Tietoturvapoikkeamat pienissä ja keskisuurissa yrityksissä sekä niiden juurisyyt ja tehokkaimmat torjuntatoimet

Turun yliopisto
Tietotekniikan laitos
LuK-tutkielma
Tietojenkäsittelytiede
Kesäkuu 2026
Anttoni Vuorio

TURUN YLIOPISTO
Tietotekniikan laitos

Anttoni Vuorio: Tietoturvapoikkeamat pienissä ja keskisuurissa yrityksissä sekä niiden juurisyyt ja tehokkaimmat torjuntatoimet

LuK-tutkielma, 24 s.
Tietojenkäsittelytiede
Kesäkuu 2026

Tietoturvapoikkeamat ovat kasvava haaste pienille ja keskisuurille yrityksille. Tietoturvapoikkeamat voivat aiheuttaa yrityksille merkittäviä taloudellisia menetyksiä ja liiketoiminnan keskeytyksiä. Pk-yritykset ovat erityisen haavoittuvaisia erilaisille tietoturvapoikkeamille pienen kokonsa ja rajallisten resurssien vuoksi.
Tämän tutkielman tavoitteena on tunnistaa yleisimmät tietoturvapoikkeamat pk-yrityksissä, sekä selvittää niiden taustalla vaikuttavat juurisyyt ja tehokkaimmat torjuntatoimet. Tutkielma toteutetaan kirjallisuuskatsauksena, jossa tarkastellaan vuosina 2020–2025 julkaistua vertaisarvioitua tutkimuskirjallisuutta. Aineiston avulla muodostettiin kokonaiskuva pk-yritysten tietoturvahaasteista ja keinoista niiden hallitsemiseksi.
Tulosten perusteella yleisimmät tietoturvapoikkeamat pk-yrityksissä ovat tietojenkalasteluyritykset, haittaohjelmat ja tietomurrot. Keskeisiksi juurisyiksi tunnistettiin inhimilliset virheet, resurssipuute ja heikot tietoturvakäytännöt. Tehokkaimmiksi torjuntatoimiksi havaittiin henkilöstön jatkuva tietoturvakoulutus, selkeä tietoturvastrategia ja tekniset kontrollit. Tutkielman perusteella voidaan päätellä, että tietoturvapoikkeamien ehkäisy pk-yrityksissä edellyttää teknisten ratkaisujen lisäksi organisaation tietoturvakulttuurin ja henkilöstön jatkuvaa kehittämistä.

Asiasanat: tietoturvapoikkeama, kyberturvallisuus, pienet ja keskisuuret yritykset, tietoturvan hallinta

Sisällys

1 Johdanto **1**

2 Tietoturvapoikkeamat pk-yrityksissä **4**

2.1 Pk-yrityksen määritelmä, merkitys ja digitalisaation vaikutus yritysten tietoturvaan 4

2.2 Tietoturvapoikkeaman määritelmä 5

3 Yleisimmät tietoturvapoikkeamat, niiden juurisyyt ja torjuntatoimet **8**

3.1 Yleisimmät tietoturvapoikkeamat pk-yrityksissä 8

3.2 Poikkeamien juurisyyt 10

3.3 Torjuntatoimet pk-yrityksissä 13

4 Pohdinta **16**

4.1 Keskeisten havaintojen merkitys 16

4.2 Juurisyiden ja torjuntatoimien välinen yhteys 17

4.3 IST-malli pk-yrityksille 18

4.4 Käytännön merkitys pk-yrityksille 20

4.5 Työn luotettavuus ja rajoitteet sekä jatkotutkimusehdotukset 20

5 Yhteenveto **22**

Lähdeluettelo **25**

Kuvat

1.1 Tutkimusmateriaalin hakuprosessi ja aineiston valinta. 2

4.1 IST-malli pk-yritysten tietoturvavalmiuden keskeisistä osa-alueista . . 18

Taulukot

3.1 Kirjallisuudessa tunnistetut yleisimmät tietoturvapoikkeamat pk-yrityksissä. 9
3.2 Kirjallisuudessa tunnistetut keskeiset tietoturvapoikkeamien juurisyyt pk-yrityksissä. 11
3.3 Kirjallisuudessa esitetyt tietoturvapoikkeamien torjuntatoimenpiteet pk-yrityksissä. 14

