolella
        - tietojen luokittelu
        - henkilötietojen käsittely ja tietosuoja
        - salassa pidettävän tietoaineiston käsittely
        - tiedostojen salaaminen
        - mobiililaitteiden käyttö
        - sähköpostin käyttö
        - internetin käyttö
        - sosiaalisen median käyttö
        - tietoturvallinen salasanojen hallinta
        - häiriötilanteissa toimiminen, esimerkiksi palveluiden käyttökatko
        - tietoturvapoikkeamissa toimiminen, esimerkiksi haittaohjelmaepäily
        - yleinen tieto tietoturvallisuudesta

2.4 Tunnistaminen ja salasanat

2.4.1 Millaista tunnistautumista ensisijaisesti käytät työasemaasi kirjautumisessa?

- virkakorttiin perustuvaa kirjautumista
- käyttäjätunnusta ja salasanaa
- biometristä tunnistusta (esimerkiksi sormenjälki tai kasvot)
- jotain muuta
    - mitä?

2.4.2 Millaista tunnistautumista käytät työtehtäviisi liittyvissä palveluissa?

- organisaationi käyttää kertakirjautumispalvelua esimerkiksi valtionhallinnossa Virtu
- organisaationi käyttää virkakorttiin perustuvaa kirjautumista
- tunnistaminen perustuu käyttäjätunnuksiin ja salasanoihin

2.4.3 Millaisia salasanoja käytät työtehtäviisi liittyvissä palveluissa?

- käytän kaikissa palveluissa pääasiassa samaa salasanaa
- käytän muutamaa eri salasanaa kaikissa palveluissa

- käytän pääsääntöisesti eri salasanaa eri palveluissa
- käytän eri salasanaa jokaisessa palvelussa
- käytän työnantajan tarjoamaa salasanojen hallintaohjelmaa

2.5 Mitkä turvallisuuteen liittyvät asiat huolestuttavat sinua eniten työtehtäviä hoitaessasi? Onko uhka toteutunut viimeisen kahden vuoden aikana? Valitse seuraavista. Voit arvioida kaikkia kohteita.
1. asia ei huolestuta minua lainkaan
2. asia huolestuttaa vain vähän
3. asia huolestuttaa paljon
4. asia huolestuttaa erittäin paljon
X uhka on toteutunut

- riittämätön johdon tuki turvallisuudelle
- riittämätön johdon tuki tietoturvallisuudelle
- riittämätön johdon tuki tietosuojalle
- minua ei ole koulutettu tietoturvallisuuteen riittävästi
- toimipaikkani tilaturvallisuus ei ole riittävällä tasolla
- organisaationi tietoturvallisuus ei ole riittävällä tasolla
- työpaikalleni iskee varas, joka vie sieltä laitteita tai salassa pidettäviä tietoja
- toimipisteessäni ei käytetä kuvallisia henkilökortteja
- työtehtäviini liittyvä käyttäjätunnus ja salasana varastetaan
- minulta yritetään urkkia tai vakoilla työtehtäviini liittyviä tietoja
- minua yritetään painostaa tai mielipiteisiini vaikuttaa työtehtäviini liittyen
- identiteettini varastetaan ja sitä hyödynnetään väärinkäytöksiin
- minua uhkaillaan nettipalvelussa
- organisaationi menettää rahaa nettihuijauksen tai kiristyksen takia
- organisaationi käyttööni antamaa luottokorttia käytetään väärin
- päätelaitteeni varastetaan
- päätelaitteessani olevia salassa pidettäviä tietoja vuotaa ulkopuolisille
- päätelaitteeseeni iskee haittaohjelma (virus tai vastaava)
- päätelaitteeni tietoturvapäivitykset eivät ole ajan tasalla
- menetän tärkeitä tietoja laiterikon takia
- saan vahingossa tietooni salassa pidettäviä tietoja, joihin minulle ei ole oikeutta
- en tiedä, kuinka henkilötietoja tulee käsitellä työtehtävissäni
- en tiedä, mitkä työtehtäviini liittyvät asiat ovat salassa pidettäviä
- en osaa käsitellä salassa pidettäviä tietoja oikeilla työvälineillä
- joudun kuljettamaan ja käsittelemään salassa pidettäviä tietoja työpaikkani ulkopuolella
- etätyöskentely ei ole turvallista työpaikan ulkopuolella
- en tiedä, miten tulee toimia häiriötilanteissa
- en tiedä, mitkä ovat vastuuni tietoturvallisuuden osalta
- minulle tärkeä palvelu ei ole toiminnassa silloin kun tarvitsen sitä
- työtehtäväni edellyttävät tietoturvaohjeiden vastaista toimintaa
- selaimesta tai jostain muusta ohjelmistosta aiheutuu tietoturvauhka

