



Tiedon suojaamisen kehittäminen hybridityössä case yritys X

Anne Koskela-Laakso

2024 Laurea



Laurea-ammattikorkeakoulu

Tiedon suojaamisen kehittäminen hybridityössä case yritys X

Anne Koskela-Laakso
Turvallisuus ja riskienhallinta
Opinnäytetyö
Huhtikuu, 2024

Opinnäytetyön tavoitteena oli kehittää yritys X:n tietoturvallisuuden tasoa työskentelysijainnista riippumatta. Tiedon lähteeksi valittiin yrityksen työntekijät, jotka saivat anonyymisti esittää oman subjektiivisen kokemuksensa yritys X:n tarjoamista ohjeista ja koulutuksista tiedon turvaamiseen ja tietoturvallisuuteen sekä tietoturvaan liittyen.

Hybridityön luonne on olla osittain paikka- ja jopa aikariippumatonta. Tämä on enenevässä määrin erityisesti tietotyön suorittamiseen tapahtuvan muutoksen primus motor. Tiedon suojaaminen laajana käsitteenä on syytä ottaa huomioon erityisellä herkkyydellä, koska suljettujen toimisto-olosuhteiden sijaan haasteita tiedon suojaamiseen tuo monimuotoisemmat olosuhteet.

Case-yrityksen tiedon suojaamisen osaamisen kokemuksen nykytila selvitettiin teemahaastatteluilla ja ryhmäkeskusteluilla, joiden vastaukset analysoitiin laadullisesti. Saatujen tulosten perusteella tehtiin kehitysehdotuksia caseyrityksen käytäntöihin sekä työntekijöille tarjottaviin tietoturvakoulutuksiin. Yritys X:n poikkeuksellisen sensitiivisestä toimialasta johtuen tiedon suojaaminen on korostetun merkityksellisessä asemassa niin asiakkaille koituvan potentiaalisen haitan kuin yrityksen maineen ja toimintaedellytystenkin vuoksi. Huolimatta siitä, että tämä kehitystyö tehtiin yhdelle nimenomaiselle organisaatiolle, ovat sen tulokset potentiaalisesti hyödynnettävissä muissakin organisaatioissa.

Opinnäytetyössä esitetty tietopohja antaa opinnäytetyön käsittekartalle merkityksen ja yhdistää sen organisaation tietoturvallisuuspolitiikkaan ja sitä kautta käytännön työelämään. Kiihtyvällä tahdilla, ympäristötekijöiden osin pakottamana, toimistotyön luonne on muuttunut ja monipaikkaisuus sekä hybridityö ovat tuoneet uudenlaisia haasteita myös tiedon suojaamiseen ja tietoturvallisuuteen.

Kehitystyöhön liittyvien selvitysten perusteella kävi ilmi, että jokapäiväisessä työssä työntekijät kohtasivat haasteita, joihin yritys X:n tarjoamat tiedon suojaamista koskevat koulutukset eivät suoraan antaneet vastausta. Yleinen tietoturvallisuusosaamisen taso oli hyvä, mutta käytännönläheisempää ohjausta jäätii kaipaamaan. Merkityksellisin esiinnoussut seikka oli, ettei kaikilla työntekijöille ollut selvää, miten ja mistä tarkempia toimintaohjeita saa.

Asiasanat: hybridityö, tiedonsuojaaminen, tietoturvallisuus

The objective of the thesis was to enhance the level of information security at Company X regardless of the working location. The source of information chosen was the company's employees, who were anonymously invited to provide their subjective experiences regarding the guidelines and training provided by Company X on information security and data protection.

The nature of hybrid work is to be location-independent and sometimes time-independent. This is increasingly the driving force behind the changes in how knowledge work is performed. Protecting information as a broad concept should be approached with particular sensitivity, as the challenges of safeguarding information in diverse conditions surpass those of closed office environments.

The current state of knowledge and experience regarding information security at the case company was investigated through thematic interviews and group discussions, the responses of which were qualitatively analysed. Based on the obtained results, development suggestions were made for the practices of the case company and the information security training provided to employees. Due to the exceptionally sensitive nature of Company X's industry, safeguarding information holds heightened significance, both due to potential harm to customers and the reputation and operational requirements of the company. Despite the fact that this development work being conducted for a specific organization, its results have potential applicability in other organizations as well.

The theoretical frame presented in the thesis provides significance to the concept map of the thesis and connects it to the organization's information security policy, thereby linking it to practical working life. With the rapidly changing nature of work, partly driven by environmental factors, the nature of office work has evolved, and multi-location and hybrid work have brought about new challenges in information security and data protection. Based on the findings of the thesis, it became apparent that employees encountered challenges in their daily work for which the information security training provided by Company X did not directly provide answers. While the general level of information security competence was sufficient, more practical guidance was desired. The most significant issue raised was that not all employees were clear on how and where to obtain more detailed operating instructions.

Keywords: hybridwork, informationprotection,informationsecurity

Sisällys

| | | |
|-------|--|----|
| 1 | Johdanto..... | 6 |
| 2 | Hybridityö ja tiedon suojaaminen | 7 |
| 2.1 | Kehittyvä työ | 8 |
| 2.2 | Tiedon suojaaminen | 10 |
| 2.2.1 | Organisaation kokonaisturvallisuuden yhteys tiedon suojaamiseen hybridityössä..... | 11 |
| 2.2.2 | Standardit, asetukset ja lait ohjaamassa toimintaa..... | 11 |
| 2.2.3 | Yritysturvallisuusmalli ja jatkuva työ..... | 12 |
| 2.2.4 | Viestinnän luottamuksellisuus | 14 |
| 2.3 | Tieto- ja viestintäsektorin erityispiirteet..... | 15 |
| 3 | Kehittämistyön toteutus..... | 16 |
| 3.1 | Kehittämistyön aineistonkeruumenetelmät | 17 |
| 3.1.1 | Haastattelut ja ryhmäkeskustelut..... | 17 |
| 3.1.2 | Kohderyhmä | 19 |
| 3.1.3 | Toteutusmenetelmät..... | 19 |
| 3.2 | Kerätyn aineiston käsittely | 20 |
| 3.3 | Kehittämistyön tavoitteet ja riskit | 21 |
| 4 | Lähtökohdista tuloksiin..... | 21 |
| 4.1 | Lähtökohdat ja etukäteisoletukset | 22 |
| 4.2 | Tulokset | 22 |
| 5 | Johtopäätökset ja kehittämissuositukset | 23 |
| 6 | Pohdintaa opinnäytetyöhön liittyen | 25 |
| | Lähteet..... | 27 |
| | Kuviot | 30 |
| | Liitteet | 31 |

1 Johdanto

Tiedon suojaaminen liittyy keskeisesti turvallisuuteen ja asettuu omalle paikalleen siinä viitekehyksessä. Hybridityö on puolestaan yleistynyt tapa tehdä asiantuntijatyötä, mutta monissa organisaatioissa se on vielä tuore ja siihen liittyvien käytänteiden muodostuminen on prosessinsa alkuvaiheessa (Työterveyslaitos 2022). Tiedon suojaaminen hybridityössä -otsikko sisältää jo itsessään vaikeita käsitteitä. Kun näitä yksittäisiä käsitteitä - tiedon suojaaminen ja hybridityö - lähdetään tarkastelemaan paremmin, päädytään monimutkaiseen käsitteiden kokonaisuuteen. Huolimatta siitä esiintyvätkö nämä käsitteet erillään tai yhdessä, on syytä avata opinnäytetyön kannalta olennaisten käsitteiden sisältöä sekä niihin liittyviä riippuvuussuhteita ja myös niitä ympäröivää viitekehystä sekä sitä, miten nämä termit yhdistyvät konkretiaan työelämässä.

Erityisesti näin maailmanlaajuisen pandemian jälkimainingeissa on jouduttu ja mahdollisesti vieläkin joudutaan siirtymään toimistoilta eristyneempiin työntekopaikkoihin pahimmillaan äärimmäisen nopeallakin aikataululla. Yrityksen riskienhallinnan ja toiminnan jatkuvuuden varmistamisen kannalta on hyvä olla varautunut erilaisiin skenaarioihin. Pandemian suvantovaiheessa oli hyvä hetki ja ajankohtaista tarkastella vallitsevaa nykytilaa kehittämismielessä ja yhteiskunta lienee oppinut koetusta pandemiasta varautumisen merkityksen aiempaa laajemmassa spektrissä.

Kun opinnäytetyön otsikon käsitteisiin lisätään vielä kehittämisen kohteena olevan yritys X:n toimialan erityispiirteet, käsitemaailma laajenee edelleen. Kokonaiskuvan hahmottamiseksi opinnäytetyön teoriaosuudessa edetään otsikon sanajärjestyksen ohjaamana seemiläiseen tapaan oikealta vasemmalle ja esitellään myös toimialasektorin vaikutus tähän case-tapaukseen. Erityisesti tieto- ja viestintäsektorilla toimivalle yritykselle asiakkaan luottamus tietojen turvalliseen käsittelyyn on äärimmäisen tärkeä organisaation toiminnan kannalta. Mikäli tämä luottamus menetetään, ei yrityksen toiminnalle ole jatkumisen edellytyksiä. Siksi jokaisen työntekijän tulee huomioida myös tämä teoria asiakkuustietoja käsitellessään. Organisaation tehtävä on integroida tämä teoria käytännön prosesseihin ja yrityksen arvoihin siten, ettei työntekijän tarvitse jokaisen uuden asiakaskohtaamisen yhteydessä perehtyä tähän regulaatioon vaan prosessin mukaan toimiessaan hänkin voi luottaa toimivansa tiedon suojaamisen periaatteiden mukaisesti.