1 Johdanto

Viimeisen vuosikymmenen aikana teknologian kehitys on muuttanut yritysmaailmaa valtavasti. Teknologia on tuonut yrityksille runsaasti etuja ja mahdollisuuksia, mutta tämän takia yrityksistä lähes kaikki ovat teknologiasta riippuvaisia. [1] Kyberiskujen määrä yrityksiä kohtaan on tämän vuoksi tasaisessa kasvussa. [2]

Erityisen herkkiä kyberiskuille ovat pienet ja keskisuuret yritykset (pk-yritykset), sillä niiltä puuttuvat usein resurssit sekä tietotaito varautua tietoturvapoikkeamiin ja kyberhyökkäyksiin. [2] Yhä useammin kyberrikolliset kohdistavat iskujaan pk-yrityksiin niiden puutteellisen tietoturvallisuuden vuoksi. Tällaisen iskun seuraukset voivat olla katastrofaaliset pk-yrityksille taloudellisten menetysten ja mainehaitan johdosta. [3] On raportoitu, että joka kolmas startup-yritys, johon on kohdistunut kyberisku ei kykene toipumaan hyökkäyksestä ja joutuu lopettamaan liiketoiminnan. [4] Näin ollen pk-yritysten kyberresilienssin parantaminen edellyttää keskeisten tietoturvauhkien tunnistamista sekä tehokkaiden torjuntakeinojen käyttöönottoa. [5]

Tämän tutkielman tarkoituksena on rakentaa kuva siitä, minkälaisia tietoturvapoikkeamia pk-yrityksiin kohdistuu, sekä löytää poikkeamien juurisyyt ja tunnistaa tehokkaimmat torjuntatoimet yrityksen rajalliset resurssit huomioiden. Tämä suoritetaan käymällä läpi alan tutkimuskirjallisuutta. Tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

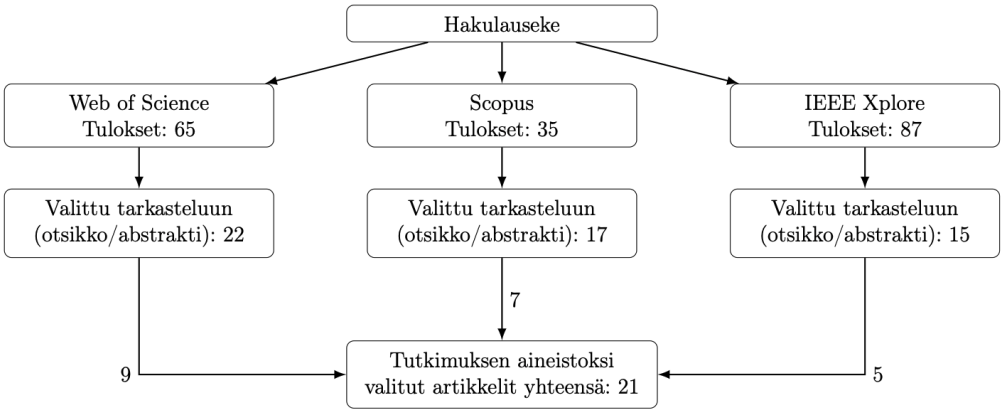
TK1: Mitkä ovat yleisimmät tietoturvapoikkeamat pk-yrityksissä?

TK2: Mitkä ovat eri poikkeamien juurisyyt?

TK3: Mitkä ovat tehokkaimmat torjuntatoimet?

