Käyttäjän tietoturvakäyttäytyminen organisaationkontekstissa ja vapaa-ajalla

Oulun yliopisto
Tietojenkäsittelytiede
Kandidaatin tutkielma
Karoliina Autio
2024

Tiivistelmä

Tietoturvaa tarvitaan suojaamaan yksityisten henkilöiden ja organisaatioiden tietoja ja resursseja. Kattavaa tietoturvaa ei voida saavuttaa pelkästään teknisin keinoin, vaan siihen tarvitaan ponnistelua myös käyttäjiltä. Organisaatioilla on yleensä enemmän resursseja ja vaihtoehtoja tietojensa turvaamiseksi, mutta kotikäyttäjät ovat itse vastuussa tietoturvastaan. Organisaatioilla on tietoturvaan liittyviä käytäntöjä ja koulutuksia, joita työntekijöiden tulee noudattaa. Käytäntöjen noudattamatta jättäminen voi johtaa esimerkiksi tietovuotoihin tai haittaohjelmien leviämiseen.

BYOD, eli Bring Your Own Device, on käytäntö, jossa työntekijät saavat tehdä töitä omilla henkilökohtaisilla mobiililaitteillaan, kuten kannettavilla tietokoneilla tai älypuhelimilla. Käytäntö on yleistynyt viime vuosina, ja siihen liittyy sekä hyviä, että huonoja puolia. BYOD on käytäntönä kustannustehokas ja voi parantaa työntekijöiden työmoraalia, mutta siihen liittyy monia tietoturvariskejä. Riskejä ovat muun muassa haittaohjelmat ja työntekijöiden väärinkäytökset.

Tutkimuksen tarkoitus oli tarkastella käyttäjän tietoturvakäyttäytymistä organisaatiossa ja vapaa-ajalla, sekä miten BYOD vaikuttaa tietoturvaan ja tietoturvakäyttäytymiseen. Tutkimusmenetelmänä oli analysoida aiempaa kirjallisuutta. Tutkimuksen tuloksia voivat hyödyntää esimerkiksi organisaatiot ja käyttäjät, jotka haluavat parantaa tietoturvaansa tai harkitsevat BYOD käytännön ottamista käyttöön.

Avainsanat

Tietoturvakäyttäytyminen, BYOD, Bring Your Own Device

Ohjaaja

Mikko Rajanen

Sisällysluettelo

Tiivistelmä 2
Sisällysluettelo 3
1. Johdanto 4
2. Tutkimusmenetelmä 6
3. Aiempi tutkimus 7
3.1 Tietoturvakäyttäytyminen organisaatioissa 7
3.2 Tietoturvakäyttäytyminen kotona 9
3.3 BYOD organisaatio- ja vapaa-ajan konteksteja sekoittavana ilmiönä 12
4. Pohdinta 15
5. Yhteenveto ja johtopäätökset 17
5.1 Johtopäätökset 17
5.2 Yhteenveto 18
Lähteet 19

1. Johdanto

Informaatioteknologia kehittyy jatkuvasti yhä älykkäämmäksi ja on isona osana organisaatioiden ja yksityisten käyttäjien toimintaa ja arkea. Myös tietoturvauhat ovat kehittyneet entistä vaarallisemmiksi ja vaikeammin tunnistettaviksi. Pilvipalvelut, virtualisointi, matkapuhelimet ja hämärtynyt raja työelämän ja yksityiselämän välillä ovat esimerkkejä muutoksista, jotka vaikuttavat organisaation tapaan käyttää informaatiota (Karlsson et al., 2022). Tietoturvamurtoja tapahtuu jatkuvasti, ja ne voivat maksaa organisaatioille miljoonia (Ramakrishnan et al., 2022). Yksi suurimmista tietoturvauhkista organisaatiolle on työntekijä, mutta Samalla työntekijä on kuitenkin tärkein voimavara organisaation tietoturvan parantamiseksi (Bulgurcu et al., 2010). Organisaation tietoturvakäytäntöjen on tarkoitus estää rikollista toimintaa, kuten hakkerointia, sopimattomilla verkkosivuilla vierailua ja yhtiön ohjelmiston varastamista (Stewart & Jürjens, 2017). Organisaatiot kouluttavat työntekijänsä noudattamaan näitä tietoturvakäytäntöjä, mutta kotona työskentelevät eivät välttämättä osallistu koulutukseen, ja näin ollen voivat olla huomattava tietoturvariski (Anderson & Agarwal, 2010).

Tietoturvakäyttäytymisestä organisaatioissa on tutkittu huomattavasti enemmän, kuin tietoturvakäyttäytymistä kotiympäristössä organisaation ulkopuolella, vaikka kotikäyttäjien tietoturva on tärkeää ei vain heidän itsensä vuoksi, mutta myös organisatorisesta näkökulmasta (Li & Siponen, 2011). Silti tiedetään, että kotikäyttäjät nähdään helppona kohteena kyberrikollisten näkökulmasta (Thompson et al., 2017) ja kotikäyttäjille suunnattuja tietoturvaohjelmia on hyvin vähän (Talib et al., 2010), eikä moni käyttäjä halua maksaa laitteidensa suojauksesta, vaan turvautuu ilmaisiin ohjelmiin, jotka tarjoavat minimaalisen suojan. Organisaatioille sen sijaan on tarjolla kaikenlaisia ohjelmia ja aloitteita tietoturvan parantamiseksi (Talib et al., 2010), ja organisaatiot tekevät suuria investointeja tietoturvanhallintajärjestelmiin ja edistyneeseen teknologiaan nykyisten ja tulevien uhkien torjumiseksi (Karlsson et al., 2022). Käyttäjän tietoturvakäyttäytymiseen voivat vaikuttaa monet eri tekijät, kuten muiden ympärillä olevien käyttäytyminen sekä käyttäjän tekemät omat havainnot esimerkiksi hyödyistä (Herath & Rao, 2009). Organisaatiot voivat yrittää suoraan vaikuttaa työntekijöiden käyttäytymiseen palkitsemalla tai rankaisemalla heitä (Siponen et al., 2010).

Informaation odotetaan olevan helposti saatavilla, jaettavissa maantieteellisesti eri paikoissa olevien työtovereiden kesken ja synkronoituvan automaattisesti (Karlsson et al., 2022). Nämä vaatimukset olivat mahdottomia täyttää muutamia vuosia sitten, mutta nykyään avaavat uusia liiketoimintamahdollisuuksia (Karlsson et al., 2022). Uudet työntekoon liittyvät trendit ja käytännöt voivat tuoda mukanaan uusia tietoturvariskejä organisaatioille. Laajasti käytössä oleva Bring Your Own Device, eli BYOD- käytäntö on työntekijöille hyödyllinen ja mieluisa, mutta se voi myös muodostaa merkittävän tietoturvariskin organisaatioille (Chen et al., 2021). Bring Your Own Device tarkoittaa käytäntöä, jossa työntekijöitä kannustetaan tekemään töitä omilla henkilökohtaisilla mobiililaitteillaan, kuten älypuhelimilla, tableteilla tai kannettavilla tietokoneilla (Olalere et al., 2015). BYOD- käytännöstä on nopeasti muodostunut enemmän sääntö, kuin poikkeus ja organisaatiot eivät voi estää sitä (Ratchford et al., 2022). Aihetta tarkastellaan seuraavien tutkimuskysymysten kautta; millaista käyttäjän tietoturvakäyttäytyminen on organisaatiokontekstissa ja vapaa-ajalla? Sekä millaista käyttäytyminen on BYOD käytännön kontekstissa? Kysymyksiä tutkittiin analysoimalla aiempaa kirjallisuutta

käyttäjien tietoturvakäyttäytymisestä, BYOD-käytännöstä ja siihen liittyvistä tietoturvariskeistä.

Tämän tutkimuksen tarkoituksena on tarkastella käyttäjien tietoturvakäyttäytymistä organisaatiossa ja vapaa-ajalla, kuten kotona, sekä painottaa tietoturvan tärkeyttä ympäristöstä riippumatta. Käyttäjät ovat tässä kontekstissa työntekijöitä ja kotikäyttäjiä. Lisäksi tarkastellaan, kuinka nopeasti yleistynyt BYOD ilmiönä vaikuttaa erityisesti organisaation tietoturvaan ja työntekijöiden tietoturvakäyttäytymiseen. Tutkimus voi auttaa ymmärtämään ihmisen tietoturvakäyttäytymistä eri ympäristöissä ja mitkä tekijät tähän vaikuttavat. Organisaatiot puolestaan voivat esimerkiksi hyödyntää tätä tietoa ja parantaa tietoturvaansa sen avulla, oli kyse sitten laitteista tai työntekijöistä. Lisäksi BYOD käytännön omaksumista pohtivat organisaatiot voivat vertailla sen hyviä ja huonoja puolia ja ohjeistaa työntekijöitään sen mukaisesti.