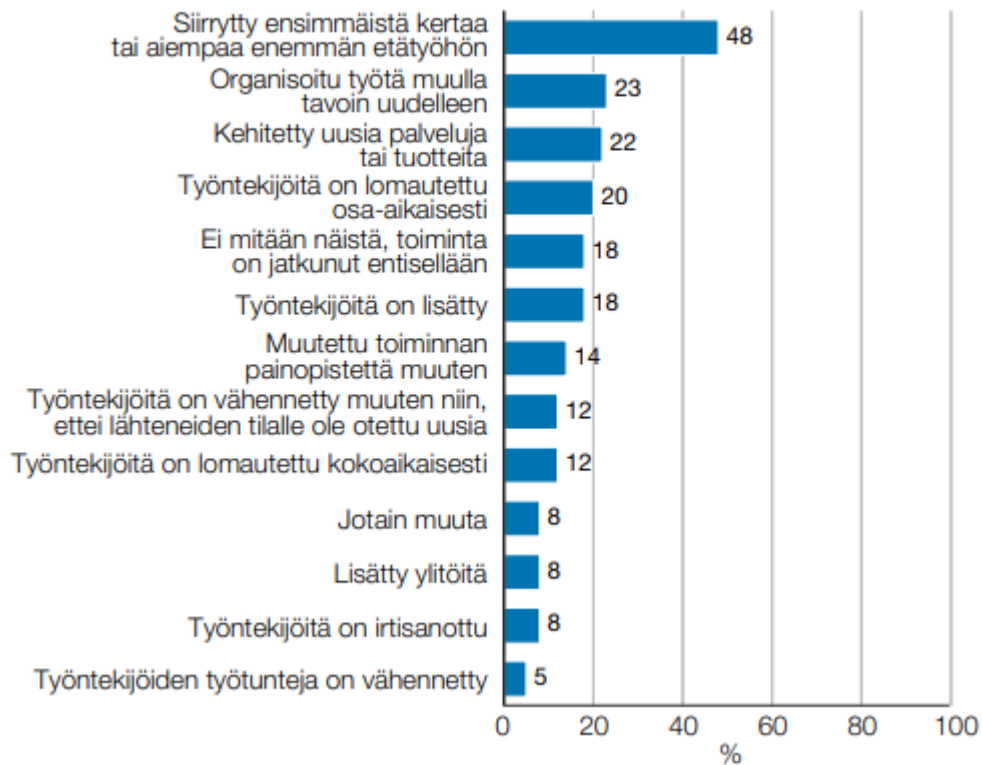
Tämän opinnäytetyön aihe, Tiedon suojaaminen hybridityössä, löytyi yhteistyössä työelämäkumppanin edustajan kanssa. Opinnäytetyöni tavoitteena oli kehittää yritys X:n tietoturvallisuuden tasoa erityisesti tiedon suojaamisen osalta vaihtelevissa

hybridityöolosuhteissa. Opinnäytetyö rajattiin tarkoituksellisesti koskemaan case-yritystä, vaikka tulosten yleistettävyys laajempaan kokonaisuuteen ei ole poissuljettua.

2 Hybridityö ja tiedon suojaaminen

Työn käsite on elänyt aikakaudesta toiseen yhteiskuntamuutosten mukana. Nykyään lisääntyvä digitalisaatio muuttaa työtä ja työn käsitettä jokaisella toimialalla. Digitalisaation suurin vaikutus näkyy toimihenkilöammateissa mutta muutos valuu myös työntekijäammatteihin. Erityisen vahvasti muutos ja muuttuneet olosuhteet vaikuttivat työhön maailmanlaajuisen pandemian puhjettua. Suomalainen digi-infrastruktuuri oli meidän suomalaisten onneksi jo valmis lisääntyneeseen etätyöskentelyyn ja pandemian aiheuttamiin muutospaineisiin. Erityisesti asiantuntijatehtävissä toimivien työolosuhteet muuttuivat radikaalisti pandemian puhjettua ja etätyön määrä lähes kaksinkertaistui vuoteen 2018 verrattuna. Kuviossa 1 näkyy etätyöhön siirtymisen prosentuaalinen muutos. Käytännössä lähes kaikki, joiden tehtävät sallivat paikkariippumattoman työskentelyn siirtyivät työnteossa etä- tai hybridimalliin. (Sutela & Pärnänen 2021, 11, 24-25, 28-31.)

Työpaikoilla tehdyt toimet koronakriisin aikana poikkeustilaan sopeutumiseksi, osuus palkansaajista %, Koronakriisin vaikutukset työelämää 2021



Kuvio 1 Sopeuttamistoimet koronakriisin aikana (Sutela ym. 2021)

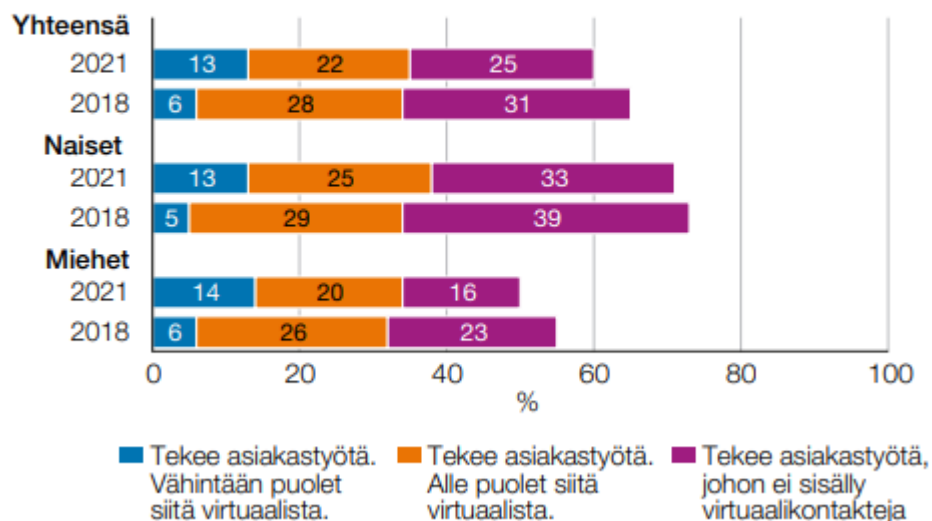
Etätyö katsotaan Tilastokeskuksen määritelmän mukaan varsinaisen työpaikan ulkopuolella työnantajan kanssa sovitusti tehtäväksi ansiotyöksi (2022). Etätyötä tekevät yleensä asiantuntijatehtävissä tai tietotyössä olevat työntekijät. Etätyötä voidaan tehdä kotona, kesämökillä tai vastaavasti missä tahansa muussa sijainnissa. Usein etätyössä edellytetään toimivia tietoliikenneyhteyksiä. Etätyötä usein määrittelee myös ajasta ja paikasta riippumattomuus, sopimuksellisuus sekä vapaaehtoisuus. Se voi olla luonteeltaan jatkuvaa tai epäsäännöllistä. (Tilastokeskus 2022; Työturvallisuuskeskus 2017; Työterveyslaitos 2022.)

Hybridityö on kuvaavampi ja nykyaikaisempi termi etätyöstä, sillä usein ansiotyötä tehdään tarpeen mukaan sekä työnantajan tarjoamalla työpaikalla että muualla. Niinpä hybridi- tai monipaikkainen työ on vahvasti yleistynyt suuntaus työelämässä. Digitalisaatio ja maailmanlaajuinen koronapandemia ovat lisänneet muualla kuin työnantajan omassa toimistossa tehtävän työn määrää. Monipaikkainen työ on luonteeltaan sellaista, että sitä tehdään vaihtelevissa paikoissa, muun muassa esimerkiksi asiakkaan luona. Hybridityön käsitteeseen voidaan sisällyttää sekä monipaikkainen etätyö että omalla, nimetyllä työpaikalla tehtävä ansiotyö, sillä hybridityön käsite ei vielä ole vakiintunut. (Tilastokeskus 2022; Työterveyslaitos 2022.)

2.1 Kehittyvä työ

Ennen pandemiaa oli yleistä, että esimerkiksi asiakaspalvelutehtävissä toimittiin perinteisessä toimistoympäristössä. Nykyään myös virtuaalinen asiakastyö on todellisuutta monella työpaikalla (Kuvio 2).

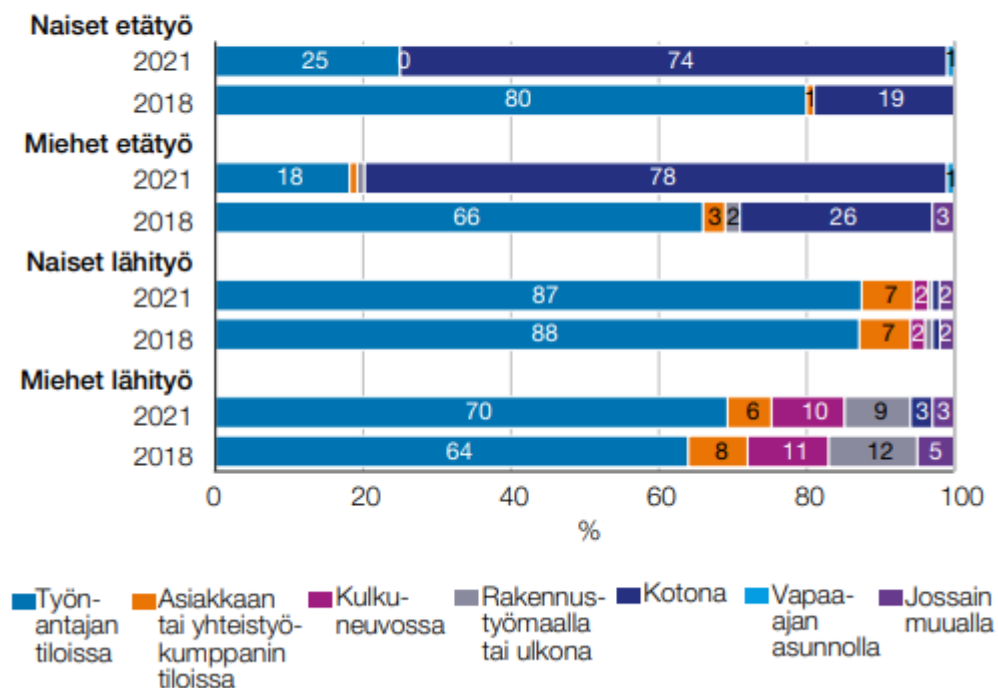
Virtuaalisen asiakastyön osuus työajasta sukupuolen mukaan, osuus palkansaajista %, Koronakriisin vaikutukset työelämään 2021 ja Työolotutkimus 2018 verkkoaineisto



Kuvio 2 Virtuaalisen asiakastyön osuus (Sutela ym. 2021)

Työn monipaikkaistuminen erilaisissa työnkuivissa on nykypäivää, vuonna 2018 jopa yli 60 % etätöitä tekevistä ilmoitti tehneensä työtä muualla kuin pääasiallisella työpisteellään. Etätöypiste sijaitsee useimmiten kotona, mutta myös asiakkaan luota, junasta, kesämökiltä tai vaikkapa lomakohteesta tehdään vaivattomasti päivän työt (kuvio 3). Koronapandemia vähensi rajusti työn monipaikkaisuutta etätöyläisten vetäytyttyä koteihinsa, mutta rajoitusten poistumisen myötä paluu monipaikkaisempaan työntekoon on todennäköistä. (Sutela ym. 2021, 31-39.)

Pääasiallinen työnteon paikka yleensä / koronarajoitusten käyttöönoton jälkeen etä-/lähityön ja sukupuolen mukaan %, Koronakriisin vaikutukset työelämään 2021 ja Työolotutkimus 2018 verkkoaineisto



Kuvio 3 Työntekopaikat (Sutela ym. 2021)

Uudenlainen työympäristö luo uudenlaiset haasteet. Vapautta tuo aika- ja paikkariippumattomuus ja vastuuta puolestaan itsensä johtaminen, turvallisuusnäkökanta sekä tavoitteiden saavuttaminen. Jaksaminen voi nousta ongelmaksi. Omasta rytmityksestä huolehtiminen ja työ- ja vapaa-ajan erottaminen jää työntekijän omalle vastuulle. Itsensä johtamiseen kuuluu työpäivän etukäteissuunnittelu, jota hyödyntäen on hyvä rytmittää niin tavoitteet kuin tauotkin ja ehdottomasti se oma, työajasta erillinen vapaa-aika. Jokaisella on oma vuorokausirytmensä, minkä avulla voi ohjata omaa ajankäyttöään. Lähi- ja etäpäivien rytmitys, ellei asiaan ole tiukkaa organisaatio-ohjausta, on hyvä suunnitella omien sosiaalisten tarpeiden mukaan ja koordinoita toimistopäivät siten, että myös kohtaamisia tapahtuu. (Malinen 2022.)