Tutkielma on suoritettu kirjallisuuskatsauksena johon, tutkimusmateriaali on haettu kolmesta eri tietokannasta. Käytetyt tietokannat ovat Scopus, Web of Science ja IEEE Explore joihin käytettiin seuraavaa hakulauseketta: *((SME* OR SMB* OR "small business*"OR "small and medium enterprise*") AND ("data breach*"OR "security incident*"OR "cyber incident*"OR ransomware OR phishing) AND ("root cause*"OR "contributing factor*"OR mitigation OR "security measure*"OR "access control"OR MFA OR "patch management"OR "security awareness"OR "cost-effective"OR "resource-constrained")).*

Haun tulokset rajattiin siten, että tutkimusmateriaali oli tuotettu vuonna 2020 tai sen jälkeen. Tämän jälkeen artikkelit valittiin tarkasteluun otsikon ja abstraktin perusteella (kuva 1.1).



Kuva 1.1: Tutkimusmateriaalin hakuprosessi ja aineiston valinta.

Tämän jälkeen artikkelit pisteytettiin asteikolla 1-5 niiden relevanssin, sisällöllisen hyödyllisyyden ja tutkimuksellisen laadun mukaan. Relevanssilla arvioitiin artikkelin yhteyttä tutkielman tutkimuskysymyksiin ja siihen, kuinka suoraan ne kä-

sittelivät tietoturvapoikkeamia pk-yrityksissä. Sisällöllisellä hyödyllisyydellä tarkasteltiin sisällön syvyyttä ja tutkimuksellisella laadulla arvioitiin artikkelin luotettavuutta, kuten läpinäkyvyyttä ja argumentoinnin johdonmukaisuutta. Lopulliseksi tutkimusmateriaaliksi valittiin vai ne artikkelit, joiden arvosana oli vähintään 4. Tämän rajauksen perusteella tutkimusmateriaaliksi valikoitui lopulta 21 artikkelia.

Tutkielma koostuu viidestä luvusta. Johdannon jälkeen toisessa luvussa käsitellään pk-yrityksen määritelmää ja merkityksellisyyttä, sekä tietoturvapoikkeamien määritelmää. Kolmannessa luvussa tarkastellaan kirjallisuuden perusteella yleisimpiä tietoturvapoikkeamia pk-yrityksissä, sekä niiden yleisimpiä juurisyitä ja tehokkaimpia torjuntatoimia. Neljännessä luvussa pohditaan tutkimustuloksia ja niiden merkitystä. Viidennessä luvussa esitellään tutkimuksen yhteenveto ja keskeiset johtopäätökset.

2 Tietoturvapoikkeamat pk-yrityksissä

2.1 Pk-yrityksen määritelmä, merkitys ja digitalisaation vaikutus yritysten tietoturvaan

Pienet ja keskisuuret yritykset (pk-yritykset) muodostavat keskeisen osan sekä Euroopan unionin että Suomen taloudesta. Euroopan komission määritelmän mukaan pk-yrityksiä ovat enintään 250 henkilöä työllistäviä ja joiden vuosittainen liikevaihto on enintään 50 miljoonan euroa. Yritykset voidaan jakaa edelleen mikroyrityksiin, pieniin yrityksiin ja keskisuuriin yrityksiin henkilömäärän ja taloudellisten lukujen perusteella. [6]

pk-yritysten merkitys Euroopan taloudelle sekä sosiaaliselle rakenteelle on merkittävä. Euroopassa on noin 32 miljoonaa pk-yritystä, jotka työllistävät 80 miljoonaa ihmistä. Tämä vastaa lähes 70 %:a koko mantereen työpaikoista. [7] Näistä valtaosa, jopa 98,9 %:a on alle 50 henkilöä työllistäviä yrityksiä. Suomessa pk-yrityksiä on Tilastokeskuksen mukaan 409 000. [8]

Euroopan unioni pyrkii aktiivisesti avustamaan pk-yritysten toimintaa eri keinoin. Näihin kuuluu myös digitalisaation edistäminen, sillä sen on todettu kohtuullistavan yritysten kustannuksia ja parantavan liiketoiminnan ylläpidon helppoutta. [6] Digitalisaatio ja teknologian kehitys tuo nykypäivänä ennennäkemätöntä arvoa

yrityksille, ja on lähes mahdotonta löytää kasvuhakuista yritystä, joka ei olisi riippuvainen teknologiasta. Viimeisen muutaman vuoden aikana digitalisaation vauhtia ovat kiihdyttäneet uudet teknologiset innovaatiot ja etenkin koronapandemian aiheuttama paine yrityksille siirtää palveluitaan verkkoon. [1]