3.1 Onko organisaatiossasi ohjeistus salassa pidettävien tietojen luokitteluun?
- kyllä
- ei
- valmisteilla

- en tiedä

    - kuinka hyvin osaat käyttää tätä luokittelua?
        - erittäin hyvin
        - hyvin
        - tyydyttävästi
        - huonosti
        - erittäin huonosti
        - en käsittele salassa pidettävää aineistoa

3.2 Tiedätkö, miten eri palveluita ja työkaluja tulee käyttää salassa pidettävien tietojen käsittelyssä, esimerkiksi millä salassa pidettäviä tietoja saa lähettää ja minne ne saa tallentaa?

- kyllä
- en
- en käsittele salassa pidettävää aineistoa

    - osaat käyttää eri palveluita ja työkaluja salassa pidettävien tietojen käsittelyyn
        - erittäin hyvin
        - hyvin
        - tyydyttävästi
        - huonosti
        - erittäin huonosti

3.3 Kuinka usein käsittelet työssäsi henkilötietoja?

- päivittäin
- useamman kerran viikossa
- kerran viikossa
- kuukausittain
- harvemmin
- en käsittele henkilötietoja

3.4 Käsitelläänkö organisaatiossa näkemyksesi mukaan vain tarpeellisia henkilötietoja?

- Kyllä, käsitellään ainoastaan käsittelyn tarkoituksen kannalta tarpeellisia tietoja
- Ei, tiedossani on, että organisaatiossani käsitellään, esim. varmuuden vuoksi, myös sellaisia henkilötietoja, jotka eivät mielestäni olisi toiminnassa tarpeen
- En osaa sanoa, käsitelläänkö tarpeellisia vai tarpeettomia henkilötietoja
- En käsittele lainkaan henkilötietoihin liittyviä asioita

3.5 Miten tietosuoja-asetukseen, joka aletaan soveltaa 25.5.2018, on organisaatiossasi valmistauduttu?

- Organisaationi on jo ryhtynyt toimenpiteisiin, joita tietosuoja-asetuksen on arvioitu edellyttävän
- Organisaatiossa on käynnistetty tai ollaan aikeissa käynnistää hanke tai hankkeita, jotka tähtäävät siihen, että tietosuoja-asetukseen oltaisiin valmiita
- Organisaatiossa ollaan tietoisia tietosuoja-asetuksesta ja sen aikataulusta. Toistaiseksi on huolehdittu siitä, että toiminta vastaa nykylainsäädäntöä (henkilölaki ja erityislainsäädäntö)
- En ole havainnut, että organisaatiossa olisi ryhdytty toimenpiteisiin
- Mikä on tietosuoja-asetus? Mihin se liittyy?

3.6 Keneltä organisaatiossasi voit kysyä tietosuoja-asioista?

- Olen se henkilö, jolta muut voivat kysyä
- En ole kuvattu henkilö, mutta tiedän, keneltä voin kysyä
- Organisaatiossani on todennäköisesti määritelty tuollainen henkilö, mutta en ole varma, kuka hän on
- En tiedä keneltä kysyä

4.1 Salliiko organisaatiosi työskentelyn oman toimipaikan ulkopuolella?

- Kyllä
    - Hyödynnät tätä kyselyä
        - useana päivänä viikossa
        - keskimäärin päivän viikossa
        - epäsäännöllisesti, kuitenkin kuukausittain
        - harvoin, muutaman kerran vuodessa
        - en hyödynnä
- Ei
- En tiedä

4.2 Onko työskentelyä toimipaikan ulkopuolella ohjeistettu riittävästi myös tietoturvallisuuden näkökulmasta?

- Kyllä
    - Pystytkö toimimaan tämän ohjeistuksen mukaisesti
        - erittäin hyvin
        - hyvin
        - tyydyttävästi
        - huonosti
        - erittäin huonosti
- Ei
- En työskentele toimipaikan ulkopuolella
- En osaa sanoa

4.3 Luetko organisaatiosi sähköpostia? Työnantajan käyttöösi antamilla työvälineillä

- Päivittäin myös viikonloppuisin
- Arkipäivisin
- Muutaman kerran viikossa
- Muutaman kerran kuukaudessa
- Muutaman kerran vuodessa
- En lue

Luetko organisaatiosi sähköpostia? Omilla vapaa-ajan laitteillasi?