Koronapandemian joudutettua omalta osaltaan hybridityön yleistymistä menetti monen organisaatiokulttuurin muutosta hidastava vaikutus merkityksensä, kun siirryttiin viranomaisjohtoisesti valtakunnalliseen etätyösuositukseen ja sitä kautta hybridisijainteihin. Suomalainen työelämä selvisi tästä haasteesta poikkeuksellisen hyvin maailmanlaajuisestikin mitattuna. Työelämän murros tuskin jää tähän ja organisaatiokulttuuritkin kehittyvät omaehtoisesti ja osin pakon sanelemasti. Työntekijälle hybridityö tuo toivottua vaihtelua niin toimisto- kuin etätöihin joustavuudellaan. Tärkeintä on työnantajan ja työntekijän välinen luottamus. Muuttunut ja muuttuva työympäristö asettaa korkeat vaatimukset myös esimiestyön kehittymiselle sekä työnohjaukselle. Muita merkityksellisiä seikkoja lisääntyvässä hybridityössä on etätöiden hiilijalanjälkeä pienentävä vaikutus, digikyvykkyyksien kasvaminen ja tehokkuuden parantaminen. (Tivi 2021; RAKLI 2022.)

Monessa työpaikassa on törmätty tavallaan uutena asiana työympäristöjohtamisen käsitteeseen tai ainakin siihen, miten laajasta kokonaisuudesta on oikeasti kysymys. Tarkemmin asiaa pohdittaessa huomataan, että työympäristöjohtamisessa yritysturvallisuus on kiinteä ja tärkeä osa tätä kokonaisuutta. Turvallisuusaspektin integroiminen etätöikäytänteisiin onkin suuri haaste ja monissa työtehtävissä ehdoton vaatimus käsiteltävän tiedon sensitiivisyyden vuoksi. (RAKLI 2022.)

2.2 Tiedon suojaaminen

Työn monimuotoisuus ja kehittyminen asettaa erilaisia vaatimuksia työlle kuin pelkkä toimistolla tehtävä työ. Kyberturvallisuuskeskus tarjoaa käytännön vinkkejä etätöihin. Näitä ovat annettujen ohjeiden noudattaminen, tietokoneen käyttöjärjestelmän ja sovellusten päivitysten suorittaminen ja turvallisten tietoliikenneverkkojen käyttäminen. Muita huomioitavia seikkoja ovat vain työnantajan tarjoamien laitteiden käyttäminen, työskentelyn suojaaminen ulkopuolisilta ja riittävän haastavat, jokaiseen järjestelmään eri salasanat. Toimisto-olosuhteiden ulkopuolella pitää myös muistaa oma vastuu työn tauottamisesta ja lepoajoista. (Kyberturvallisuuskeskus 2022.)

Tiedon suojaaminen on osa tietoturvallisuuskokonaisuutta. Tietoturvallisuus on kokonaisuus, joka Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen (2020) määritelmän mukaan on niiden hallinnollisten ja teknisten toimien summa, joiden avulla pystytään varmistamaan tiedon luottamuksellisuus, eheys sekä käytettävyys. Määritelmää voidaan vielä tarkentaa lisäämällä siihen kiistämättömyyden ja todentamisen ulottuvuudet, mainitsee blogin kirjoittaja, tietoturvapääällikkö Matti Laakso blogissaan Tietojesiturvaksi.fi (2022).

Usein puhutaan tietoturvasta, kun tarkoitetaan itse asiassa tietoturvallisuutta.

Tietoturvallisuuden ja tietoturva ero ei siis ole aivan yksiselitteinen, mutta tietoturvallisuus käsitetään yleisesti tietoturvaa laajempänä kokonaisuutena, johon tietoturva eli hallinnolliset ja tekniset käytännön toimet sisältyvät. Tietoturvallisuuteen sisältyy myös tietosuojan käsite.

(Tietojesiturvaksi.fi 2022.) Näiden käsitteiden sisältö sekoittuu erityisesti puhekielessä, mutta on hyvä tarkentaa, mitä mikäkin itse asiassa sisältää. Tietoturva voidaan rajata aineiston suojaamiseksi tuhoutumista, muuttumista tai varkautta ajatellen sen käsittelyn, säilytyksen ja siirron aikana. Tietosuoja puolestaan varmistaa henkilötietojen tietoturvallisen käsittelyn ja niiden yksityisyyden suojaamisen oikeudettomalta käytöltä. (Termipankki 2022.)

2.2.1 Organisaation kokonaisturvallisuuden yhteys tiedon suojaamiseen hybridityössä

Yritysturvallisuus on osa-alue, joka vastaa yrityksen kokonaisturvallisuudesta. Sen keskeisinä tehtävinä nähdään esimerkiksi Elinkeinoelämän keskusliiton mukaan tuottavuuden parantaminen sekä yrityksen kilpailukyvyyn edistäminen muuhun hallintotoimeen integroituna osana. Yritysturvallisuus olennaisena osana yrityksen johtamiskokonaisuutta ja yrityksen riskienhallintaa varmistaa edellytykset yrityksen toiminnan jatkumiselle ja turvalliselle, säätelymukaiselle toiminnalle. (EK 2022.)

Kokonaisturvallisuus taataan yritysjohtoa ja henkilökuntaa sitouttavalla turvallisuusjohtamisella. Turvallisuusjohtaminen käsitetään kokonaisvaltaisena ihmisten ja prosessien johtamisena. Hyvän turvallisuusjohtamisen tavoitteet ovat niin turvallisuuden kuin terveellisyydenkin edellytysten jatkuva monitorointi suunnittelun ja toiminnan, kuten riskien arvioinnin, keinoin. Kun organisaatioon on juurtunut laadukas turvallisuuskulttuuri, turvallisuuden hallinta helpottuu, mutta tekeminen ei koskaan pääty. Riskien arviointi ja riskien hallinta on jokapäiväistä tekemistä. Suuremmilla työpaikoilla erityistä huomiota tulisi kiinnittää työsuhteen elinkaarenhallintaan ja sen myötä ilmeneviin muutostarpeisiin työntekijöiden osaamisen varmistamisessa sekä oikeuksien määrittelyissä. (Työsuojeluhallinto 2010; EK 2022.)

2.2.2 Standardit, asetukset ja lait ohjaamassa toimintaa

Työsuojeluorganisaatio omalta osaltaan tekee turvallisuustyötä, mutta kokonaisturvallisuus on koko henkilökunnan asia. Työturvallisuuslaki asettaa omia vaatimuksiaan työpaikoille, kuten työsuojelun toimintaohjelman laatiminen ja ylläpito, haitta- ja vaaratekijöiden tunnistaminen - toisin sanoen riskien arviointi, työntekijöiden ohjaus ja muun muassa toimintaohjeiden päivittäminen, vaara- ja haittatekijöiden poistaminen tai niiden vaikutusten lieventämiseen johtavat toimenpiteet - eli riskien hallinta ja käsittely - ja niin edelleen. Tärkeäksi keinoksi tukea turvallisuutta koetaan henkilöstön kouluttaminen ja sitä kautta hyvän turvallisuuskulttuurin luominen yritykseen. ISO/IEC 27000 -standardissa kaikki hyvän turvallisuuskulttuurin ja riskienhallinnan tekijät esitellään kattavasti. (Työsuojeluhallinto 2010; Työturvallisuuslaki 738/02; EK 2022; ISO/IEC 27000.)

Organisaatiolle turvallisuussertifiointi on hyvä keino osoittaa oman kokonaisturvallisuuden tasokkuus. ISO/IEC 27000 -standardiperheessä kattavasti esitellään parhaita käytänteitä ja

vaatimuksia, joita informaatioteknologia-alalla tietoturvallisuuden hallintajärjestelmille on luotu tieto-omaisuuden hallintaan liittyen. Seuranta ja valvontaa tehdään esimerkiksi auditointien, vaikuttavuusarviointien ja mittauksen keinoin. (ISO/IEC 27000.)

2.2.3 Yritysturvallisuusmalli ja jatkuva työ

Tietoturvallisuus löytyy Elinkeinoelämän yritysturvallisuusmallin (Kuvio 4) sisemmästä ympyrästä kiinteänä osana koko yritysturvallisuuden kokonaisuutta.



Kuvio 4: Elinkeinoelämän yritysturvallisuusmalli (EK 2022.)

Kyseessä ei tässäkään ole irrallinen kokonaisuus, vaan kiinteä osa kaikkea yrityksen toiminnan hallintaa ja toiminnan jatkuvuuden edistämistä. Tietoturvallisuudessa korostetaan kolmea seikkaa, joihin palataan tämän aihepiirin sisällä tavan takaa. Nämä kolme asiaa ovat tiedon

luottamuksellisuus, tiedon käytettävyys sekä tiedon eheys. Nämä kolme käsitettä muodostavat niin sanotun CIA-mallin. (EK 2022.)

CIA-malli on laajalti käytetty tietoturvallisuuden määrittelyssä. Mallin nimitys tulee englanninkielisistä sanoista confidentiality, integrity ja availability, eli luottamuksellisuus, eheys ja käytettävyys. Malli rakentuu näiden peruskäsitteiden varaan. Luottamuksellisuutta määritellään siten, että tieto ei ole saavutettavissa sellaisten tahojen toimesta, joilla ei ole siihen oikeutta. Eheyttä määritellään tiedon ehjyydellä ja tarkkuudella. Saavutettavuus on määritelty siten, että tieto on käytettävissä ja siihen päästään tarvittaessa käsiksi. Mallin variaatioita löytyy muun muassa ISO-standardista. Mallia on kehitetty edelleen ja sitä on myös kritisoitu joko liiasta ylimalkaisuudesta mutta myös liian ahtaasta tulkinnasta ja joustamattomuudesta. (Lundgren & Möller 2019.) Oli miten tahansa, nämä mainitut peruseriaatteen pätevät pitkälti tänäkin päivänä, erityisesti sovellettuina kohdeorganisaation tarpeisiin. Luottamuksellisuus korostuu etenkin monipaikkaisessa työskentelyssä, jossa työnteko tapahtuu oman yrityksen ulkopuolisissa tiloissa. Eheyden ja käytettävyyden käsitteet ovat yksinkertaisempia toteuttaa, sillä nykyisillä tietoliikenneyhteyksillä tiedon saavutettavuus enää harvoin muodostaa ongelmaa eikä tiedon eheys ole työskentelypaikkariippuvaista. Erityishuomiota tulee siis kiinnittää luottamuksellisuuden osuuteen ja korostaa sitä niin asiakkaan kuin yrityksen oman edun vuoksi. Työpaikan ulkopuolella olosuhteet ovat työnantajan hallitsemattomissa, jolloin työntekijän vastuu kasvaa. Yrityksen riskien mitigointipolitiikassa tuleekin huomioida työntekijän ohjeistaminen oikeanlaisiin työskentelytapoihin. (Helle 2004, 4.4; 5.4-5.5; 6.3; 12-13.)