Lukemattomien teknologisten hyötyjen ja liiketoimintaa kehittävien digitaalisten ratkaisujen seuraamukset eivät ole kuitenkaan kaikki positiivisia. [1] Nämä äkilliset muutokset yritysten digitaalisen infrastruktuuriin ovat aiheuttaneet valtavan nousun kyberrikollisuudessa. [4] Tutkimuksen mukaan 73 %:a yrityksestä, oli kärsinyt kyberhyökkäyksestä viimeisen 12 kuukauden aikana. [3] Niistä valtaosalla ei ollut kykyä estää ja käsitellä niitä. [9] On todettu, että pk-yritykset ovat yleisiä kohteita kyberrikollisille rajallisten resurssien ja koulutuksen puutteen vuoksi. [10] Kyberiskuista aiheutunut taloudellinen menetys ja aseman heikentyminen liiketoiminnan näkökulmasta johtavat usein siihen, että yritys ei kykene jatkamaan liiketoimintaa. [4]

Monelle pk-yritykselle on erityisen hankalaa varautua kyberiskuihin tietämättömyyden ja koulutuksen puutteen vuoksi. Vaikka nykypäivän digitalisoituneessa liiketoimintaympäristössä varautumisesta on tullut haastavampaa ja kalliimpaa, pk-yritykset voivat merkittävästi pienentää riskejään yksinkertaisilla ja ennakoivilla toimenpiteillä. Ennen toimenpiteisiin ryhtymistä on kuitenkin tärkeää, että yrityksillä ja niissä työskentelevillä henkilöillä on käsitys siitä, millaisia tietoturvaan liittyviä poikkeamia voi esiintyä. [3]

2.2 Tietoturvapoikkeaman määritelmä

Tässä tutkielmassa termillä "tietoturvapoikkeama" (engl. information security incident) tarkoitetaan yhtä tai useampaa toisiinsa liittyvää odottamatonta tai ei-toivottua tietoturvatapahtumaa, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti. [11]

Kansainvälisissä standardeissa tietoturva määritellään kolmen periaatteen mukaan: luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Nämä muodostavat yhdessä CIA-mallin. [12] Tietoturvapoikkeamana voidaan siis pitää mitä tahansa tapatumaa, joka rikkoo yhtä tai useampaa näistä periaatteista.

Tietoturvapoikkeamat voidaan jaotella karkeasti kolmeen eri kategoriaan, tahallisiin hyökkäyksiin, inhimillisiin virheisiin sekä teknisiin vikoihin. Tahallisiin hyökkäyksiin sisältyvät ulkopuolisten toimijoiden aiheuttamat kyberhyökkäykset, kun taas inhimilliset virheet ovat esimerkiksi tiedon huolimaton käsittely. Teknisiin vikoihin kuuluvat esimerkiksi ohjelmistoviat ja laitehäiriöt. [13], [14]

Tietoturvapoikkeamat voidaan luokitella tarkemmin niiden toteutustavan mukaan, yleisimpiä tyyppejä ovat: [15]

- **Tietomurrot** (engl. data breach), joissa luvatonta tietoa päätyy väärän henkilön saataville.
- **Haittaohjelmat** (engl. malware), haitallinen ohjelma joka jollain tavalla saadaan asennettua uhrin laitteelle.
- **Palvelunestohyökkäykset** (engl. DDos attack), hyökkäys jossa kuormitetaan järjestelmää niin paljon, että se ei pysty jatkamaan normaalia toimintaa.
- **Tietojenkalastelu** (engl. phishing), uhria pyritään huijaamaan luovuttamaan arkaluontoista tietoa tai pääsyn järjestelmään.
- **Sisäiset tietoturvapoikkeamat**, voi viitata mihin tahansa tahattomaan virheeseen yrityksen sisällä esimerkiksi työntekijän huolimaton tietojen käsittely tai järjestelmän vanhentunut ohjelmistopäivitys joka sisältää haavoittuvuuden. [15]