Luvussa kaksi esitellään tutkimusmenetelmät. Luvussa kolme käsitellään käyttäjän tietoturvakäyttäytymistä. Tämä on jaettu kahteen alalukuun, joista ensimmäisessä käsitellään tietoturvakäyttäytymistä organisaatioissa, ja toisessa tietoturvakäyttäytymistä vapaa-ajalla. Kolmannessa alaluvussa käsitellään BYOD käytäntöä. Neljännessä luvussa tuodaan tutkimuksen päätulokset esiin. Viides luku sisältää yhteenvedon tutkimustyön tuloksista.

2. Tutkimusmenetelmä

Tutkimuksen tekemiseen käytetty menetelmä on kirjallisuuskatsaus. Boell & Cecez-Kecmanovic, 2015 määrittelee kirjallisuuskatsauksen seuraavasti: kirjallisuuskatsaus on yleensä yleiskatsaus aiempaan tehtyyn tutkimukseen. Systematic literature review eli SLR on kirjallisuushaun tärkeyttä painottava menettelytapa, joka pyrkii tarjoamaan mahdollisimman hyvää materiaalia tutkimukselle.

Tutkimuksessa käytettyä materiaalia kerättiin käyttämällä Google Scholar hakukonetta ja eri tietokantoja, kuten Scopusta, ScienceDirect:ä, Emerald Insight:a, IEEE Xplorea ja Research Gate: a.

Tietoa etsittiin ensin hakulauseella user's and "information security" and behavior and organizational and free time and context, joilla löytyi Google Scholarista ja ScienceDirectistä yli 2000 tulosta. Lisäksi käytettiin hakulausetta Bring your own device and security, jolla löytyi 486 Scopuksesta ja 670 tulosta ScienceDirectistä, mutta lähes 19 000 tulosta Google Scholarista. Rajasin jälkimmäistä hakua viimeisen neljän vuoden aikana tehtyihin tutkimuksiin, jolloin tulosten määrä putosi noin 6 500 tulokseen. Hakulauseet olivat liian yleiskäsitteisiä, joten pyrin tekemään tarkempia hakuja tietynlaisilla hakulauseilla, jotka liittyvät suoraan tutkimusaiheeseeni ja tutkimuskysymyksiin. BYOD and "information security" and organizations tuotti 90–2 600 tulosta tietokannasta ja hakukoneesta riippuen. Muita käytettyjä hakulauseita olivat "information security behavior" and "at home", jolla Google Scholar ja ScienceDirect löysivät reilut 200 tulosta, mutta Scopus löysi vain 4. Seuraava hakulause oli "information security" and "in organizations", jolla tuloksia kertyi Google Scholarissa yli 17 000 ja Scopuksessa 505.

Löysin monia hyviä lähteitä käytettäväksi, vaikka tuloksia olikin välillä liikaa ja monet lähteet käsittelivät samoja asioita hyvin samalla tavalla. Kävin yleensä läpi 5–10 ensimmäistä sivua tuloksista. Pyrin etsimään ja valitsemaan lähteiksi sellaisia tutkimuksia ja artikkeleita, jotka parhaiten vastaisivat tutkimuskysymyksiini ja käsittelevät aihetta eri näkökulmista ja eri konteksteissa. Tulosten määrä vaihteli hyvin paljon eri hakusanojen ja -lauseiden välillä. Hakuja tehdessä tuli hyvin selväksi, mitä aiheita on tutkittu paljon ja mitä hyvin vähän tai ei juuri ollenkaan. Aluksi pelkäsin tämän muodostuvan ongelmaksi, mutta löysin kuitenkin tarpeeksi erilaisia lähteitä käsittelemään tutkielman eri osia.

Koska halusin tutkielmassani käsitellä erikseen käyttäjän tietoturvakäyttäytymistä kahdessa eri ympäristössä, sekä Bring Your Own Device -käytäntönä ja kontekstissa näihin kahteen eri ympäristöön, päädyin valikoimaan lähteiksi tutkimuksia ja artikkeleita, jossa perehdyttiin ihmisten tietoturvakäyttäytymiseen kotona ja organisaatioissa, sekä mitkä asiat vaikuttavat käyttäjän tietoturvakäyttäytymiseen kyseisissä ympäristöissä. Lisäksi keräsin lähteitä, joissa kerrottiin sekä BYOD- käytännöstä yleisesti, että siihen liittyvistä tietoturvariskeistä ja hyödyistä ja kuinka ne vaikuttavat organisaatioihin ja käyttäjiin.

3. Aiempi tutkimus

Organisaatioiden turvallisuus on ollut huolenaiheena internetin kehityksestä asti (Ratchford et al., 2022). Tietoturvaan liittyy lukuisia riskejä, joilla voi olla vakavia seurauksia, kuten mittavat rahalliset menetykset, tai se, että organisaatio menettää uskottavuutensa (Bulgurcu et al., 2010). Organisaatiot pyrkivät panostamaan teknologiaan tietoturva-asioissa, mutta hyvää tietoturvaa ei valitettavasti voida saavuttaa pelkästään teknisin keinoin, vaan tarvitaan vankka ymmärrys ongelmista ja siitä, kuinka itseään voi suojella (Talib et al., 2010). Sekä tutkijat, että ammatinharjoittajat ovat huomanneet, että työntekijöillä on tärkeä rooli organisaation ponnistelussa hyvän tietoturvan suhteen (Posey & Shoss, 2023). Ihmisen toimintaa pidetään jopa kaikista kriittisimpänä tekijänä organisaation tietoturvan hallinnassa (Stewart & Jürjens, 2017). Organisaatiot ovatkin alkaneet panostaa enemmän työntekijöiden kouluttamiseen tietoturva-asioissa (Anderson & Agarwal, 2010). Organisaation turvallisuuspolitiikan noudattaminen ja usein tapahtuva tietoturvakoulutus voivat positiivisesti vaikuttaa tietoturvallisuuden inhimilliseen puoleen (Stewart & Jürjens, 2017). Aiemmin suurin osa tietoturvan parantamiseksi tehdyistä ohjelmista ja suunnitelmista oli suunnattu organisaatioille, ja vain pieni määrä kotikäyttäjille (Talib et al., 2010). Silti useissa organisaatioissa työntekijät käsittelevät arkaluonteisia tietoja ilman minkäänlaista tietoturvakoulutusta (Yerby & Floyd, 2018). Tutkimukset käyttäjän tietoturvakäyttäytymisestä organisaatiokontekstissa ovat paljon yleisempiä, kuin kotikäyttäjien käyttäytymiseen liittyvät tutkimukset (Thompson et al., 2017). Organisaatio- ja kotiympäristön tietoturvakäyttäytymisessä on jonkin verran samankaltaisuuksia, mutta enemmän eroja, kuten tekninen tuki, koulutus ja sanktiot (Thompson et al., 2017). Monet tutkimukset ovat pyrkineet löytämään teknisiä ratkaisuja ohjelmistojen turvallisuuden parantamiseksi, mutta on välttämätöntä ymmärtää sosiotekniset näkökohdat vallitsevien ongelmien tunnistamiseksi ja ohjelmiston suojausprosessin tehokkuuden parantamiseksi (Arenas et al., 2024).

Henkilökohtainen tietojenkäsittely on laajentunut nopeasti ensisijaisesta tietokonepohjaisesta kattamaan erilaisia mobiililaitteita, ja tällä on vaikutusta yksityisten henkilöiden lisäksi organisaatioihin, jotka antavat työntekijöille mahdollisuuden käyttää henkilökohtaisia online-tilejä organisaation tietokoneilta, tai tukevat Bring Your Own Device -käytäntöä (Thompson et al., 2017). Mobiililaitteiden kehitys on parantanut niiden toiminnallisuutta ja laskentatehoa vuosien varrella niin paljon, että niitä voidaan käyttää sekä henkilökohtaisiin, että työtarkoituksiin (Wani et al., 2022). Pysyäkseen mukana jatkuvasti kasvavan älykkäiden mobiililaitteiden kulutuksessa työpaikoilla, monet organisaatiot ovat päättäneet omaksua Bring Your Own Device -käytännön sillä perusteella, että se positiivisesti parantaa liiketoimintaprosesseja (Downer & Bhattacharya, 2022). Hyötyjen lisäksi BYOD voi tuoda mukanaan huomattavia riskejä käyttäjille ja organisaatioille. Monet työntekijöiden käyttämät BYOD laitteet eivät esimerkiksi täytä organisaation tietoturvakäytäntöön liittyviä vaatimuksia (Musarurwa et al., 2018).