Tietoturvallisuuskokonaisuus rakentuu Elinkeinoelämän keskusliiton mukaan seuraavista osialueista: tiedon merkityksen arviointi, tiedon luokittelu ja sen käsittely, hallinnollinen ja tekninen tietoturvallisuus, tietosuoja, yksityisyydensuoja sekä järjestelmä- ja prosessitoiminnan jatkuvuuden varmistaminen. Muitakin tapoja määritellä tietoturvallisuuden kokonaisuutta on. Elinkeinoelämän keskusliiton jako on toimiva ja yleisesti käytetty. (EK 2022.)

Tiedon suojaaminen on osa tietoturvallisuuden hallinnan kokonaisuutta ja siten tärkeä osialue myös organisaation kokonaisturvallisuudessa. ISO/IEC 27000 -standardissa määritellään tietoturvallisuuden hallinnointi toiminnaksi, jolla ohjataan ja valvotaan organisaation tietoturvatoinenpiteitä. Standardissa myös sisällytetään tiedon luottamuksellisuus, eheys ja saatavuus tietoturvallisuuden käsitteeseen. Näiden kolmen tietoon liittyvään periaatteen toteutuessa tietoa suojataan, sen jatkuvuus taataan ja mahdollisten häiriöiden vaikutusta pienennetään tai se poistetaan täysin. (ISO/IEC 27000.)

Olennaista tiedon suojaamisessa on myös määritellä mitä tieto on. ISO/IEC 27000 -standardin määritelmässä tiedolle mainitaan, että tieto on organisaatiolle erittäin tärkeä

liiketoiminnallinen kohde, jota voidaan säilyttää monin eri tavoin, myös aineettomasti, ja jota voidaan välittää monella tavalla, mutta säilytys- ja välitystavasta riippumatta se tulee aina asianmukaisesti suojata. Tietoon liitettäviä toimintoja ovat sen luominen, käsittely, varastointi, siirtäminen, suojaaminen sekä tuhoaminen. Tiedon hallintaan liittyy aina myös Elinkeinoelämän keskusliiton yritysturvallisuusmallissa esitetyt ja ISO/IEC 27000 -standardissa mainittavat jatkuva valvonta, katselmointi sekä parantaminen tai kuten ne ovat Elinkeinoelämän keskusliiton mallissa nimetty, arviointi, parantaminen, suunnittelu ja toteutus. Näiden toimintojen tulee olla kiinteästi organisaation liiketoimintaprosesseihin integroituja. (ISO/IEC 27000; EK 2022.) Prosesseihin sisällytettynä tiedon suojaaminen osa työntekijän arkipäiväistä tekemistä ja samalla oma osansa koko organisaatiturvallisuuden kokonaisuutta turvaten yrityksen toiminnan nyt ja tulevaisuudessa.

2.2.4 Viestinnän luottamuksellisuus

Yleinen tietosuoja-asetus tuli Suomessa voimaan vuonna 2016 ja se kumosi voimaansaatuun vanhan henkilötietolain 523/1999. Uusi tietosuojalaki 1050/2018 toteuttaa EU:n tietosuoja-asetusta, General Data Protection Regulationia eli tuttavallisemmin GDPR:ää. GDPR eli mainittu yleinen tietosuoja-asetus on osa Suomea sitovaa EU-lainsäädäntöä, joka astui voimaan huhtikuussa 2016. Yleisellä tietosuoja-asetuksella säädellään luonnollisten henkilöiden henkilötietojen käsittelyä sekä rajataan näiden tietojen vapaata liikkuvuutta ja suojataan luonnollisten henkilöiden perusoikeuksia ja -vapauksia sanottujen tietojen suojaamiseen liittyen. Asetuksella säädettyjä pääperiaatteita ovat tietojen lainmukainen ja läpinäkyvä käsittely, oikeus kerätä tietoja vain nimenomaista, laillista tarvetta varten, kerätyn tiedon tarpeellisuuden varmistaminen suhteessa käyttötarkoitukseen, kerättyjen tietojen täsmällisyys ja päivitettävyys, tietojen säilytys tunnistettavana vain tarpeellisen ajan sekä kerättyjen tietojen turvallinen käsittely, samalla suojaten niitä luvattomalta käytöltä ja vahingoittumiselta. Henkilötietojen käsittelyn turvallisuus siis perustuu tietoturvallisuuden pyhään kolminaisuuteen, luottamuksellisuuteen, eheyteen ja käytettävyyteen ja siitä vastaa rekisterinpitäjä. Rekisterinpitäjä on se organisaatio, jonka päätöksellä tieto kerätään. Organisaatiossa työskentelevät työntekijät puolestaan toteuttavat rekisterinpitäjän tehtävää, he eivät siis ole henkilötietojen käsittelijöitä. Käsittelijän roolissa toimivat esimerkiksi ulkoistettujen palkkapalveluiden työntekijät. (Yleinen tietosuoja-asetus 2016; Tietosuojalaki 1050/2018; EU 2022.)

Edellä mainittuun lainsäädäntöön ja asetuksiin perustuva velvollisuus vähentää tarpeetonta henkilöön kohdistuvien tietojen käsittelyä suojaamalla rekisteröityjä henkilöitä. Tietosuojan vaikutusarvioinnin ohjaamana voidaan tehdä päätöksiä, milloin ja minkä tiedon käsittely on sallittua. Jokaiseen käsittelykertaan tulee löytyä peruste. Tietosuojan vaikutusarviointi toimii ohjenuorana tietosuojan toteutumisessa sekä riskien hallinnassa, erityisesti kun

puhutaan viestintäsalaisuuden alaisen tiedon käsittelystä, joka luokitellaan rekisteröidyn kannalta ns. korkean riskin tietomateriaaliksi. (Tietosuojavaltuutetun toimisto 2021.)

Tiedon suojaamisen tulee tapahtua niin hallinnollisten, teknisten kuin rakenteellistenkin ratkaisujen kautta. Hallinnollisia keinoja suojata tietoa ovat vaikkapa työnkuvaan liittyvät eri käyttäjäoikeustasot tai työntekijöille teetetyt turvaselvitykset. Teknisiä puolestaan ovat yksilölliset käyttäjätunnukset, salasana vaatimukset sekä suojatut yhteydet, datapalvelimien peilaus ja kahdentaminen ja tietoliikenneyhteyksien varmennus. Rakenteellisia ratkaisuja edustaa vaikkapa kulunhallinta, varavoimaratkaisut ja olosuhdevalvonta, kuten automaattiset sammutusjärjestelmät toimitiloissa. Erityisessä roolissa on henkilöstön kouluttaminen tiedon hallintaan ja käsittelyyn ja käytäntöihin. (Valtiovarainministeriö 2021.)

2.3 Tieto- ja viestintäsektorin erityispiirteet

Digitaalinen infrastruktuuri on nykypäivän toimintaympäristö. Harvassa ovat ne sektorit, joiden toiminta ei sitä hyödynnä. Digitaaliseen infrastruktuuriin katsotaan Liikenne- ja viestintäministeriön strategiasuunnitelman mukaan sisältyvän yksityisen ja julkisen sektorin sijaintiriippumattomien palveluiden mahdollistava nopea ja toimintavarma kiinteä ja mobiili tietoverkko. Kehittyvät, laadukkaat ja nopeat tietoliikenneyhteydet mahdollistavat teollisuuden IoT-toiminnot, tekoälyn hyödyntämisen, automaatioasteen nostamisen, potentiaalisen liikenneautonomian sekä muun muassa virtuaalitodellisuusratkaisut. (Liikenne- ja viestintäministeriö 2018.)

NIS-direktiivi eli verkko- ja tietoturvadirektiivi (EU) 2016/1148 määrittelee reunaehdot ja tieto- ja viestintäliikesektorin toimijoille. Täytäntöönpanoasetuksessa (EU)2018/151 eli niin sanotussa DSP-asetuksessa on vielä tarkennettu direktiivin regulaatiota ja toimijoiden velvollisuuksia, kuten digitaalisten palvelujen osalta toimialan yritysten riskinhallinta- ja häiriöraportointivelvoitteita. (EUR-LEX 2016/1148; EUR-LEX 2018/151.) NIS-direktiiviä tulee korvaamaan NIS2-direktiivi - kyberturvallisuudirektiivi, joka pyritään vuoden 2024 aikana integroimaan Suomen lainsäädäntöön (Valtioneuvosto 2022).

Näitä niin sanottuja teleyrityksiä eli digitaalisen infrastruktuurin toimijoita koskee myös teletoiminnan säätely. Kohderyhmää koskevaa regulaatiota löytyy myös laista sähköisen viestinnän palveluista FINLEX 917/2014, jonka tarkoituksena on varmistaa toimijoiden tuottamien palvelujen saatavuus, toimintavarmuus, laatu sekä kohtuullinen hinta ja sähköisen viestinnän luottamuksellisuus ja käyttäjien yksityisyyden suoja (Laki sähköisen viestinnän palveluista FINLEX 917/2014). Myös pakkokeinolain (FINLEX 806/2011) pykälissä on digitaalisen infrastruktuurin toimijoita koskevaa lainsäädäntöä useammassa luvussa. Esimerkiksi voidaan nostaa pakkokeinolain 10. luvun Telepakkokeinot, jotka oikeuden päätöksellä antavat viranomaisille pääsyn normaalisti viestintäsalaisuuden piirissä olevaan materiaaliin, kuten televalvonnan tunnistamistietoihin (Pakkokeinolaki FINLEX 806/2011).

Oma lukunsa ovat ne tiedot, joiden käsittelyä on rajattu. Tällaisia tietoja saattavat olla esimerkiksi sensitiiviset henkilötiedot tai ammattiyhdistyksen jäsenyys.

Asiakkuusorganisaation oma tietoturvallisuuskäytäntö saattaa edellyttää, ettei tietoja esimerkiksi käsitellä Suomen valtion rajojen ulkopuolella tai vastaavasti EU/ETA-alueen ulkopuolella. Tiedon sensitiivisyyden vuoksi voi olla myös tarpeen työskennellä vain suojatuissa toimisto-olosuhteissa siten, ettei määrättyjä tietokokonaisuuksia voi etätyöolosuhteissa lainkaan käsitellä. Monikansallisissa organisaatioissa tällaiset rajaukset ovat erityisen haasteellisia. (FINLEX 917/2014; Yleinen tietosuojalaki 2016; Tietosuojalaki 1050/2018; EUR-LEX 2016/1148; EUR-LEX 2018/151.)