On myös tärkeää huomata, että tietoturvapoikkeaman erityispiirteenä on se, että se harvoin johtuu yksittäisestä tekijästä. [15] Esimerkiksi tietojenkalasteluyritys voi

onnistua, koska työntekijä ei tunnistanut huijausta, mutta myös siksi, että käytössä ei ollut kaksivaiheista tunnistautumista. [16]

3 Yleisimmät tietoturvapoikkeamat, niiden juurisyyt ja torjuntatoimet

3.1 Yleisimmät tietoturvapoikkeamat pk-yrityksissä

Tutkimusaineiston perusteella pk-yrityksissä esiintyy useita toistuvia tietoturvapoikkeamien muotoja. Tutkimusaineistoa tarkasteltaessa rakennettiin taulukko 3.1 kaikista aineistoissa esiintyvistä tietoturvapoikkeamista. Yleisimmiksi tietoturvapoikkeamiksi nousi erityisesti tietojenkalasteluyritykset, tietomurrot sekä luvaton pääsy. Taulukossa 3.1 on esitetty tutkimuskirjallisuudessa yleisimmät tietoturvapoikkeamat pk-yrityksissä. Taulukon 3.1 perusteella tietoturvapoikkeamat voidaan jakaa kolmeen eri kategoriaan: henkilöstöön kohdistuvat tietoturvapoikkeamat (P1-P3), teknisiin järjestelmiin kohdistuvat tietoturvapoikkeamat (P4-P6) sekä ulkopuolisiin tekijöihin liittyvät tietoturvapoikkeamat (P7-P8).

Tutkimusaineistoissa korostuvat etenkin henkilöstöön kohdistuvat tietoturvapoikkeamat. Useissa tutkimuksissa tietojenkalastelu ja sosiaalinen manipulointi ovat yleisiä tietoturvauhkia pk-yrityksille. Hyökkäykset kohdistuivat erityisesti sähköpostiin, kirjautumisjärjestelmiin ja henkilöstön toimintaan liittyviin huijauksiin. [17], [18] Lisäksi useissa tutkimuksissa esiintyi luvattomaan pääsyyn liittyviä tietoturva-

Taulukko 3.1: Kirjallisuudessa tunnistetut yleisimmät tietoturvapoikkeamat pk-yrityksissä.

Kirjoittaja, vuosi, viittaus	P1: Phishing	P2: Sosiaalinen manipulointi	P3: Luvaton pääsy	P4: Ransomware	P5: Haittaohjelmat	P6: Tietojärjestelmien haavoittuvuudet	P7: Tietomurrot	P8: Kolmannen osapuolen hyökkäykset
Ali et al. 2022 [14]					X			
Awan et al. 2025 [5]	X	X	X	X	X		X	X
Button et al. 2025 [18]	X	X	X					
Cartwright et al. 2025 [24]							X	
Dua et al. 2024 (Third-party risk) [23]								X
Dua et al. 2024 (Asset management) [1]			X			X	X	
El-Hajj et al. 2024 [4]			X	X	X		X	
Falch et al. 2022 [16]	X			X				
Hadap et al. 2025 [10]							X	
Huaman et al. 2021 [2]	X	X	X	X			X	
Kandpal et al. 2023 [17]	X			X	X		X	
Kocksch et al. 2024 [19]	X	X	X					
Lill et al. 2025 [21]	X	X	X	X	X		X	
Loskorikh et al. 2025 [20]	X	X	X					
Mkhulisi et al. 2024 [25]			X					
Ncubukezi et al. 2020 [22]					X	X		
Saban et al. 2021 [26]	X		X					
Tamimi et al. 2025 [13]	X	X						
Tetteh 2024 [3]	X			X			X	
Tsiodra et al. 2023 [9]			X				X	
Valdes-Rodriguez et al. 2024 [27]					X			

poikkeamia, jossa asiaton toimija saa pääsyn yrityksen järjestelmiin ilman asianmukaisia käyttöoikeuksia. [19], [20]