3.1 Tietoturvakäyttäytyminen organisaatioissa

Posey & Shoss, 2023) mukaan työntekijät voivat yhtä hyvin suojella organisaation etuja, kuin aiheuttaa vakavia vahinkojakin monilla eri tavoilla tahattomasti ja tahallaan. Stewart & Jürjens, 2017 mukaan työntekijöihin liittyvät tietoturvariskit johtuvat huonosta

tietoturvatietoisuudesta, huonosta tietoturvakoulutuksesta ja huonosti johdetuista työryhmistä. Parantaakseen tietoturvaa ja vähentääkseen riskejä, organisaatiot ovat luoneet tietoturvakäytäntöjä, joita työntekijöiden tulee noudattaa (Bulgurcu et al., 2010). Kyberturvallisuuskäytäntöjen toimeenpano ja menestys ovatkin vahvasti riippuvaisia yksilöiden käyttäytymisestä (Ramakrishnan et al., 2022). Usein työntekijää pidetään heikoimpana lenkkinä tietoturvaan liittyen, jonka vuoksi tietoturvakoulutus on erityisen tärkeää ja lähes kaikilla organisaatioilla onkin jonkinlainen koulutusohjelma tietoturvasta työntekijöilleen (Talib et al., 2010). Koulutusohjelmien tulisi korostaa niitä lopputuloksia, joihin työntekijät uskovat tietoturvakäyttäytymisen johtavan, kuten mahdollisiin olennaisiin kustannuksiin, hyötyihin ja turvallisuuteen (Anderson & Agarwal, 2010). Useimmat tietoturvakoulutuksen käyneet kokevat, että heidän tietoisuutensa tietoturvasta on kasvanut paljon tai hyvin paljon (Talib et al., 2010). Organisaatioiden olisi hyvä kouluttaa myös ylempiä esimiehiä valvomaan muiden työntekijöiden ja alaisten tietoturvakäyttäytymistä (Siponen et al., 2010), koska organisaation hallinto on vastuussa niiden toimintojen valvomisesta ja ohjaamisesta, jotka parantavat työntekijöiden tietoisuutta tietoturvasta (Stewart & Jürjens, 2017). Ylin johto yksin ei välttämättä kykene takaamaan onnistunutta riskinhallintaa, mutta sen on välttämätöntä toteuttaa ja valvoa tietoturvatoimia (Stewart & Jürjens, 2017).

Työntekijän tietoturvakäyttäytymiseen voi vaikuttaa esimerkiksi tämän asenne, aikaisempi kokemus, havaitut hyödyt ja mahdollinen vaikutus omaan tehokkuuteen (Ramakrishnan et al., 2022). Ahkeruutta pidetään hyvin tärkeänä ominaisuutena työntekijässä, mutta monien mielestä työntekijöiden ahkeruus on laskenut viime vuosien aikana (Ramakrishnan et al., 2022). Ahkeruuden puute voi johtaa huolimattomuuteen, ja huolimattomuus voi vaarantaa organisaation resurssit ja jopa maineen, puhumattakaan tietoturvasta (Siponen et al., 2010). Organisaatiot ovat pitkään käyttäneet erilaisia tapoja potentiaalisten uusien työntekijöiden testaamiseen nähdäkseen, sopivatko he osaksi organisaatiota (Ramakrishnan et al., 2022). Samalla tavalla organisaatiot voivat selvittää kandidaattien yleistä tietoturvakäyttäytymistä ja tarvetta tietoturvakoulutukselle, jonka perusteella tehdä palkkaamista koskevat päätökset (Ramakrishnan et al., 2022).

Työntekijöiden tietoturvakäyttäytymiseen organisaatioissa voidaan vaikuttaa sekä sisäisillä että ulkoisilla tekijöillä (Herath & Rao, 2009). Ulkoisesti työntekijän tietoturvakäyttäytymiseen vaikuttaa muun muassa muiden ympärillä olevien käyttäytyminen (Herath & Rao, 2009). Tämä tukee (Vedadi et al., 2021) argumenttia, jonka mukaan laumakäyttäytymisellä on suurempi osuus yksilöiden tietoturvakäyttäytymiseen, kuin yksilön henkilökohtaisesti havaitsemalla tehokkuudella. Esimerkki sisäisestä työntekijän tietoturvaan vaikuttavasta tekijästä on tämän havaitsema hyöty, joka voi seurata tämän tekemistä toimista (Herath & Rao, 2009). Johtamiskäytännöillä, valvontakäytännöillä ja työtovereiden sosialisoinnilla on myös huomattu olevan positiivinen yhteys työntekijöiden käsitykseen organisaation tietoturvailmapiiristä (Yerby & Floyd, 2018). Organisaatiokulttuurillakin voi olla merkitystä työntekijän tietoturvakäyttäytymisessä. Karlsson et al., 2022 tekemän tutkimuksen päätulos oli, että työntekijät, jotka luonnehtivat organisaationsa kulttuuria byrokraattiseksi, todennäköisemmin noudattavat organisaation tietoturvakäytäntöjä. Organisaatiot voivat vaikuttaa työntekijöiden tietoturvakäyttäytymiseen palkinnoilla, tai rangaistuksilla (Siponen et al., 2010). Erityisesti sanktioiden pelko vaikuttaa työntekijöiden käyttäytymiseen siten, että he todennäköisemmin noudattavat tietoturvakäytäntöjä, koska sanktio voi pahimmassa tapauksessa johtaa työsopimuksen purkamiseen (Siponen et al., 2010). Yllättäen palkinnoilla ei kuitenkaan Siponen et al., 2010 tekemän tutkimuksen mukaan ole suurta vaikutusta työntekijöiden

tietoturvakäytäntöjen noudattamiseen mahdollisesti siksi, että palkkiota ei sovelleta yksinomaan tietoturvakäytäntöjen noudattamisesta, tai ei sovelleta aineettomia palkkioita tietoturvakäytäntöjen noudattamisesta.

On mahdollista, että hyvistä aikomuksista huolimatta työntekijä voi vahingossa harjoittaa riskialtista käyttäytymistä, kuten tietoturvakäytäntöjen passiivista noudattamatta jättämistä, laiskuutta tai motivaation puutetta (Shropshire et al., 2015). Organisaatioiden täytyy selvittää, mitkä asiat parhaiten motivoivat työntekijöitä noudattamaan tietoturvakäytäntöjä (Herath & Rao, 2009). Suurin osa organisaation kohtaamista uhkista on peräisin internetistä, ja työntekijä voi asettaa organisaation tietoturvan vaaraan pelkästään klikkaamalla sähköpostiin saapunutta harmittomalta vaikuttavaa linkkiä, jakamalla salasanansa tai jättämättä internetin käyttöön liittyviä käytäntöjä noudattamatta (Ramakrishnan et al., 2022). Eri asemassa tai tehtävissä olevat työntekijät saattavat käyttäytyä eri tavoin tietoturvaan liittyen esimerkiksi siten, että yksi lukee organisaation tietoturvakäytännöistä todennäköisemmin kuin toinen (Yerby & Floyd, 2018). Organisaatioille on monia vaihtoehtoja hankkia työntekijöilleen tietoturvakoulutukseen resursseja, esimerkiksi ostamalla tai tilaamalla niitä (Yerby & Floyd, 2018). Ei riitä, että tietoturvakäytännöt ovat pelkästään työntekijöiden saatavilla, sillä ilman koulutusta ja tukea tietoturvakäytäntöihin liittyen, niistä ei ole juuri hyötyä (Yerby & Floyd, 2018). Tutkimukset ovat osoittaneet, että useat organisaatiot vähättelevät ihmisen käyttäytymisen keskeisyyttä tietoturvan hallinnassa, joka on aiheuttanut häiriöitä tietoturvassa (Stewart & Jürjens, 2017). Organisaatioiden täytyy sitoutua työntekijöiden kouluttamiseen, koska siihen tarvitaan aikaa, resursseja ja motivaatiota kummaltakin osapuolelta (Talib et al., 2010). Pienemmillä organisaatioilla voi kuitenkin olla vaikeuksia panostaa tietoturvakoulutukseen (Talib et al., 2010).

Lukuisissa tutkimuksissa on havaittu, että tietoturvaresurssien väärinkäyttö on suuri ongelma, joka havaitaan usein silloin, kun tietoturvaa lievennetään (Stewart & Jürjens, 2017). Työntekijöiden sopimaton käytös on johtanut siihen, että organisaatiot ovat keskittyneet asettamaan esteitä ja ennaltaehkäiseviä järjestelmiä työntekijöille tietokoneiden väärinkäytöksistä (Stewart & Jürjens, 2017). Rangaistus on usein toimiva tapa vaikuttaa työntekijöiden käyttäytymiseen ja ennaltaehkäistä riskialtista käytöstä. Siponen et al., 2010 tekemä tutkimus on osoittanut, että sanktioilla on merkittävä vaikutus työntekijöiden tietoturvakäytäntöjen noudattamiseen. Työntekijöiden täytyy uskoa, että tietoturvakäytäntöjen noudattamatta jättäminen huomataan nopeasti ja ankarat seuraamukset tapahtuvat yhtä nopeasti (Siponen et al., 2010).