3 Kehittämistyön toteutus

Kehittäminen on toiminto, jolla on tarkoitus. Kehittäminen ei ole tutkimusta, vaikka joskus siinä voi tutkimuksellisenkin aspekti olla. Tässä opinnäytetyössä pyrin kehittämään tiedon suojaamisen toimintoa ja tutkimuksellisuuden kautta löytämään uutta tietoa tuon kehittämistyön lähtökohdaksi. Opinnäytetyön tavoitteena on kehittää yritys X:n tietoturvallisuuden tasoa erityisesti tiedon suojaamisen osalta vaihtelevissa hybridityöolosuhteissa. Tutkimuksellinen ote kehittämistyössä edellyttää suunnitelmallisuutta ja kriittistä analyttisyyttä. Konkretia tekee puolestaan työstä kehittämistä eikä tutkimusta. (Ojasalo, Moilanen & Ritalahti 2015, 14-16; 21.)

Kehittämistyön tavoitteena oli löytää mahdollisia epäkohtia tai puutteita yritys X:n tietoturvaluustietoisuudessa tai tarjotuissa koulutuksissa. Kehityskohteiden löytäminen ja niiden saattaminen tiedoksi organisaatiotaholle, joka pystyy tekemään konkreettisia muutoksia vallitsevaan tilanteeseen on olennainen osa tätä kehittämistyötä. Opinnäytetyön kautta löydettyjä mahdollisia riskejä yritys X:n tietoturvallisuuden tasossa sen työntekijöiden koulutusta kehittämällä ja siten potentiaalisia riskejä vähentämällä päädytään varmistamaan organisaation tietoturvallisuuden edelleenkehittymistä sekä helpottamaan työntekijöiden arkea entistä selkeämmillä toimintamalleilla ja -prosesseilla.

Kehittäminen on nykyaikaa työelämässä, vaikka työtehtävä ei nimellisesti sitä sisältäisikään. Työelämä tänä päivänä edellyttää jokaiselta työntekijältä jonkin asteista kehittämistyötä vähintään oman työtehtävän osalta. Kehittämistyössä tarvitaan muun muassa tavoitteellisuutta, kriittistä arviointikykyä, tiedonhankintataitoja, ongelmanratkaisukykyä, kykyä itsensä johtamiseen sekä yhteistyötaitoja. Opinnäytetyön osalta kyseessä on kehittämispohjainen oppiminen, jossa työn tekijä tai tekijät edelleen kartuttavat osaamistaan tuottaen samalla konkreettista lisäarvoa työelämän kumppanuudelle. (Ojasalo et al. 2015, 14-16.)

Laadullinen eli kvalitatiivinen ote tarkoittaa lyhyesti sitä, että kohdetta pyritään tarkastelemaan osallistujien näkökannalta. Osallistujien näkökulmat, ajatukset ja tunteet tutkittavan kohteen suhteen ovat pääosassa. Tavoitteena laadullisessa näkökulmassa on saada tarkkaa ja kokemusperäistä tietoa kohteesta. Laadullisen lähestymistavan etuna on sen joustavuus, mikäli odotusarvot työn edetessä muuttuvat. Pyrkimys vahvaan ymmärrykseen taas ohjaa työtä case-tyyppiseen toteutukseen. Tärkeää on löytää ne ilmiöt, jotka osallistujien keskuudessa kehityskohteen suhteen nousevat. Kvalitatiivisesta näkökulmasta toteutetussa analyysissä löydöksen toistuvuudella ei ole merkitystä. (Puusa & Juuti 2020, luku 4.)

Opinnäytetyön keskustelu- ja haastatteluosuuksien aikataulutus tehtiin case-yrityksen ehdoilla. Haastattelujen ja ryhmäkeskustelujen aikataulutus hehtisessä työelämässä tehtiin täysin operatiivisten osastojen ehdoilla ja osallistujien aikataulujen mukaan siten, että varsinaiselle linjatyölle aiheutui mahdollisimman vähän häiriöitä. Kiireettömästi aikataulutetut tilaisuudet myös tukivat tilanteen avoimuutta ja lisäsivät osallistujien valmiutta paneutua keskusteluun ja aiheeseen.

3.1 Kehittämistyön aineistonkeruumenetelmät

Kehittämistyön aineisto päädyttiin keräämään haastatteluilla ja ryhmäkeskusteluilla, jotka ovatkin tyypillisin keruumenetelmä laadullisissa tutkimuksissa. Haastattelumetodin valinta tämän laadullisen kehittämistyön menetelmäksi on perusteltua, sillä kehittämiskohteita voidaan löytää nimenomaan haastateltavien subjektiivisten kokemusten perusteella. Haastateltavien omakohtaiset kokemukset saamansa opastuksen riittävydestä heidän työtehtävissään tuo tutkimusaineistoon tarvittavaa sisältöä (Puusa 2020). Kehittämistyössä päädyttiin aineistonkeruumenetelminä käyttämään yksilöhaastattelujen lisäksi ryhmäkeskusteluja. Punaisena lankana kaikissa näihin teemahaastattelun formaattiin perustuviin menetelmiin on selvittää, miten tietoturvallisuus ja erityisesti tiedon suojaaminen toteutuu käytännössä monimuotoisessa työympäristössä.

3.1.1 Haastattelut ja ryhmäkeskustelut

Haastatteluja ja ryhmäkeskusteluja varten koottu keskustelurunko toimi apuna keskustelun kulkua eteenpäin vietäessä (LIITE 1). Monessa tapauksessa tätä apurunkoa ei paljoakaan tarvittu, sillä tilaisuus luontaisesti eteni aihepiirin teemojen ympärillä kattaen suunnitellut keskustelunaiheet. Rungosta oli kuitenkin hyötyä siinäkin mielessä, että mikään teema ei unohtunut käsittelemättä ja siten se edesauttoi eri tilaisuuksien sisältöjen määrätynlaisen homogeenisuuden säilymisessä ja siinä, että jokaista opinnäytetyön kannalta olennaista teemaa käsiteltiin tasapuolisesti joka tilaisuudessa. Keskustelurunko koottiin teorian pohjalta siltä osin, että käytetyt käsitteet käytiin läpi ja että ymmärrys käsitteistä sekä opinnäytetyön tekijän että osallistujien mielestä yhtenevä. Lisäksi keskustelurunko piti sisällään ne

aihealueet, joiden kautta pyrin selvittämään nykytilannetta ja osallistujien kokemuksia siitä ja myös heiltä nousevia tarpeita.

Haastattelu metodina on monipuolinen ja joustava menetelmä. Haastattelut ja keskustelut mielletään vuorovaikutteisiksi tilanteiksi. Näiden tilanteiden tarkoituksena on kerätä aineistoa, jonka perusteella voidaan tehdä johtopäätöksiä ja päätelmiä. Edellytyksenä aineiston uskottavuuteen on tehtävien haastattelujen tallennus. Haastattelumetodilla kerätty aineisto on aina subjektiivista, siihen vaikuttavat sekä haastattelijan että haastateltavien omakohtaiset kokemukset. Subjektivisuus tulee siis pitää mielessä yleistäviä johtopäätöksiä tehtäessä. (Puusa 2020.) Avoimessa keskustelutilanteessa tai haastattelussa saattaa spontaanisti nousta esiin aiheita, joita ei aiheiston keruun yhteydessä ole edes ymmärretty pohtia. Haastattelujen ja ryhmäkeskustelun valinta aineistonkeruumenetelmäksi on myös tätä kautta siis perusteltua.

Ryhmäkeskustelua on tavattu pitää taloudellisena ja tehokkaaksi koettuna aineistonkeruumenetelmänä. Ryhmäkeskustelua voidaan käyttää joko yksittäisenä aineistonkeruumenetelmänä tai yhdessä toisten menetelmien kanssa. Erityisesti ryhmän vuorovaikutustilanteen huomioiminen on merkittävä ero ryhmäkeskustelun ja ryhmähaastattelun välillä. Ryhmähaastattelu on yksi tutkimuksessakin käytetty aineiston keräämisen metodi, jossa useampi haastateltava on paikalla keskustellakseen sovitusta teemasta. Haastattelu on itse asiassa pitkälti vapaamuotoista keskustelua, mutta punaisena viivana on haastattelun aihe. Fasilitoija, eli ryhmänvetäjä tai moderaattori, mitä nimitystä hänestä nyt käytetäänkin, ohjaa ryhmähaastattelussa keskustelua kahdenvälisesti osallistujien kanssa, ryhmäkeskustelussa puolestaan kannustetaan vapaaehtoisia osallistumaan keskusteluun keskenään. Aineistonkeruumenetelminä niin ryhmähaastattelu kuin -keskustelukin ovat nekin molemmat laadullisia menetelmiä. (Pietilä 2017; Valtonen & Viitanen 2020, 7-8.)

Ryhmäkeskusteluun kootusta ryhmästä voidaan myös käyttää nimitystä fokusryhmä tilanteessa, jossa ryhmä kokoontuu käsittelemään ennalta sovittua aihetta. Fokusryhmä-termillä korostetaan käsiteltävän aiheen merkitystä keskustelussa. Terminologia ei ole täysin vakiintunutta, joten ryhmäkeskustelu-termillä usein tarkoitetaan juuri fokusryhmä-tyyppistä tilannetta eikä ryhmähaastattelu-terminkään käyttö tässä yhteydessä kotimaisessa kontekstissa ole täysin poissuljettu. (Pietilä 2017.)

Fasilitaattorin keinoja vuorovaikutuksen parantamiseen ryhmäkeskustelussa ovat tasoittaa aktiivisten ja passiivisten osallistujien välisiä eroja sekä ohjata keskustelua etenemään kiistakysymyksistä tai vaikeiden aiheiden yli. Keinoja tähän ovat esimerkiksi tehtävät rinnastukset tai vertailut ja tarvittaessa fasilitaattori voi jopa provosoimalla pyrkiä saamaan reaktioita, toki tutkimusetiikan sallimissa rajoissa. (Pietilä 2017.)

Yksilöhaastattelussa kysymys - vastaus -formaatti on tyypillisin (Pietilä 2017). Tämä rakenne tekee tilanteesta haastattelun kuten myös osallistujien tiedon kerääjän ja tiedon antajan roolitkin. Myös tilanteen tallentaminen ja se, että edellä mainittu tilanteeseen liittyvä roolitus on molemmille osapuolille selvää, strukturoi aktuaalista tilannetta. (Ruusuvaori & Tiittula 2017.) Tilanteen ja vallitsevien pelisääntöjen ollessa selkeät kaikille osapuolille muodostui haastattelutilanne jokaisen vastaajan kanssa vuorovaikutteiseksi, joskin rakenteellisesti suunnitelluksi kokonaisuudeksi ja eteni vaivatta.

3.1.2 Kohderyhmä

Opinnäytetyöhön valikoituneet haastateltavat sekä ryhmätilanteiden keskustelijat ovat rekisterinpitäjän eli yritys X:n palveluksessa olevia työntekijöitä. Heidän toimiaan ohjaa sanotun rekisterinpitäjän määrittelemät tekniset ja organisatoriset menetelmät. Menetelmiltä edellytetään todennettavissa olevia, riittäviä suojatoimia eli käytettävien sovellusten teknisten ominaisuuksien sekä käyttöoikeuksien tulee täyttää tietosuoja-asetuksen minimivaatimukset. (Tietosuojavaltuutetun toimisto 2021.) Haastattelutilaisuuksia järjestettiin neljä ja ryhmäkeskusteluja kaksi, joihin molempiin osallistui yli viisi organisaation jäsentä.