- Päivittäin myös viikonloppuisin
- Arkipäivisin
- Muutaman kerran viikossa
- Muutaman kerran kuukaudessa
- Muutaman kerran vuodessa
- En lue

5.1 Millaisena koet tietoturvallisuuden merkityksen omassa työssäsi?

- Tietoturvallisuus mahdollistaa laadukkaan toiminaan ja antaa organisaatiostani luotettavan kuvan
- Tietoturvallisuutta tarvitaan, jotta voin käsitellä työssäni tarvitsemiani tietoja

- Ymmärrän, miksi tietoturvallisuutta tarvitaan, mutta se aiheuttaa ylimääräistä työtä
- Tietoturvallisuus on jatkuva riesa, en ymmärrä mihin sitä tarvitaan
    - Perustele vastauksesi

5.2 Miten koet, että tietoturvallisuus on toteutettu organisaatiossasi? Tietoturvallisuus toteutuu mielestäni

- Erittäin hyvin
- Hyvin
- Huonosti
- Erittäin huonosti
    - Perustele vastauksesi?

5.3 Miten arvioit seuraavien osa-alueiden tärkeyden, haasteellisuuden ja toteutumisen omassa organisaatiossasi?
Tärkeys:
4. Erittäin tärkeä
3. Tärkeä
2. Ei niin tärkeä
1. Ei lainkaan tärkeä
0. En osaa arvioida
Vaikeus:
4. Erittäin vaikea
3. Vaikea
2. Kohtalaisen helppo
1. Erittäin helppo
0. En osaa arvioida
Toteutuminen
4. Erittäin hyvin
3. Hyvin
2. Huonosti
1. Hyvin huonosti
0. En osaa arvioida

- Johto on sitoutunut tietoturvallisuuden toteuttamiseen
- Johto on sitoutunut tietosuojan toteuttamiseen
- Johto tietää mistä toimintaa koskevat tietoturvavaatimukset tulevat
- Itselläni ja organisaationi muulla johdolla on tietoturvallisuuteen tarvittava osaaminen
- Organisaationi käytössä ovat tietoturvallisuuteen tarvittavat henkilöstö- ja talousresurssit
- Organisaation käytettävissä oleva tietoturvaosaaminen on riittävän korkeatasoista
- Organisaation tietoturvatehtävät on organisoitu ja vastuut on määritelty
- Henkilöstö noudattaa tietotuvallisuutta koskevia ohjeita
- Tiedonkulku organisaation sisällä toimii ja organisaation ylin johto saa turvallisuudesta tietoa, jalostettua informaatiota ja analyysiä
- Organisaatio saa johtamisen tueksi riittävästi tietoa tietoturvallisuuden tilasta
- Tietoturvapoikkeamien ja häiriötilanteiden toimintamalli on määritelty ja toiminnassa
- Häiriötilanteiden hallintaa harjoitellaan riittävästi
- Riskienhallinta organisaation eri tasoilla on toimivaa
- Organisaation sopimuksissa on tietoturvallisuus huomioitu vaadittavalla tasolla

- Organisaatio ilmoittaa tietoturvapoikkeamista Viestintävirastossa toimivalle Kyberturvallisuuskeskukselle
- Tietoturvapoikkeamista viestiminen on suunniteltu ja vastuutettu
- Organisaatio toteuttaa riittävän määrän tietoturva-auditointeja ja muita tarkastuksia
- Tekninen tietoturvallisuus on riittävän hyvällä tasolla estämään keskeisimpien tietoturvauhkien toteutumisen

5.4 Miten organisaatiosi tietoturvallisuutta voitaisiin kehittää?
Vastausohje: Älä kohdista palautetta yksittäisiin henkilöihin!
6.1 Miten toivoisit organisaatioisi tietoturvallisuutta kehitettävän
6.2 Mitä olet itse tehnyt tietoturvallisuuden parantamiseksi organisaatioissasi?
6.3 Palaute kyselystä?