3.2 Tietoturvakäyttäytyminen kotona

On hyvin yleistä, että yksittäiset tietokoneen käyttäjät eivät toteuta aikomustaan turvallisesta tietokonekäyttäytymisestä, jota on salasanan vaihtaminen usein, haittaohjelmien etsiminen, tärkeiden tietojen arkistointi ja se, että ei avaa epäilyttäviä sähköposteja (Shropshire et al., 2015). Tietotekniikan kotikäyttäjät ovat melko aliedustettuja, eikä heidän tietoturvakäyttäytymisestänsä löydy yhtä paljon tehtyjä tutkimuksia, kuin esimerkiksi tietoturvakäyttäytymisestä organisaatioissa (Thompson et al., 2017). Anderson ja Agarwal 2010 kuitenkin suorittivat kaksi tutkimusta kotikäyttäjän tietoturvakäyttäytymisestä. Ensimmäisessä tutkimuksessa käytettiin käsitteellisenä perustana suojamotivaatioteoriaa ja suunnitellun käyttäytymisen teoriaa. Tulokset osoittivat, että useat kognitiiviset ja psykososiaaliset komponentit vaikuttavat

kotikäyttäjien turvallisuuskäyttäytymiseen. Toisessa tutkimuksessa hyödynnettiin tavoitteellisen viljelyn ja itsenäkemyksen käsitteitä, jotta voitaisiin tutkia, kuinka ensimmäisessä tutkimuksessa tunnistettuihin turvallisuuteen liittyvien aikomusten proksimaalisiin tekijöihin voidaan vaikuttaa sopivilla viesteillä. Tämän tutkimuksen tuloksista kävi ilmi, että käyttäytymisen positiivisiin seurauksiin keskittyvät viestit voivat olla vaikuttavampia turvallisuuskäyttäytymisen yhteydessä.

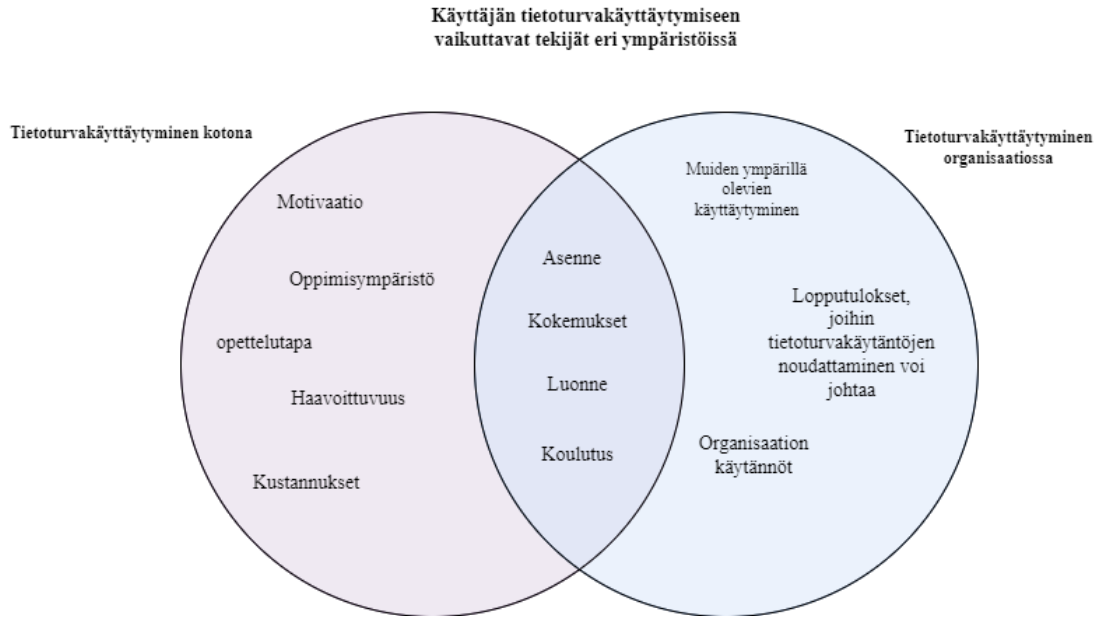
Kotikäyttäjien tietoturvallisuutta pitäisi silti tutkia enemmän, sekä heidän suojelemiseksensa ja siksi, että organisaatiotkin hyötyisivät siitä (Li & Siponen, 2011). Rikolliset valitsevat usein uhrikseen helppoja kohteita, ja kotikäyttäjät usein nähdään tällaisina (Thompson et al., 2017). Suurin osa tietoturvahyökkäyksistä kohdistuukin kotikäyttäjiin (Talib et al., 2010). Kotikäyttäjät saattavat tarjota tärkeää tietoa tunkeilijoille, kuten sähköposteja, pankkitunnuksia, pikaviestejä ja tietoja osakekaupoista, jonka vuoksi organisaatioidenkin pitäisi olla huolissaan kotikäyttäjien tietoturvasta (Li & Siponen, 2011). Kaapatut laitteet ovat oiva kasvualusta hakkereille ja laittoman ja kyseenalaisen materiaalin jakelijoille (Li & Siponen, 2011).

Kotikäyttäjien alttius tietoturvauhkille johtuu useimmiten siitä, että heillä ei yksinkertaisesti ole riittäväsi tietoturvaan liittyviä tietotaitoja, jotta he voisivat suojata laitteensa ja henkilökohtaiset tietonsa (Kritzinger & Von Solms, 2010). Kotikäyttäjien tietoturvatietämys tulee useimmiten työpaikalta, verkosta tai sanomalehdistä (Talib et al., 2010). Koti- ja työympäristön tietoturvakäyttäytymisessä on samankaltaisuuksia, mutta huomattavia eroja näiden kahden välillä ovat muun muassa teknisen tuen rooli, koulutus ja organisaation käytännöt (Thompson et al., 2017). Kotiympäristössä harvoin on apuna tekninen tuki tai olemassa tiettyjä käytäntöjä, joita tulisi noudattaa. Kukaan ei valvo tai varmista, että kotikäyttäjät saavuttavat tietoturvaan liittyvän tietoisuuden ja toteuttavat sitä (Kritzinger & Von Solms, 2010), jonka vuoksi kotikäyttäjät ovat merkittävä heikkous kyberinfrastruktuurin turvallisuuden saavuttamisessa (Anderson & Agarwal, 2010). Lisäksi kotiympäristössä yksilöt voivat valita, jos ja miten he toteuttavat tietoturvakäyttäytymistä, jonka vuoksi on mahdollista, että käyttäjän tietoturvakäyttäytyminen kotona eroaa käyttäytymisestä työpaikalla (Li & Siponen, 2011). Yksi käyttäytymisero voi esimerkiksi olla se, että työntekijän ei tarvitse asentaa vakoiluohjelmien torjuntaa laitteelle, koska organisaation IT-osasto tekee sen, mutta kotikäyttäjän täytyisi itse arvioida, sisältääkö laite riskejä ja tarvitsevatko he kyseistä ohjelmistoa (Li & Siponen, 2011). Toinen esimerkki on salasanaan liittyvät tavat. Työntekijät voivat pitää työhön liittyvän salasanan salaisena, koska siihen liittyy tiukka turvakäytäntö ja työntekijöiden täytyy ottaa huomioon ne vaikeudet, jotka seuraavat salasanan paljastamisesta muille (Li & Siponen, 2011). Omien salasanojen salassa pitämiseen ei liity määräyksiä, ja niitä voi vaikka jakaa kenelle tahansa halutessaan (Li & Siponen, 2011).

Kasvava internetin käyttö muun muassa sosiaaliseen verkostoitumiseen ja pankkiasioiden hoitamiseen asettaa tietämättömät kotikäyttäjät asemaan, jossa he saattavat paljastaa liikaa itsestään (Kritzinger & Von Solms, 2010). Riippuvuus tietokoneista ja internetistä on tehnyt käyttäjistä entistä haavoittuvampia ja alttiita tietoturvauhkille (Arenas et al., 2024). Ennen ostokset ja pankkiasiat hoidettiin tietokoneella, mutta nykyään yhä enemmän älypuhelimilla ja tableteilla (Thompson et al., 2017). Silti on huomattu, että useat käyttäjät käyttäytyvät vähemmän turvallisesti mobiililaitteiden kuin kotitietokoneiden kanssa ja harkitsevat vain kotitietokoneiden turvallisuusuhkia (Thompson et al., 2017). Kuten muukin käyttäytyminen, tietoturvakäyttäytyminen on opittua käyttäytymistä, johon vaikuttavat monet tekijät, kuten motivaatio, ympäristö,

jossa opetellaan ja tapa, jolla opetetaan (Talib et al., 2010). Myös luonteella on huomattu olevan vaikutus käyttäjän käyttäytymiseen asenteen ja aikomuksen lisäksi (Shropshire et al., 2015). Tärkeimpiä vaikuttajia tietoturvakäyttäytymiseen ja aikomuksiin ovat havaittu haavoittuvuus, vastauskustannukset ja psykologinen omistajuus (Thompson et al., 2017). Tutkijoiden on kuitenkin ollut vaikea ennustaa turvallisuuden noudattamista koskevaa käyttäytymistä, koska käyttäytymistarkoituksen ja todellisen käyttäytymisen välillä on liikaa tuntemattomia muuttujia (Shropshire et al., 2015). Monet käyttäytymistä tutkivat tietoturvatutkimukset käyttävät aikomukseen perustuvia malleja, jotka puolestaan käyttävät käyttäytymistarkoitusta todellisen käyttäytymisen sijaisena, mutta yksilöt eivät aina välttämättä käyttäydy kuten ovat aikoneet (Thompson et al., 2017). Näistä tutkimuksista on silti ollut paljon hyötyä kotikäyttäjien tietoturvakäyttäytymisen ymmärtämisessä (Arenas et al., 2024). Arenas et al., 2024 tekemän tutkimuksen mukaan tietoturvatyökaluilla- ja toiminnalla on erilaiset vaikutukset esimerkiksi haittaohjelmien tarttumisessa. Tietoturvatyökaluilla on positiivisempi vaikutus, mutta niihin ei kannata tukeutua liikaa.