Valitut henkilöt kuuluivat pääsääntöisesti ryhmään, jolle hybridityöskentely ja sen tuomat haasteet oli verrattain uusi tapa työskennellä. Tällä nimenomaisella rajauksella pyrittiin nostamaan esiin kehityskohteita - ongelmia - joita työntekijät työssään joutuvat kohtaamaan ja joihin he tarvitsevat ratkaisun. Miksi tiedon suojaaminen sitten on niin tärkeää? Miten nämä käsitteet, asetukset ja lait vaikuttavat yksittäisen työntekijän työtehtävästä suoriutumiseen? Vastaus näihin kysymyksiin on kuluttajan luottamus organisaatioon. Kokeneempien hybridityöntekijöiden voidaan olettaa taklanneen näitä ongelmia kukin omalla tavallaan, joten ei koettu tarkoituksenmukaiseksi haastatella heitä. Rutiinin jo luoneilla työntekijöillä kehittämiskohteet eivät tilanteiden jokapäiväistymisen myötä välttämättä esiintyisi ongelmina, joihin tarvitaan ratkaisua. Kokeneempien hybridityöntekijöiden työssä esiintyvät samat tilanteet kuin tuoreempienkin, mutta yhtä lailla heidänkin ratkaisujensa tulisi olla prosessin mukaisia eikä sovellettuja. Tämä teoreettinen otosrajaus tehtiin yhteistyössä yritys X:n työpaikkaohjauksen kanssa. Osallistujille oli etukäteen toimitettu tieto käsiteltävästä aiheesta. Heitä oli tiedotettu myös siitä, ettei heitä yksilöiviä tietoja kerätä. Myös se, että keskustelutilanne nauhoitettiin oli ennalta tiedossa.

3.1.3 Toteutusmenetelmät

Keskusteluissa käytetty teemarunko on viitteellinen ja laaditut haastattelukysymykset fasilitoijan apuna siinä kohdassa, jos keskustelu muuten olisi tyrehtynyt.

Haastattelukysymyksiä hyödynnettiin laajemmassa mitassa yksilöhaastatteluilissa, joissa vuorovaikutus oli fasilitaattorin ja haastateltavan välistä dialogia. Tässäkin lähestymistapa oli

väljä eikä kysymyksiin välttämättä menty, jos keskustelu omalla painollaan eteni tavoiteltuun suuntaan.

Aineistonkeruu suoritettiin Microsoft Teams -ohjelmistoa hyödyntäen osallistujien maantieteellisen hajanaisuuden vuoksi. Lisäetuna valitulle metodille oli tallennusmahdollisuus, jota hyödynnettiin tässä yhteydessä. Tallennettuun aineistoon saattoi palata yksityiskohtia ja painotuksia varmistettaessa.

3.2 Kerätyn aineiston käsittely

Tyypillisin piirre tämänlaiselle aineistolle on sen moniäänisyys ja siksi se sopii hyvin kehittämistyöhön, jonka tarkoituksena on selvittää yksilöiden kokemuksia ja käsityksiä. Kerätyn tiedon analyysissä huomioon otettiin sekä usean henkilön toimesta esille nostetut aiheet sekä myös yksittäiset huomiot, joilla nähtiin olevan lisäarvoa tiedon suojaamisen kehittämiseen. Kerätyn aineiston kannalta ei ole relevanttia päädytäänkö keskustelussa yhteismielisyyteen, jokaisella mielipiteellä on arvonsa vaikka se nousisi esille vain kerran. Yksilöiden perustelut ovat merkityksellisempiä ja ryhmädynamiikan luoman vuorovaikutuksen kautta esille nousevat yksityiskohdat tärkeitä. (Pietilä 2017.) Aineistoa laadullisesti analysoidessa nämä seikat nousivat hyvin esille, sillä jokaisen työntekijän kokemuksella on merkitystä sitä kautta, että ellei ole varmuutta siitä, mikä on oikeanlainen tiedon käsittelytapa, saattaa tulla virheitä joko itse käsittelyssä tai tilanteen suhteen syntyneen epävarmuuden kokemuksen johdosta.

Kehittämistyön analyysissä keskitytään aineistosta esiin nouseviin tulkinnan kannalta olennaisiin piirteisiin huomioiden ryhmäkeskusteluissa vuorovaikutustilanteet osaksi litteraattia. Aineistoanalyysissä pyritään välttämään ryhmädynamiikan normatiivisuuden sudenkuopat ja säilyttämään ryhmätilanteen konteksti. Esiin nousevat näkökantaerot ja ristiriitatilanteet huomioidaan systemaattisesti analyysivaiheessa aineistoon kuuluvina ominaisuuksina ja erityishuomion arvoisina nostoina. (Pietilä 2017.) Näitä yksittäiskokemuksia ja nostoja pidän aineiston arvokkaana antina, mutta koko organisaation kannalta kaikkein merkityksellisimpiä ovat ne huomiot, jotka saivat joukkokannatusta. Niistä voidaan päätellä, että koulutuksen osalta olisi mahdollisuuksia kohottaa työntekijöiden valmiuksia yleisemmällä tasolla. Yksittäisten nostojen merkitystä ei kuitenkaan kvalitatiivisesti käsitellyssä aineistossa voi sitäkään ohittaa.

Aineiston analysointia suoritettiin induktiivisen sisällönanalyysin keinoin, eli aineistosta esille nousseita kategorioita poimien sekä sitten näitä esille nousseita käsitteistä teemoitellen. Aineiston tulkinnassa huomioitiin kuitenkin myös yksittäisetkin nostot, jos ne toivat kehittämistyön tavoitteelle lisäarvoa. Tavoitteena oli analysoida aineistoa, ei luoda siitä synteesia, sillä teoria ei tässä kohtaa palvelisi organisaation tavoitetta parantaa toimintatapoja. (Hirsijärvi & Hurme 2022, 7.4-7.5)

3.3 Kehittämistyön tavoitteet ja riskit

Kehittämistyön tavoitteena oli kehittää yritys X:n tietoturvallisuuden tasoa erityisesti tiedon suojaamisen osalta vaihtelevissa hybridityöolosuhteissa ja tähän tavoitteeseen pyrin löytämällä organisaation jäsenten kokemuksista kehittämiskohteita. Havaittujen kehittämiskohteiden kautta opinnäytetyöni tuottaa työelämän lisäarvoa. Työelämäkumppanina toimivalle yritys X:lle yhteistyön arvoa tuovat konkreettiset kehittämiskohteet, joilla toimintaa voidaan sujuvoittaa ja tiedon suojaamisen tasoa parantaa.

Yksilöhaastatteluissa ja ryhmäkeskusteluissa esille nousseiden mahdollisten ongelma- ja epäkohtien poimiminen teemoittelemalla kerätyn aineiston sisällöstä tuo juuri sitä kokemusperäistä tietoa, joka auttaa parantamaan tietoturvakoulutusta ja osaamista tiedon suojaamiseen liittyen. Yksittäinenkin löydetty huomio, joka kuvaa tapahtunutta ongelmatilannetta, voi parantaa koko yrityksen tiedon suojaamisen tasoa. Teoriassa olemassa oleva, jatkuva tietoturvaluuskoulutus kattaa aiheen kuin aiheen, mutta käytännössä niin sanotusti kentällä tulkinnan vaikeus saattaa aiheuttaa ongelmatilanteita.

Opinnäytetyön riskien arvioinnin korkeimmat pisteet sai haastattelujen ja ryhmäkeskustelujen peruuntuminen. Muita korkean riskin tekijöitä olivat oma fyysinen terveys, ja tilaisuuksien tallenteiden katoaminen/korruptoituminen. Fyysisen terveyden riski realisoitui, mutta sen vaikutus oli kokonaisuuden kannalta lopulta vähäinen. Tallenteiden osalta riskiä mitigoitiin käyttämällä kahdennettua tietovarastoa niiden säilyttämiseen, niin fyysistä tietovarastoa kuin pilvitallennustilaakin. Tilaisuuksien aikataulutuksella myös pienennettiin riskiä siitä, etteivät tilaisuudet olisi toteutuneetkaan linjatyön vaatimusten vuoksi.

4 Lähtökohdista tuloksiin

Kehittämistyötä varten kerätty aineisto kertoi osallistuneiden työntekijöiden henkilökohtaisesta kokemuksesta organisaation tiedon suojaamisen nykytilasta hybridityömallissa työskenneltäessä. Tavoitteena oli näiden subjektiivisten kokemusten kautta löytää mahdollisia kehityskohteita. Määrittäväksi tekijäksi muodostui työntekijöiden omakohtainen kokemus saadusta ohjeistuksesta ja vallitsevista käytänteistä verrattuna arkiseen työhön ja siinä vastaantuleviin tiedon suojaamista toimisto-olosuhteissa ja muualla tapahtuvassa työskentelyssä esiinnousseisiin haasteisiin. Lähtökohtaisesti kaikki työntekijät, niin pidemmän ajan yritys X:n palveluksessa olleet kuin vastapalkatutkin työntekijät olivat suorittaneet kaikki edellytetyt, organisaation tarjoamat koulutukset ja uudelleen koulutukset.

Löydösten ja organisaation oletetun tavoitetilan välinen ero osoittautui suhteellisen vähäiseksi, mutta työskenneltäessä tietosensitiivisten asioiden parissa on syytä kiinnittää

huomiota kaikkiin löydöksiin riskienhallinnan ja -käsittelyn nimissä. Yksittäisenkin työntekijän virhearviointi saattaisi aiheuttaa korvaamatonta mainehaittaa organisaatiolle.

4.1 Lähtökohdat ja etukäteisoletukset

Opinnäytetyön lähtökohtaisena oletuksena oli, että jotain kehitettävää organisaatiossa työskentelevät haastateltavat nostaisivat esiin, sillä harvoin, jos koskaan, voitaneen törmätä tilanteeseen, jonka kaikki kokisivat täydellisenä. Hypoteesi osoittautui oikeaksi, sillä ongelmiksi tai epäkohdiksi nousseita aiheita nousi esiin haastatteluissa ja keskusteluissa.

Avoin teemahaastattelu sekä ryhmäkeskustelu osoittautuivat toimiviksi tavoiksi saada juuritason tietoa siitä, miten työssään jatkuvasti sensitiivisiä tietoja käsittelevät työntekijät itse kokivat saamansa koulutuksen ja tiedon riittävyyden toimivan juuri heidän työtehtävässään vaihtelevissa fyysisissä työntekotilanteissa. Ryhmäkeskusteluissa saatiin tarkennuksia ja oivalluksia esille nousseiden aiheiden ympäriltä ja yksilöhaastatteluissa puolestaan päästiin ehkä hieman syvemmälle.

Opinnäytetyöhön osallistuneet työntekijät osallistuivat työpajoihin aktiivisesti ja toivat rohkeasti omia mielipiteitään esille. Aiheista syntyi hyvää keskustelua. Osittain tämä saattaa liittyä anonymitteettiyteen, mutta joka tapauksessa avoimuus ja vilkas keskustelu edesauttoivat tiedon saantia.