Teknisiin järjestelmiin kohdistuvia tietoturvapoikkeamia voidaan tutkimuskirjallisuuden perusteella pitää merkittävänä uhkana pk-yrityksille. Erityisesti haittaohjelmat ja kiristyshaittaohjelmat ovat uhka yritysten liiketoiminnalle. Niillä pyritään keskeyttämään liiketoiminta ja kiristämään rahaa. Yleiseksi uhaksi havaittiin myös tietomurrot, joilla on vakavia seurauksia luottamuksellisten tietojen paljastuessa ja ne voivat pahimmillaan johtaa koko yrityksen konkurssiin. Lisäksi tutkimusaineis-

tossa esiintyi erilaisia tietojärjestelmien haavoittuvuuksia, jotka edesauttavat monenlaisien tietoturvapoikkeamien syntyä. [2], [21], [22]

Yrityksen ulkopuolisiin tekijöihin liittyi myös tietoturvariskejä. Kolmannen osapuolen kautta tapahtuvat hyökkäykset ovat myös mahdollisia. Tulosten perusteella yritysten tietoturvariskit eivät siis rajoittuneet pelkästään niiden omiin järjestelmiin, vaan myös yhteistyökumppaneihin ja palveluntarjoajiin. [5], [23]

Tutkimusaineiston perusteella pk-yritysten tietoturvapoikkeamat muodostavat monimuotoisen kokonaisuuden, jossa korostuu henkilöstöön kohdistuvat hyökkäykset sekä teknisiin järjestelmiin liittyvät poikkeamat. Tulokset viittaavat siihen, että tietoturvapoikkeamat eivät johdu yksittäisistä irrallisista tapahtumista, vaan muodostuvat useista toisiinsa liittyvistä tekijöistä. Näitä tietoturvapoikkeamien taustalla olevia juurisyitä käydään läpi seuraavassa luvussa.

3.2 Poikkeamien juurisyyt

Tutkimusaineiston perusteella pk-yritysten tietoturvapoikkeamien taustalla vaikuttavat useat organisaatiolliset, inhimilliset ja tekniset tekijät. Vaikka tietoturvapoikkeamien muodot vaihtelevat tutkimuksittain, juurisyyt korostuvat samankaltaisina. Kirjallisuudesta rakennettiin taulukko 3.2, jossa näkyy yleisimmät juurisyyt tietoturvapoikkeamille pk-yrityksissä. Taulukossa 3.2 esiintyy erityisesti inhimilliset virheet sekä puutteellinen riskienhallinta ja tietoturvastrategia merkittävinä juurisyinä tietoturvapoikkeamiin. Taulukon 3.2 perusteella juurisyyt voidaan jaotella kolmeen kategoriaan: inhimilliset ja osaamisen liittyvät virheet (J1-J2), organisatoriset ja strategiset puutteet (J3-J5) sekä teknologiset ja ulkoisiin tekijöihin liittyvät tekijät (J6-J8).

Inhimilliset ja osaamiseen liittyvät virheet nousivat tutkimusaineistossa esille selkeästi pk-yritysten tietoturvapoikkeamien juurisyiksi. Inhimilliset virheet ja tietoturvaosaamisen puute sekä heikot päivittäiset tietoturvakäytännöt (cyber hygie-

Taulukko 3.2: Kirjallisuudessa tunnistetut keskeiset tietoturvapoikkeamien juurisyyt pk-yrityksissä.