Kritzinger & Von Solms, 2010 mukaan kotikäyttäjille suunnattuja tietoturvaohjelmia on huomattavasti vähemmän, kuin muille. Ne ovat usein verkko-ohjelmia, joita aloittelevan kotikäyttäjän on vaikea löytää, eivät ole tarpeeksi ymmärrettäviä, eivätkä käsittele kaikkia oleellisia tietoturvaongelmia. Kotikäyttäjien on vaikea hankkia syvällisempää tietoturvatietämystä, koska tietoturvaohjelmia tarjoavat verkkosivut eivät tarjoa dynaamista vuorovaikutusta käyttäjien kanssa esimerkkien tai harjoitusten muodossa. Ohjelmia ei myöskään päivitetä tarpeeksi usein, jotta ne kattaisivat uudet kasvavat teknologiat. Koska työympäristössä opitut tietoturvakäytännöt siirtyvät käyttäjien mukana kotiympäristöön, olisi mahdollista siirtyä tietynlaisista organisaation tietoisuusohjelmista tietoisuutta lisääviin strategioihin, jotka kehittäisivät monipuolista ja yksilöllistä tietoturvakulttuuria käyttäjille riippumatta ympäristöstä, jossa he toimivat (Talib et al., 2010).



Kuva 1. Käyttäjän tietoturvakäyttäytyminen eri ympäristöissä.

3.3 BYOD organisaatio- ja vapaa-ajan konteksteja sekoittavana ilmiönä

BYOD, eli Bring Your Own Device, -ilmiö tarkoittaa työntekijöiden henkilökohtaisten mobiililaitteiden ja sovellusten tarjontaa ja käyttöä sekä yksityisiin, että työtarkoituksiin (Barlette et al., 2021). Työntekijät valitsevat yleensä mieluummin laitteet, joilla he työskentelevät, mikä tuo tyydytystä ja tyytyväisyyttä heille (Musarurwa et al., 2018). Lisäksi mahdollisuus työskennellä tutuilla laitteilla missä vain lisää työntekijöiden joustavuutta ja vähentää turhautumista (Chen et al., 2021). Näiden hyötyjen vuoksi BYOD onkin työntekijöiden suosiossa. Barlette et al., 2021 mukaan uudet käytännöt organisaatioissa otetaan yleensä käyttöön ylemmän johdon aloitteesta, mutta BYOD on poikkeus tähän kirjoittamattomaan sääntöön, sillä useimmissa tapauksissa sen omaksuminen on lähtöisin työntekijöistä, usein ilman minkäänlaisia säännöksiä tietoturvasta. Tämä voi olla yksi syy, miksi kaikki organisaatiot eivät ole olleet yhtä innokkaita ottamaan BYOD- käytäntöä käyttöön, kuin toiset (Downer & Bhattacharya, 2022). Toisaalta Garba et al., 2015 mukaan motivaatio BYOD:n takana on lähtöisin 1980-luvun organisaatioista, jotka kuvailivat ihanteellista työntekijää luovaksi, oma-aloitteiseksi ja päättäväiseksi ja joka saisi asiat hoidettua kaikin keinoin jopa maantieteellisistä rajoista riippumatta. Työntekijät halusivat todistaa pätevyytensä työnantajilleen ottamalla käyttöön uusia ja nopeita tapoja työskennellä (Garba et al., 2015). COVID-19 pandemian pakotti lopulta vastahakoisemmatkin organisaatiot hyödyntämään BYOD- käytäntöä helpottaakseen etätyöskentelyä (Downer & Bhattacharya, 2022). Monikäyttöiset ja kaikkialla läsnä olevat mobiililaitteet olivatkin avain mahdollistamaan etätyöskentelyn maailmalaajuisesti (Wani et al., 2022). Suuret muutokset ja epävarmat ajat kuitenkin houkuttelevat organisaation ulkopuolisia hyökkääjiä hyödyntämään tilannetta ja kehittämään sosiaalisia taitojaan, kuten työntekijöiden manipulointia petoksen avulla (Posey & Shoss, 2023). Siirtyminen etätyöskentelyyn tapahtui lähes yhdessä yössä, eivätkä monet organisaatiot olleet riittävän varautuneita käsittelemään niin monia fyysisesti eri paikkoihin sijoittuneita työntekijöitä, jonka vuoksi johtajat turvautuivat hätäisesti koottuihin käytäntöihin etätyöskentelystä (Posey & Shoss, 2023). Koska BYOD on kehittyvä ilmiö, organisaatioiden on ymmärrettävä täysin sen tuomat mahdolliset turvallisuusriskit, joita se tuo organisaatiolle ja että turvatoimenpiteiden tai -politiikkojen toteuttaminen voi tehokkaasti suojata sen tietoturvaa (Tu et al., 2019).

Olalere et al., 2015 mukaan kaikista BYOD:n haasteista suurimaksi on koettu tietoturvaan liittyvät riskit, joita voivat olla esimerkiksi haittaohjelmat, tietovuodot ja tietomurrot, koska organisaation IT-osasto ei hallinnoi työntekijöiden omistamia laitteita. Vuonna 2017 yli puolet työntekijöiden omistamista laitteista oli syyllinen organisaation tietomurtoihin (Barlette et al., 2021). Tietomurrot eivät vaaranna vain organisaatiota, sillä ne saattavat tarjota pääsyn organisaation ulkopuolisiin kumppaneihin verkon tai muun digitaalisen vaihtokaupan kautta, joka tekee heistä haavoittuvampia kyberhyökkäyksille (Barlette et al., 2021). Silti hyvin monet organisaatiot sallivat omien laitteiden käytön ja niiden yhdistämisen yhtiön tietoverkkoon, ja yllättävän moni organisaatio jopa luottaa siihen, että työntekijöillä on omat laitteet tähän tarkoitukseen (Tu et al., 2019). Organisaatioilta usein kuitenkin puuttuu kirjatut ja allekirjoitetut käytännöt ja sopimukset BYOD:n liittyen (Downer & Bhattacharya, 2022). Organisaatiot voivat jäljittää ja valvoa työntekijöiden verkkokäyttäytymistä, jos he käyttävät mobiililaitteiden hallintatyökaluja (Garba et al., 2015). BYOD tietomurtojen vuoksi organisaatiot ovat alkaneet toteuttaa hallintatoimenpiteitä, joiden avulla he voivat esimerkiksi etänä tyhjentää tiedot BYOD

laitteilta, pakkoasentaa sovelluksia, sekä etänä valvoa laitteen käyttöä (Garba et al., 2015).

BYOD:n liittyvät huonot puolet eivät rajoitu vain organisaatioihin. Vaikka käytäntö on laajasti työntekijöiden suosiossa, he myös kokevat, että raja työnteon ja vapaa-ajan, sekä organisaation ja henkilökohtaisten tietojen välillä hämärtyy (Garba et al., 2015). Työntekijöiden voi myös olla vaikea sovittaa yhteen henkilökohtaiset käyttötottumukset ja organisaation turvallisuusvaatimukset (Chen et al., 2021). Garba et al., 2015 on listannut monia muitakin työntekijöiden huolia BYOD:n liittyen; työntekijät ovat huolissaan yksityisyydestään ja henkilökohtaisista tiedoistaan. He kokevat yksityisyytensä loukatuksi, jos työnantaja valvoo heidän henkilökohtaisia mobiililaitteitaan, jonka vuoksi työntekijät haluavat rajoittaa työnantajan pääsyä laitteilleen muun muassa epäämällä työnantajilta pääsyn laitteille asennettuihin sovelluksiin. Työntekijät myös pelkäävät, että työnantajat valvovat heidän verkkokäyttäytymistänsä laitteilla työajan ulkopuolellakin. Pelko henkilökohtaisten tietojen häviämisestä laitteilta on myös läsnä etänä tapahtuvien tietojen tyhjennysten vuoksi (Garba et al., 2015). Lisääntynyt valvonta ja kohonnut huoli työntekijöiden yksityisyydestä on saanut työntekijöitä edustavat liitot vaatimaan organisaatioille lisää ohjesääntöjä työntekijöiden turvaksi (Posey & Shoss, 2023). Riippumatta siitä, sallivatko työntekijät työnantajilleen pääsyn laitteilleen, heidän tulisi toteuttaa hyviä tietoturvakäytäntöjä. Käytäntöjä ovat esimerkiksi laitteen suojaaminen vahvalla salasanalla, kuviolla tai biometrisella tunnistuksella ja asettamalla jokaiselle sovellukselle omat käyttäjätunnukset (Wani et al., 2022).