4.2 Tulokset

Aineiston kollektiivisista ja yksittäisistä huomioista löysin seuraavia kehityskohteita. Kollegojen avun merkityksestä tuli useita huomioita ja sitä kautta tiedon suojaamiseen liittyvänä mielenkiintoisena havaintona aivan ensimmäiseksi nousi esiin se, että mitä tuoreempi työntekijä, sen mieluummin hän halusi työskennellä toimistolta käsin. Tämä vaikutti vahvasti liittyvän epävarmuuden kokemukseen. Tätä en nähnyt kuitenkaan kehitysaikheeksi, vaikka se aineistosta esille nousikin.

Useimpien työntekijöiden hybridityöpisteet sijaitsivat kodeissa, joissa enemmän ja vähemmän oli mahdollista suojata tietoa ulkopuolisilta. Hybridityöskentelyä koskevia tiedon suojaamisen ohjeistuksia ei erityisesti oltu tarjottu, ja tämä nousi useammassa yhteydessä esille. Eräs huomioni oli myös, että vastaajien keskuudessa koettiin, että asiantuntijatyössä tiedon suojaamista olisi helpompaa toteuttaa kuin suoraan asiakasrajapinnassa työskenneltäessä.

Merkittäväksi löydökseksi koin sen, että tiedon luokitteluun liittyvää syventävää koulutusta jäätiiin kaipaamaan. Asiakasrajapinnassa työskentelevät olivat hyvin tietoisia siitä, että he toimivat organisaation edustajina ulos päin ja kokivat, että kohdennetumpi koulutus toisi heille varmuutta toimia arjessa. Samassa yhteydessä nousi esiin, että lisätiedon saantiin ei

kaikilla tuntunut olevan toimivia kanavia. Tämä oli suurin yllättänyt teema, joka aineistosta nousi.

Voimassa olevista koulutuskäytännöistä todettiin, että organisaation verkkokoulutukset useimmiten hoidetaan alta pois mahdollisimman vähällä vaivalla, koska niiden suorittamiseen menevä aika on pois linjatyöskentelystä. Tällöin ei jää aikaa pohtia itse aiheita, kun verkkotentti suoritetaan suoritus- eikä asiakeskeisesti. Varsinaista vuoropuhelua ei koulutusaineiston kanssa ehdi syntyä ja sitä kuitenkin jäätettiin kaipaamaan. Aineistosta nousi myös esille toive siitä, että työntekijöitä osallistettaisiin koulutusten suunnittelussa. Uudet työntekijät kokivat niin sanottua verkkotenttiähyä työhönperehtymisen ohessa, kun kaikki mahdolliset koulutukset tuli suorittaa nopeasti alta pois varsinaiseen työhön päästäkseen.

Varsinaisen aiheen ohi esille muutamassa yhteydessä nousi yritys X:ssä toteutettu tietosuojalähettiläskoulutus, joka sai kehuja toteutustavastaan ja -aikatauluistaan ja toivottiinkin, että tätä mallia voisi jalkauttaa myös muihin tietoturvallisuuteen ja tiedon suojaamiseen liittyviin koulutuksiin. Vuoropuhelu niin aineiston kuin kouluttajan kanssa koettiin niin tärkeänä, että toive läsnäolokoulutuksista oli käytännössä homogeeninen. Käsitukseksi jäi, että mainitussa koulutuksessa oli ollut mahdollisuus keskustella, esittää kysymyksiä ja jakaa kokemuksia ja mielipiteitä.

Erinomainen huomio eräältä osallistujalta oli, että motivaatio suorittaa koulutuksia kasvoi, kun koulutusten syyt perusteltiin. Merkityksellisyys oman tehtävän kannalta lisäsi mielenkiintoa koulutuksia kohtaan. Käytössä olevien koulutusten konkretia ja reflektoitavuus omaan arkeen koettiin matalaksi. Myös mahdolliset poikkeamien aiheuttamat seuraukset askarruttivat. Näistä syistä koulutukset koettiin varsin ylätasoisiksi, joku jopa viittasi tähän käyttäen sanaa norsunluutorninäkökulma. Samaa asiaa kuvaa myös hyvin erään toisen osallistujan suora kommentti ”löyhä kosketuspinta omaan työnkuvaan nähden”.

Pääteemoiksi nousivat siis tiedon luokittelun osaamisen kehittämistarve, koulutusten ylätasoisuus ja vuorovaikutuksen puute sekä tietoisuus yhteydenottokanavan olemassaolosta. Edellä mainittujen teemojen sisälle voidaan upottaa uusien työntekijöiden halu työskennellä lähityössä vanhempien kollegojen kanssa, vapaamman aikaresurssin käyttö koulutuksiin ilman huolta tuottavuuden kärsimisestä ja syy-seuraus -suhteiden avaaminen ja elävän elämän esimerkkien läpikäyminen.

5 Johtopäätökset ja kehittämisehdotukset

Oli ilahduttavaa huomata, että käytännössä kaikki osallistujat olivat suorittaneet tarjotut koulutukset ja niiden sisältö, annetusta kritiikistä huolimatta, koettiin, vaikkakin ylätasoiseksi, kuitenkin relevantiksi ja hyödylliseksi. Suurempaa konkretiaa ja kosketuspintaa

omaan tehtävään kaivattiin. Lisäksi esille nousi ongelmana se, ettei kaikilla ollut varmuutta mistä lisätietoa tiedon suojaamisen toteuttamiseen saisi. Työskentelypisteen sijaintiin ja sijaintien erityisolosuhteisiin liittyvää koulutusta ei osallistujien kokemusten mukaan oltu tarjottu.

Perustuen keskusteluissa ja haastattelutilaisuuksissa esille nousseisiin kehityskohteisiin, edellisessä luvussa ja kappaleessakin esitettyjen koettujen ongelma-kohtien purkamiseksi esitän ylätasoa, koko organisaatiota koskevien koulutusten lisäksi kohdennettuja, ryhmäkohtaisia koulutustapahtumia, joissa keskustelu ja kysymysten esittäminen mahdollistettaisiin. Vuorovaikutuksen ja konkreettisten, työssä vastaantulleiden tapausten käsittely ryhmätilanteessa lisäisi nähdäkseni kaikkien työntekijöiden varmuutta kohdata haastavia tilanteita omassa työssään. Tilaisuuksia voisi järjestää vaikkapa tiimipäivien yhteydessä vuosittain tai puolivuositain. Toinen vaihtoehto on järjestää vastaava tilaisuus haastavan tilanteen jälkeen niin sanottuna purkutilaisuutena - retronä, jossa tarvittaessa anonymisoituna casenä käytäisiin ryhmänä läpi mitä tapahtui, miten asiaa lähdettiin ratkaisemaan, mikä olisi ollut organisaation kannalta optimaalinen tapa hoitaa asia ja mitkä ovat ne kontaktipinnat, joista tukea saa. Teoksessaan Ohjaustyön opas (2020), luvussa 9 Sanna Vehviläinen sanookin: ”Ohjauskohtaamista voi pitää ongelmanratkaisutilanteena.”

Kaikki osallistujat ymmärsivät tiedon suojaamisen merkityksen niin asiakkaan kuin organisaation näkökulmasta ja oli hienoa havaita, miten jokainen halusi kehittää osaamistaan tälläkin osa-alueella. Tätä innokkuutta organisaation kannattaa hyödyntää tarjoamalla henkilöstölle mahdollisuus vaikkapa vapaaehtoiseen lisäkoulutautumiseen. Ehdotankin, että yritys X voisi tarjota työntekijöilleen esimerkiksi verkko-opiskelumateriaaleja tai vaikkapa aihepiiriin koulutuskokonaisuutta sopivalta yhteistyöorganisaatiolta.

Perustelut koulutusten tarpeellisuudesta ja niiden sitominen yksilön työnkuvaan varmasti lisääisivät ymmärryksen lisäksi motivaatiota suorittaa koulutuksia ja esille nousseen termin ’mekaaninen klikuttelu’ sijaan pyrkiä saamaan tarjotuista koulutusmateriaaleista oman tehtäväkuvan kannalta oleelliset asiat irti. Interaktiivisten koulutustilanteiden tarjoamat mahdollisuudet mielestäni hyödyttäisivät koko organisaatiota lisääntyneen osaamisen kautta sekä siltä kannalta, että koettaisiin organisaation välittävän juuritason työntekijöidenkin osaamistarpeista - heidän, jotka omien sanojensa mukaan toimivat organisaation kasvoina ulospäin.

Erityishuomiota ansaitsee myös ohjeistus hybridityöskentelyyn liittyen. Sensitiivisten asiakastietojen käsittely organisaation tiloissa mutta erityisesti näiden tilojen ulkopuolella edellyttää selkeitä käytäntöjä. Opinnäytetyöhön osallistuneiden työntekijöiden mielestä asiakkaalla, mökillä, kotona tai missä tahansa organisaation ulkopuolisessa sijainnissa tehtävää työtä ei ole tiedon suojaamisen kannalta ohjeistettu. Tilaturvallisuuden ottaminen

osaksi turvallisuuskoulutuskokonaisuuteen myös tiedon suojaamisen tarpeiden osalta on nähdäkseni siis tarpeellista. Mikäli tämä aspekti on jo osa koulutusmateriaalia, on mielestäni tarpeellista terävöittää koulutussisältöä tältä osin.

Minusta kaikkein tärkeimmäksi kehityskohteeksi nousi tiedon saannin kanavista tiedottaminen, sillä tämä nousi aineistossa monen henkilön nostamana esille. Huolestuttavan moni koki, ettei heidän tiedossaan ollut selkeää polkua, mistä tietoa tarvittaessa tiedon suojaamiseen liittyen saa. Tietoturvallisuuden tason turvaamiseksi ja tiedon suojaamisen varmistamiseksi kaikille työntekijöille tulee olla selvää, mistä ja keneltä apua ongelmatilanteissa voi kysyä ja ratkaisumalleja saada. Kaikissa tapauksissa ratkaisua ei oltu saatu esimerkiksi kollegoilta, esihenkilöiltä tai muilta tiedossa olleilta kontaktipinnoilta. Organisaation sisäisten verkkosivujen kautta oikeaa kanavaa ei oltu osattu löytää.

Tiedon suojaamiseen liittyen organisaatiossa on olemassa oikea kanava, mutta tieto siitä ei keräämäni aineiston perusteella ole saavuttanut kaikkia organisaation jäseniä. Intranet-tiedote, sähköpostitietoisku tai vastaavanlaisen informatiivisen viestin välittäminen koko organisaatioon olisi nopea ja helppo tapa korjata tätä asiantilaa. Sisäisten verkkosivujen osalta kyseistä organisaation osaa koskien hakusanojen tarkennukset saattaisivat olla toinen nopea, konkreettinen tapa parantaa löydettävyyttä. Näen organisaation tiedon suojaamisen kannalta ensiarvoisen tärkeäksi, että tämä informaatio olisi välittömästi työntekijöiden saatavilla.

Osa kehitysehdotuksista on helposti ja pienin resurssein toteutettavissa ja ne silti tuottavat merkittävää lisäarvoa organisaation tiedon suojaamisen kannalta, hybridityössä ja toimisto-olosuhteissakin. Osa kehitysehdotuksista vaatii suurempia muutoksia, osa lisäksi jonkinlaisia aikaresursseja, ja näillä on myös kustannusvaikutuksia. On selvää, ettei kaikkia muutoksia varmasti voida ainakaan nopealla aikataululla, tai välttämättä ollenkaan, toteuttaa, mutta toivon, että tässä opinnäytetyössä tehdyistä havainnoista on hyötyä tiedon suojaamisen kehittämisessä, erityisesti hybridityössä, mutta myös organisaatiossa kokonaisvaltaisesti. Hyvä on myös pitää mielessä J.K. Rowlingin Harry Potter -kirjasarjasta tutun henkilöhaamon auri Alastor Moodyn korostama alituisen valppauden periaate (2001, 206). Korostan vielä lopuksi jatkuvan oppimisen sekä niin yksilö- kuin organisaatiotasolla tapahtuvan omien toimintatapojen kriittisen arvioinnin merkitystä. Avainasemassa on myös organisaation sisäinen tieto kanavista, joista apua tarvittaessa saa.

Opinnäytetyöni lähti hyvin käyntiin ja kohderyhmän henkilöiden tavoittaminenkin osoittautui pienistä, kohderyhmän työkuormaan liittyvistä viiveistä huolimatta helpoksi. Tietopohjan selvittäminen ja sen auki kirjoittaminen eteni myös aikataulussa. Myös aineiston läpikäyminen ja teemojen käsittely ja kehitysideointi olivat hyvässä vauhdissa vielä loppukevästä 2022.

Valitettavasti odottamaton ja arvioimaton riski minun elämässäni realisoitui. Kaksi nopeatahtista työpaikanvaihdosta sekä uuden työn mukanaan tuomat haasteet ja jatkuva työmatkoilla olo viivästytti työn valmistumista merkittävästi. Tällaista riskiä en keväällä 2022 mitenkään osannut aavistaa enkä siihen varautua. Työkuormasta johtuva pitkä tauko aktiivisissa opinnoissa lisäsi opinnäytetyön valmistumisen viivettä entisestään.

Monessa kohdassa organisaatiossa on saatettu jo edistyä aineiston keräämisen ajankohdan tilanteesta, mutta moni johtopäätökseni varmasti on vieläkin ajankohtainen. Sensitiivisellä toimialalla on erityisen tärkeää, että toimintatavat, prosessiohjeet ja avunsaannin yhteyskanavat ovat kaikille organisaation jäsenille saavutettavissa nopeasti ja viiveettä. Esille nousseet teemat ovat kuitenkin kokemuserusteisesti yleistettävissä yli organisaatorajojen ja esittämäni kehitysehdotukset toteutettuina tuovat lisäarvoa ja varmuutta organisaatiossa työskentelevien arkeen ja siten tukevat organisaation tietoturvallisuutta.

Lähteet

Painetut

Helle, M. 2004. Etätyö. Edilex Libri.

Rowling, J.K. 2002. Liekehtivä pikari. Hämeenlinna: Karisto.

Sähköiset

EU. Mikä on rekisterinpitäjä tai tietojen käsittelijä? Viitattu 16.3.2022.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fi#viitteet

Elinkeinoelämän keskusliitto. Yritysturvallisuus. Viitattu 15.3.2022. <https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/>

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148. 2016. <https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI>

GDPR. 2016. Viitattu 18.2.202 <https://gdprinfo.eu/fi>

Helle, M. 2004. Etätyö. Edita.

Hirsijärvi, S. & Hurme, H. 2022. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Gaudeamus. E-kirja

Komission täytäntöönpanoasetus (EU) 2018/151. 2018. <https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32018R0151&from=FI>

Kyberturvallisuuskeskus. Viitattu 10.3.2022.

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tee-etatyosta-turvallista-vinkkiemme-avulla>

Kyberturvallisuuskeskus. Tietoturva. 2020. Viitattu 16.3.2022.

<https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva>

Laki sähköisen viestinnän palveluista FINLEX 917/2014. Viitattu 21.3.2024.

Liikenne- ja viestintäministeriö. Suomi tietoliikenneverkkojen kärkimaaksi - Digitaalisen infrastruktuurin strategia 2025. 2018.

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161066/LVM_10_2018_Suomi_tie

[toliikenneverkkojen_karkimaaksi_Digitaalisen_infrastruktuurin_strategia.pdf?sequence=1&isAllowed=y](#)

Lundgren, B. & Möller, N. 2019. Defining Information Security. Viitattu 15.5.2022.

<https://link.springer.com/article/10.1007/s11948-017-9992-1>

Malinen, J. 2022. Pandemian synnyttämä tapa tehdä töitä ajaa pahimmillaan työuupumukseen - Nämä viisi vinkkiä auttavat hybridityöarjen suunnittelussa. Helsingin Sanomat. Viitattu 10.5.2022. <https://www.hs.fi/hyvinvointi/art-2000008679807.html>

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. SanomaPro Oy. Helsinki. E-kirja.

Pakkokeinolaki FINLEX 806/2011. Viitattu 7.3.2022.

<https://www.finlex.fi/fi/laki/ajantasa/2011/20110806#V9>

Pietilä, I. Ryhmäkeskustelu. 2017. Toim. Hyvärinen, M., Nikander, P. & Ruusuvuori, J. Tutkimushaastattelun käsikirja. Vastapaino. Tampere. E-kirja.

Puusa, A. 2020. Haastattelutyypit ja niiden metodiset ominaisuudet. Toim. Juuti, P. & Puusa, A. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus. E-kirja.

RAKLI. Tulosraportti. Tulevaisuudenkestävät työympäristöt ja työympäristöjohtaminen - klinikka. Viitattu 17.3.2022. [Tulosraportti, Tulevaisuudenkestävät työympäristöt ja työympäristöjohtaminen -klinikka \(taiqa.com\)](#)

Ruusuvuori, J. & Tiittula, L. Tutkimushaastattelu ja vuorovaikutus. Toim. Hyvärinen, M., Nikander, P. & Ruusuvuori, J. Tutkimushaastattelun käsikirja. Vastapaino. Tampere. E-kirja.

Standardi. ISO/IEC 27000. 2020. Viittaaminen sähköisiin dokumentteihin tai niiden osiin. ISO.

Sutela, H. & Pärnänen, A. 2021. Koronakriisin vaikutus palkansaajien työoloihin.

Tilastokeskus. Viitattu 10.5.2022.

https://www.stat.fi/tup/julkaisut/tiedostot/julkaisuluettelo/ywrrp1_202100_2021_25870_net.pdf

Termipankki. Viitattu 10.5.2022. <https://termipankki.fi/tepa/fi/>

Tietosuojavaltuutetun toimisto. Tietosuojan vaikutustenarvioinnin ohje. 2021.

<https://tietosuoja.fi/documents/6927448/66036250/TVA+ohje.pdf/ff0b6e1b-5b89-e85e-a2e5-6c4bd4c0ccfc/TVA+ohje.pdf?t=1639729535787>

Tilastokeskus. Käsitteet. Viitattu 18.2.2022. <https://www.stat.fi/meta/kas/etatyo.html>

Tivi. Miten onnistua hybridityössä. 2021. Tietoviikko-lehti. [Miten onnistua hybridityössä? - Tivi](#)

Työsuojeluhallinto. Työsuojeluoppaita ja -ohjeita 35. Turvallisuusjohtaminen. 2010.
https://www.tyosuojelu.fi/documents/14660/2426906/Turvallisuusjohtaminen_TSO_35.pdf/ef0c3554-4593-49d6-9530-64c28f404cb0

Työturvallisuuskeskus 2017. Etätyössä turvallisesti. Digijulkaisu. Viitattu 10.5.2022.
https://ttk.fi/oppaat_ja_ohjeet/digijulkaisut/etatyossa_turvallisesti

Työterveyslaitos. Etätyö, hybridityö ja monipaikkainen työ. Viitattu 2.4.2022.
va<https://www.ttl.fi/teemat/tyoelaman-muutos/etatyo-hybridityo-ja-monipaikkainen-tyo>

Työturvallisuuslaki 738/02. Viitattu 19.2.2022.
<https://www.finlex.fi/fi/laki/ajantasa/2002/20020738>

Valtioneuvosto. Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä. 2022. Viitattu 22.3.2024.
<https://valtioneuvosto.fi/hanke?tunnus=LVM044%3A00/2022>

Valtiovarainministeriö. Tiedonhallintalautakunta. Suosituskokoelma tiettyjen tietoturvasäännösten soveltamisesta. 2021.
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163596/VM_2021_65.pdf?sequence=1&isAllowed=y

Valtonen, A. & Viitanen, M. 2020. Ryhmäkeskustelut laadullisena tutkimusmetodina. Toim. Juuti, P. & Puusa, A. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus. E-kirja.

Vehviläinen, S. 2020. Ohjaustyön opas. Yhteistyössä kohti toimijuutta. Gaudeamus. E-kirja

Kuviot

| | |
|--|----|
| Kuvio 1 Sopeuttamistoimet koronakriisin aikana (Sutela ym. 2021) | 7 |
| Kuvio 2 Virtuaalisen asiakastyön osuus (Sutela ym. 2021) | 8 |
| Kuvio 3 Työntekopaikat (Sutela ym. 2021) | 9 |
| Kuvio 4: Elinkeinoelämän yritysturvallisuusmalli (EK 2022.) | 12 |

Liitteet

| | |
|--|----|
| Liite 1: Ryhmäkeskustelun ja haastattelun apurunko | 32 |
|--|----|

Liite 1: Ryhmäkeskustelun ja haastattelun apurunko

Haastattelua/ryhmäkeskustelua tukeva runko

Lyhyt esittely itsestä, koulutuksesta ja opinnäytetyöstä.

Haastattelun tallennus osallistujien luvalla.

Haastateltavien lyhyt esittäytyminen epävirallisesti ja luokittelematta.

Tavoitteena vapautunut keskustelu, joka luontevasti kattaa apurungon aiheet.

Hybridityö

- Mitä hybridityö sinusta/teistä on
- Miten se poikkeaa toimistolla työskentelystä
- Miten tietoturva ja asiakastietojen suojaaminen toteutuu omassa hybridityössäsi
- Mitä mielestäsi pitää huomioida tietoturvaa ajatellen hybridilokaatiossa

Tietoturvallisuus ja tietoturva, tiedon suojaaminen

- Millaisen tietoturvakoulutuksen olette käyneet
- Missä vaiheessa työsuhdetta tämä koulutus oli
- Mitä asioita siinä korostettiin
- Miten koulutusta voisi parantaa, mitä siinä pitäisi korostaa
- Miten tiedon luokittelu on teille opetettu

Yleistä tietoturvallisuudesta

- Mistä saatte tarvittaessa lisätietoja
- Mihin ilmoitat, jos huomaat tietoturvaongelman/ Miten toimit, jos...
- Miten tietoturvaosaamistasi on päivitetty työsuhteen aikana

Kiitos