BYOD turvallisuutta ei ole vieläkään tutkittu tarpeeksi, koska se on edelleen melko nuori verrattuna muihin verkon tietoturvaongelmiin, joka puolestaan on johtanut siihen, että organisaatiot ratkaisevat tietoturvahyökkäyksiä ja sulkevat porsaanreikiä niiden näyttäytyessä (Downer & Bhattacharya, 2022). Työntekijöitä houkuttelee BYOD:n tuomat hyödyt, mutta organisaatioiden täytyy harkita tarkkaan käytännön hyödyntämistä (Chen et al., 2021). Organisaatioita uhkaavat niin sisäiset kuin ulkoisetkin tekijät, kuten virukset ja työntekijöiden asiaton tiedon ja muiden resurssien käyttö (Chen et al., 2021). Työntekijöiden luvaton pääsy ja arkaluontoisten tietojen jääminen entisten työntekijöiden laitteille ovat BYOD:lle omia uniikkeja tietoturvariskejä (Downer & Bhattacharya, 2022). Henkilökohtaisen ja yritystietojen yhdistäminen samalla laitteella muodostaa suuren uhan organisaatioille arkaluonteisten tietojen tarkoituksellisen tai tahattoman paljastamisen vuoksi (Tu et al., 2019). Organisaatioiden on varmistettava, että tietojen luottamuksellisuus, eheys ja saatavuus säilyvät (Ratchford et al., 2022). BYOD ei kuitenkaan ole hyödyllinen pelkästään työntekijöille. Riskeistä huolimatta organisaatiotkin voivat hyötyä sen käytöstä (Coker, 2022). On kustannustehokasta sallia työntekijöiden käyttää omia laitteitaan työn tekemiseen sen sijaan, että organisaatio kustantaisi heille tarvittavat laitteet (Coker, 2022). Organisaatiot voivat säästää useita satoja dollareita työntekijää kohden vuosittain BYOD mahdollisuuksien ansiosta (Barlette et al., 2021). Koska työntekijät pitävät itse huolta laitteistaan, organisaation ei tarvitse käyttää yhtä paljon IT-palveluita laitteiden hallintaan, jolloin niiden resursseja voidaan hyödyntää tehokkaammin (Tu et al., 2019). Organisaatioita palvelee myös työntekijöiden kohonnut tuotteliaisuus ja suoriutuminen, sillä BYOD tarjoaa työntekijöille tehokkaan kanavan yhteistyöhön kollegoiden välillä ja vuorovaikutukseen asiakkaiden kanssa (Coker, 2022 ja Zhiling Tu et al., 2019). Tietosuojan lisäksi BYOD:n käyttöönotto pakottaa organisaatiot pohtimaan henkilökohtaisten tietojen suojausta, sekä oikeudellisia näkökohtia, jotka voivat negatiivisesti vaikuttaa organisaatioon, jos ne jätetään käsittelemättä (Ratchford et al., 2022).

Tutkijat ovat selvittäneet, mitkä tekijät vaikuttavat työntekijöiden aikomuksiin noudattaa nimenomaan organisaation BYOD:n liittyviä tietoturvakäytäntöjä; Tulokset osoittavat, että havaittu tehokkuus vaikuttaa erityisesti silloin, kun laite sisältää sekä henkilökohtaisia tietoja, että organisaation liiketoimintaan liittyviä tietoja (Tu et al., 2019). Mukana kannettavissa laitteissa onkin se riski, että ne saattavat kadota tai tulla varastetuiksi, jolloin organisaation tietoturva on uhattuna (Tu et al., 2019). Työntekijät ovat myöntäneet käyttävänsä hyväksi porsaanreikiä, kun he ovat eri mieltä BYOD tietoturvakäytännöistä, tai kun heillä on vaikeuksia käyttää käytännön turvallisuusmenetelmiä (Downer & Bhattacharya, 2022). Organisaation ulkopuolella olevat BYOD laitteet saattavat joissain tapauksissa olla yhteydessä suojaamattomaan verkkoon, josta haittaohjelmat saattavat päästä laitteeseen, ja kun laite yhdistetään taas organisaation verkkoon, haittaohjelma pääsee leviämään (Tu et al., 2019). Lisäksi kaikissa mobiililaitteissa, kuten matkapuhelimissa, ei välttämättä ole virusten torjuntaohjelmia suojaamassa niitä (Tu et al., 2019).

Organisaatioiden kannattaa lähestyä BYOD tietoturvaa loppukäyttäjän näkökulmasta, sillä se voi paljastaa heikkouksia, joita voidaan käyttää mahdollisten sisäisten uhkien havaitsemiseen tarjoamalla tietoa työntekijöiden laitteiden käyttötavoista (Downer & Bhattacharya, 2022). Tällä tavoin voidaan vahvistaa BYOD turvallisuutta varoittamalla organisaatioita tietyistä uhkista ja ehkäistä tulevaisuuden uhkia (Downer & Bhattacharya, 2022). Ratchford et al., 2022 argumentoi, että päätös BYOD:n käyttöönotosta tulee tehdä organisaation hallituksen tasolla, koska hallinto on erittäin tärkeää BYOD:n onnistumisen kannalta. Organisaation johdon tulee valvoa BYOD:n käyttöä, ja määritellä sille linjaukset (Ratchford et al., 2022). Koska BYOD laitteet eivät yleensä ole yrityksen omistamia, turvatoimia ja käytäntöjä toteutetaan harvemmin henkilökohtaisilla laitteilla (Tu et al., 2019). Yksittäisten työntekijöiden täytyy ottaa vastuu oman laitteensa käytön turvallisuudesta, jonka vuoksi on arvokasta tutkia, kuinka työntekijät noudattavat organisaation turvallisuustoimenpiteitä ja -käytäntöjä BYOD turvallisuusuhan vähentämiseksi (Tu et al., 2019). Inhimillisiä tekijöitä, jotka on myös otettava huomioon BYOD:n suunnittelussa, ovat koettu luottamus, koettu hyödyllisyys ja työntekijöiden koettu helppokäyttöisyys (Coker, 2022). BYOD laitteiden käyttöä voitaisiin tehdä turvallisemmaksi esimerkiksi kaksivaiheisen todennuksen avulla, jolla voidaan estää luvaton pääsy organisaation resursseihin (Olalere et al., 2015). Järjestämällä pakollista koulutusta organisaatiot voivat lisätä työntekijöiden tietoisuutta BYOD:n liittyvistä tietoturvauhkista, käytännöistä ja vastatoimista (Tu et al., 2019). Organisaatiot voivat kannustaa työntekijöitä osallistumaan koulutukseen tarjoamalla palkkion ja alustan keskustelulle ongelmista (Tu et al., 2019). Organisaation käytäntöjä vahvistamalla voidaan vahvistaa myös työntekijöiden tietämystä kyberriskeistä ja rohkaista heitä auttamaan organisaatiota suojelemalla itse laitteitaan, jolloin voidaan vähentää tietovuotoja ja haittaohjelmien leviämistä (Downer & Bhattacharya, 2022). Organisaatioiden olisi hyvä myös hyödyntää monikäyttöisiä BYOD:lle suunnattuja mekanismeja, jotka sisältävät esimerkiksi valvontakäytäntöjä mobiililaitteille ja sisäänrakennettuja etätyhjennystoimintoja (Downer & Bhattacharya, 2022).

4. Pohdinta

Tämän tutkimuksen tavoitteena oli tutkia käyttäjän tietoturvakäyttäytymistä organisaatiokontekstissa ja vapaa-ajalla, sekä miten BYOD ilmiönä vaikuttaa tähän. BYOD tuo nämä kaksi ympäristöä yhteen ja voi sumentaa rajaa niiden välillä. Hain vastausta siihen, miten käyttäjän tietoturvakäyttäytyminen kotiympäristössä eroaa tietoturvakäyttäytymisestä organisaatiokontekstissa, ja mitkä tekijät vaikuttavat käyttäytymiseen näissä kahdessa ympäristössä. Tämän lisäksi hain vastausta BYOD:n vaikutuksista organisaation tietoturvaan ja tietoturvakäyttäytymiseen. Vastauksia kysymyksiini hain lukemalla ja analysoimalla aiempaa kirjallisuutta aiheista.

Ihmiset ovat nykyään yleisesti tietoisia verkossa vaanivista uhkista. Kaikki eivät kuitenkaan välttämättä ymmärrä niiden vakavuutta, ja kuinka helposti niille voi altistua. Lähes kaiken asioinnin voi hoitaa nykyään helposti ja nopeasti verkossa, kuten pankki asiat, ostokset, sosiaalisen verkostoitumisen ja työskentelyn, jonka vuoksi olemme nykyään hyvin riippuvaisia tietokoneista ja internetistä. Informaatioteknologian jatkuva kehitys tuo usein mukanaan uusia uhkia, ja vanhat kehittyvät vaarallisemmiksi. Varoittavista uutisista ja tiedotteista huolimatta moni joutuu tietomurtojen, haittaohjelmien ja kyberrikollisten uhriksi. Kotikäyttäjät ovat edelleen erityisen haavoittuvaisia tietoturvan suhteen. Puutteellisesta tietoturvasta voi aiheutua vakaviakin rahallisia tai sosiaalisia vahinkoja. Kuitenkaan mahdollisuuksia suojautua ei ole yhtä kattavasti, kuin kokonaisille organisaatioille. Moni kotikäyttäjä ei halua tai kykene maksamaan rahaa ja vaivaa kunnollisesta suojauksesta ja tyytyy ilmaisiin vaihtoehtoihin, jotka eivät välttämättä ole tarpeeksi tehokkaita. Lisäksi kotikäyttäjien voi olla vaikea edes löytää tietoa siitä, miten he voivat parantaa omaa tietoturvaansa.

Etätyöskentely oli ennen maailmanalaajuista pandemiaakin melko yleistä työpaikoilla ja korkeakouluissa, eivätkä kaikki organisaatiot ole palanneet siitä entiseen työskentelytapaan sen jälkeen. Jotta etätyöskentely olisi mahdollista, täytyy työntekijöillä olla pääsy tarvittaviin organisaation resursseihin ja käyttäjätileihin. Etätyöskentelyyn liittyy kuitenkin riskejä, jotka organisaation on huomioitava. Varojen ja muiden resurssien turvaamiseksi organisaatioilla on tietoturvakäytäntöjä, joiden ymmärtämisen ja noudattamisen varmistamiseksi työntekijöille järjestetään koulutusta. Töistä saatujen tietojen ja taitojen avulla käyttäjät voivat oppia suojaamaan laitteensa myös kotona. Kaikki työpaikat eivät välttämättä tarjoa tietoturvakoulutusta resurssien puutteen tai muun syyn vuoksi, mutta tietoa siitä voidaan saada muualtakin. Organisaatioissa työntekijät yleisesti noudattavat tietoturvakäytäntöjä siksi, että se nähdään hyödyllisenä. Työntekijät saattavat myös pelätä seurauksia käytäntöjen noudattamatta jättämisestä. Organisaatiokontekstissa on monia sisäisiä ja ulkoisia tekijöitä, jotka vaikuttavat käyttäjän tietoturvakäyttäytymiseen. Näitä tekijöitä ovat muun muassa muut ympärillä olevat ihmiset ja käyttäjän itse havaitsemat hyödyt. Yhtä hyvin työntekijä saattaa tarkoituksella laiminlyödä organisaation tietoturvakäytäntöjä erimielisyyksien tai laiskuuden vuoksi. Tahaton tietoturvakäytäntöjen laiminlyönti voi johtua tietojen ja taitojen puuttumisesta, joka voi kertoa puutteellisesta koulutuksesta tai ohjeistuksista organisaatiossa. Kotiympäristössä vaikuttavia tekijöitä on tutkittu huomattavasti vähemmän, koska kotiympäristön käyttäytyminen perustuu käyttäytymisen ennustamiseen, mikä on hyvin vaikeaa eikä välttämättä pidä paikkaansa. Kotikäyttäjien

tietoturvakäyttäytymistä tulisi tutkia enemmän, koska siitä voivat hyötyä muutkin, kuin pelkästään kotikäyttäjät.

BYOD sumentaa rajan työn ja vapaa-ajan käytön välillä. Vaikka se on työntekijöiden suosima ja omaksuma käytäntö, se on herättänyt myös huolta muun muassa yksityisyydestä. Työntekijät haluavat tehdä töitä omilla laitteillaan, mutta eivät halua suostua kaikkiin organisaation käytäntöihin, joilla se pyrkii suojaamaan resurssinsa. Työntekijät eivät välttämättä luota siihen, että laitteita ei valvota työajan ulkopuolella ja pelkäävät, että henkilökohtaiset tiedot laitteilla saattavat kadota. Hyödyt siis kelpaavat, mutta mieluiten ilman niitä toimia, joilla organisaatio kykenee suojelemaan itseään. Organisaatioiden johtotasot eivät välttämättä ole olleet innoissaan käytännöstä siihen liittyvien tietoturvariskien vuoksi. Voi olla kuitenkin haastavaa estää työntekijöitä omaksumasta käytäntöä, varsinkin jos organisaatio ei kustanna tarvittavia laitteita työntekijöilleen. Organisaation voi olla myös vaikea sopeutua uusiin käytäntöihin nopeasti, erityisesti jos ne eivät ole lähtöisin organisaation johtotasolta. Moni organisaatio ei ole välttämättä ehtinyt luoda BYOD:n käyttöön liittyviä sääntöjä ja käytäntöjä, ennen kuin vahinko on jo tapahtunut. BYOD laitteet ovat olleet vastuussa lukuisista organisaatioiden tietomurroista ja tietovuodoista.

Kaikella on kuitenkin kääntöpuoli, ja BYOD ei ole poikkeus tähän. BYOD voi tuoda organisaatiolle varteenotettavia säästöjä vuosittain, ja raha on usein ratkaiseva tekijä monissa päätöksissä. Lisäksi työntekijöiden on havaittu olevan tuotteliaampia ja sitoutuneempia BYOD:n ansiosta. Lisäksi omilla tutuilla laitteilla työskentely voi parantaa työmoraalia. Kuitenkin riskit on otettava huomioon ja viitekehys säännöille laadittava ennen lopullisten päätöksien tekoa. BYOD:iin liittyy monia tietoturvariskejä, kuten tietovuodot ja tietomurrot, sekä erilaiset haittaohjelmat. Teknisten riskien lisäksi on käyttäjiin liittyviä riskejä. Työntekijät voivat tarkoituksella käyttää väärin organisaation tietoja ja resursseja ja aiheuttaa suurta vahinkoa. Työntekijät voivat vaarantaa organisaation tietoturvan myös puhtaasti vahingossa. BYOD laite voidaan yhdistää suojaamattomaan verkkoon, ja se voi kadota tai tulla varastetuksi. Työntekijöillä voi olla vaikeaa muuttaa tottumuksiaan omien laitteiden käytön suhteen.

On olemassa monia keinoja, joilla organisaatio voi tehdä BYOD- käytännön käytön turvallisemmaksi ja yleisesti parantaa tietoturvaansa. Organisaation on tunnistettava ne tekijät, jotka vaarantavat tietoturvan ja mitkä tekijät puolestaan parantavat sitä. Työntekijä on yksi tärkeimmistä tekijöistä organisaation tietoturvan kannalta, joten vahvistamalla työntekijöiden tietoja ja taitoja koulutuksen ja käytäntöjen avulla, sekä tarjoamalla tukea ongelmatilanteissa voidaan päästä pitkälle. Lisäksi on mahdollista valvoa työntekijän laitetta etänä, ja tehdä tarvittavia toimenpiteitä vahinkojen vähentämiseksi. Hyvän tietoturvan eteen on nähtävä vaivaa, aikaa ja varattava resursseja. On todennäköisesti halvempaa investoida hyvään tietoturvaan, kuin korjata sen puutteesta aiheutuvia vahinkoja. On myös pysyttävä valppaina siltä varalta, että uusia uhkia ilmestyy, tai vanhat kehittyvät haastavammiksi. Uusiin asioihin ei ole helppoa investoida aikaa ja resursseja siltä varalta, että ne menevät kokonaan hukkaan. Mutta vasta ottamalla riskin ja kokeilemalla selviää, onko jokin uusi trendi tai käytäntö hyödyllinen organisaatiolle pitkällä tähtäimellä. Uudet innovatiiviset työskentelytavat voivat osoittautua hyvin tuottoisiksi.

5. Yhteenveto ja johtopäätökset

5.1 Johtopäätökset

Niin organisaatiot, kuin kotikäyttäjätkin, ovat nykyään riippuvaisia tietokoneista, mobiililaitteista ja internetistä (Talib et al., 2010). Tietoturva on ollut ajankohtainen huolenaihe jo pitkään. Informaatioteknologian kehittyessä siihen liittyvät vaarat kehittyvät myös yhä haastavammiksi torjua. Hyvää tietoturvaa ei voida enää saavuttaa pelkästään teknisin keinoin, sillä ongelman korjaamiseksi sitä tulee ensin ymmärtää (Talib et al., 2010). Organisaatioissa työntekijä nähdään usein tietoturvan heikoimpana lenkkinä, mutta todellisuudessa työntekijä on kuitenkin avain parempaan tietoturvaan (Talib et al., 2010 ja Bulgurcu et al., 2010). Hyödyntääkseen työntekijöitä paremman tietoturvan saavuttamiseksi, organisaatioiden täytyy panostaa heidän tietoturvakoulutukseensa (Talib et al., 2010). Organisaatiot voivat ulkoistaa tietoturva-asiat ulkoisille osapuolille, mutta Kotikäyttäjien tietoturva on heidän itsensä vastuulla, ja heidän täytyy itse tehdä kaikki siihen liittyvät päätökset. Kotikäyttäjät ovat usein haavoittuvaisempia, jonka vuoksi he ovat useimmiten kyberrikollisten tähtäimessä (Thompson et al., 2017). Kotikäyttäjillä ei yleensä ole riittävästi tietoja ja taitoja suojata tietojaan kunnolla, koska tietoa on vaikea löytää tai se on vanhentunutta (Kritzinger & Von Solms, 2010).

Käyttäjien tietoturvakäyttäytymisessä organisaatiokontekstissa ja vapaa-ajalla on samankaltaisuuksia, mutta paljon enemmän eroja (Li & Siponen, 2011). Organisaatioympäristössä työntekijän tietoturvakäyttäytymiseen voi vaikuttaa esimerkiksi tämän asenne ja havaitut hyödyt (Ramakrishnan et al., 2022). Organisaatiot voivat myös yrittää vaikuttaa käyttäjän tietoturvakäyttäytymiseen eri tavoilla (Herath & Rao, 2009). Useimmat käyttäjät saavat tietoturvaan liittyvän tietämyksensä työpaikalta tai verkosta (Talib et al., 2010). Kotiympäristön tietoturvakäyttäytymistä on vaikea tutkia, mutta käyttäytymiseen vaikuttavia tunnistettuja tekijöitä ovat muun muassa motivaatio, asenne ja havaittu haavoittuvuus (Shropshire et al., 2015,Talib et al., 2010 jaThompson et al., 2017).

BYOD on ajan myötä yleistynyt monissa organisaatioissa. Organisaatioiden ei kuitenkaan ole aina helppoa omaksua uusia käytäntöjä, varsinkaan jos ne eivät ole alun perin organisaation johtotason omaksumia (Barlette et al., 2021). BYOD on hyödyllinen käytäntö sekä työntekijöille että organisaatioille, mutta siihen liittyy hyötyjen lisäksi monia tietoturvariskejä. BYOD:n tuomia hyötyjä organisaatioille ovat esimerkiksi kustannustehokkuus ja työntekijöiden kohonnut tuotteliaisuus (Coker, 2022). Tietoturvariskejä ovat esimerkiksi tietovuodot ja haittaohjelmat (Olalere et al., 2015). Työntekijöiden kokemat hyödyt liittyvät lähinnä siihen, että on mukavampi työskennellä tutuilla laitteilla (Chen et al., 2021). Työntekijöillä on kuitenkin myös BYOD käytäntöön liittyviä huolia. He ovat huolissaan muun muassa yksityisyydestään ja henkilökohtaisten tietojen katoamisesta (Garba et al., 2015).

Organisaatiot voivat pyrkiä tekemään BYOD käytännön käyttämisestä turvallisempaa erilaisilla keinoilla, kuten kaksivaiheisen todennuksen avulla ja järjestämällä

työntekijöille pakollista tietoturvakoulutusta (Olalere et al., 2015 ja Zhiling Tu et al., 2019). Organisaatioille on tarjolla myös erilaisia BYOD laitteille tarkoitettuja mekanismeja, kuten laitevalvontaa ja tietojen etätyhjennystoimintoja (Downer & Bhattacharya, 2022). Vahvistamalla työntekijöiden tietämystä tietoturvaan liittyvistä uhkista auttaa organisaatiota vähentämään tietovuotoja ja haittaohjelmien leviämistä (Downer & Bhattacharya, 2022).

5.2 Yhteenveto

Tutkimuksen aihe oli käyttäjän tietoturvakäyttäytyminen organisaatiokontekstissa ja vapaa-ajalla. Käyttäytymisessä on huomattavia eroja eri ympäristöissä. Organisaatiokontekstissa käyttäjälle on tarjolla tietoturvakoulutusta ja IT-tuki. Käyttäytymiseen vaikuttavat erilaiset sisäiset ja ulkoiset tekijät, kuten muut ympärillä olevat ihmiset, asenne ja hyödyt. Vapaa-ajan ympäristössä käyttäjä on itse yksin vastuussa tietoturvastaan ja siihen liittyvistä päätöksistä. Tietoturvakäyttäytymiseen vaikuttaa lähinnä oma asenne ja motivaatio. Työpaikalta tai verkosta saatua tietoa voidaan hyödyntää, mutta totuttua käyttäytymistä on vaikea muuttaa. BYOD käytännön kontekstissa tietoturvakäyttäytyminen on samankaltaista, kuin vapaa-ajan käyttäytyminen. Omilla laitteilla työskennellessä käyttäjät saattavat unohtaa organisaation tietoturvakäytännöt, ja toimivat kuten ovat tottuneet. Tämä altistaa organisaatiot useille tietoturvauhkille.

Tutkimusta rajoitti huomattavasti se, että tietoturvakäyttäytymistä kotiympäristössä on tutkittu paljon vähemmän. Lisätutkimusta kotikäyttäjien tietoturvakäyttäytymisestä siis tarvitaan. Tulevaisuudessa olisi myös hyvä tutkia BYOD käytännön vaikutuksia organisaation tietoturvan lisäksi kotikäyttäjien ja kotiympäristön tietoturvaan. Kyselyjen avulla voitaisiin yrittää kartoittaa kotikäyttäjien tietoturvakäyttäytymistä jatkotutkimuksissa. Voitaisiin myös suorittaa tutkimus, jonka aikana osallistujien laitteita valvottaisiin tietoturvakäyttäytymisen seuraamiseksi. Tutkimukset voivat auttaa organisaatioita kehittämään tietoturvaansa erityisesti työntekijöiden avulla. Kotikäyttäjätkin voivat oppia hyviä tietoturvakäytäntöjä. Lisäksi BYOD käytännön käyttöön ottamista pohtivat organisaatiot voivat vertailla sen hyviä ja huonoja puolia.

Lähteet

Anderson, C. L., & Agarwal, R. K. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly,* 34(3), 613-643. http://dx.doi.org/10.2307/25750694

Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting and Social Change,* 198. https://doi.org/10.1016/j.techfore.2023.123028

Barlette, Y., Jaouen, A., & Baillette, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International Journal of Information management,* 56. https://doi.org/10.1016/j.ijinfomgt.2020.102212

Boell, S., & Cecez-Kecmanovic, D. (2015). On being 'Systematic' in Literature Reviews in IS. *Journal of Information Technology,* 30(2), 161-173. https://doi.org/10.1057/jit.2014.26

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Chen, H., Li, Y., Chen, L., & Yin, J. (2021). Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue. *Journal of Enterprise Information Management.* 34(3), 770-792. https://doi.org/10.1108/JEIM-10-2019-0318

Coker, T. E. (2022). What Human Factors Are Associated With The Adoption Of BYOD in an organization. https://doi.org/10.31234/osf.io/ey4qm

Downer, K., & Bhattacharya, M. (2022). BYOD Security: A Study of Human Dimensions. *Informatics,* 9(1). https://doi.org/10.3390/informatics9010016

Bello Garba, A., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences.* 10(3), 1279-1287.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *information and Computer Security,* 30(3), 382-401. https://doi.org/10.1108/ICS-06-2021-0073

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protecting through awareness enforcement. *Computers and Security,* 29(8), 840-847. https://doi.org/10.1016/j.cose.2010.08.001

Li, Y., & Siponen, M. (2011). A Call For Research On Home Users' Information Security Behaviour. *PACIS Proceedings,* 112. https://aisel.aisnet.org/pacis2011/112

Musarurwa, A., Flowerday, S., & Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. *SA Journal of Information Management,* 20(1). http://dx.doi.org/10.4102/sajim.v20i1.980

Olalere, M., Abdullah, M. T., Mahmod, R., &Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *Sage Open,* 5(2). https://doi.org/10.1177/2158244015580372

Posey C., & Shoss, M. (2023). Employyes as a Source of Security Issues in Times of Change and Stress: A Longitudinal Examination of Employees' Security Violations during the COVID-19 Pandemic. *Journal of Business and Psychology.* https://doi.org/10.1007/s10869-023-09917-4

Ramakrishnan, T., Hite, D. M., Schuessler, J. H., & Prybutok, V. (2022). Work ethic and information security behavior. *Information and Computer Security,* 30(3), 364-381. https://doi.org/10.1108/ICS-02-2021-0017

Ratchford, M., El-Gayar, O., Noteboom, C., &Wang, Y. (2021). BYOD security issues: a systematic literature review. *Information Security Journal: A Global Perspective,* 31(3), 253-273. https://doi.org/10.1080/19393555.2021.1923873

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security. *Computers and Security,* 49, 177-191. https://doi.org/10.1016/j.cose.2015.01.002

Siponen, M., Pahnila, S., & Mahmood, A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *computer,* 43(2), 64-71. 10.1109/MC.2010.35

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security,* 25(5), 494-534. https://doi.org/10.1108/ICS-07-2016-0054

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *ARES 2010 – 5th International Conference on Availability, Reliability and Security,* 196-203. https://doi.org/10.1109/ARES.2010.27

Thompson, N., McGill, T., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computer and Security,* 70, 376-391. https://doi.org/10.1016/j.cose.2017.07.003

Tu, C. Z., Adkins, J., & Zhao, G. Y. (2019). Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory. *Journal of the Midwest Association for Information Systems,* 1(2). DOI: 10.17705/3jmwa.000045

Vedadi, A., Warkentin, M., & Dennis, A. (2021). Herd behavior in information security decision-making. *Information and Management,* 58(8). https://doi.org/10.1016/j.im.2021.103526

Wani, T., Mendoza, A., Gray, K., & Smolenares, F. (2022). BYOD usage and security behaviour of hospital clinical staff: An Australian survey. *International Journal of Medical Informatics,* 165. https://doi.org/10.1016/j.ijmedinf.2022.104839

Yerby, J., & Floyd, K. (2018). Faculty and Staff Information Security Awareness and Behaviors. *Journal of The Colloquium for Information Systems Security Education,* 6(1).