Kirjoittaja, vuosi, viittaus	J1: Inhimilliset virheet	J2: Kyberosaamisen puute	J3: Resurssipuute	J4: Puutteellinen riskienhallinta	J5: Puutteellinen tietoturvastrategia	J6: Cyber hygiene -puutteet	J7: Puutteelliset tekniset kontrollit	J8: Kolmannen osapuolen riskit
Ali et al. 2022 [14]				X			X	
Awan et al. 2025 [5]	X	X	X	X	X		X	
Button et al. 2025 [18]	X	X			X			
Cartwright et al. 2025 [24]			X		X			
Dua et al. 2024 (Third-party risk) [23]				X	X			X
Dua et al. 2024 (Asset management) [1]				X		X	X	
El-Hajj et al. 2024 [4]				X	X		X	
Falch et al. 2022 [16]			X		X			
Hadap et al. 2025 [10]	X		X	X	X			
Huaman et al. 2021 [2]	X	X		X	X			
Kandpal et al. 2023 [17]		X		X	X		X	
Kocksch et al. 2024 [19]	X					X		
Lill et al. 2025 [21]	X	X	X	X	X	X	X	
Loskorikh et al. 2025 [20]	X			X			X	
Mkhulisi et al. 2024 [25]		X			X			
Ncubukezi et al. 2020 [22]						X	X	
Saban et al. 2021 [26]		X			X			
Tamimi et al. 2025 [13]	X				X			
Tetteh 2024 [3]		X		X	X			
Tsiodra et al. 2023 [9]				X			X	
Valdes-Rodriguez et al. 2024 [27]		X			X		X	

ne) ja edesauttavat tietoturvapoikkeamien syntyä. Tutkimuksissa korostuivat heikot salasanakäytännöt, epäonnistuminen kalasteluyritysten tunnistamisessa sekä puutteellinen ymmärrys tietoturvariskeistä. Tästä voidaan päätellä, että tietoturvakoulutukset pk-yrityksissä ovat puutteelliset mikä lisää henkilöstön alttiutta tietojenkalastelulle ja sosiaalisen manipuloinnin hyökkäyksille. [10], [21]

Organisatoriset ja strategiset puutteet esiintyivät kirjallisuudessa eniten resurssien rajallisuutena, puutteellisena riskienhallintana ja puuttuvana tietoturvastrategiana. Tutkimuksissa havaittiin, että pk-yrityksillä ei usein ollut tietoturvasta vastaavaa työntekijää tai edes selkeitä toimintamalleja uhkien tunnistamiseen ja ennal-

taehkäisyyn. Lisäksi tutkimuksissa korostui se, että pk-yrityksissä tietoturvaa käsiteltiin enemmän teknisenä kustannuksena kuin strategisena liiketoimintaa turvaavana ratkaisuna. Tämä näkyy vähäisinä tietoturvainvestointeina sekä ennakoivien tietoturvakäytäntöjen puutteena. Tietoturvapoikkeamiin reagoitiin vasta niiden tapahduttua, joka on lähes aina liian myöhään. Tulokset viittaavat, että organisatorisilla käytännöillä ja johdon sitoutumisella on siis merkittävä vaikutus pk-yrityksen tietoturvan tasoon. [10], [24], [25]

Teknisiin ratkaisuihin ja ulkoisiin tekijöihin liittyvät juurisyyt on myös helposti havaittavissa tutkimuskirjallisuudessa. Useissa tutkimuksissa korostuivat puutteelliset tekniset kontrollit, vanhentuneet järjestelmät sekä riittämätön järjestelmävalvonta. Näistä pystyttiin havaitsemaan tilanteita, joissa esimerkiksi ohjelmistojen päivittämättä jättäminen ja puutteelliset käyttöoikeuksien hallintakeinot altistivat pk-yrityksiä tietomurroille ja luvattomalle pääsylle. Lisäksi yhdessä tutkimuksessa havaittiin kolmannen osapuolen kautta tulevasta tietoturvauhasta, jossa ulkoisen palveluntarjoajan heikot tietoturvakäytännöt voivat heijastua suoraan yrityksen omaan tietoturvaan. Tulokset viittaavat siihen, että yrityksen omat järjestelmät, digitaalinen riippuvuus ja toimitusketjuihin liittyvät riskit muodostavat merkittävän ja laajan tietoturvaympäristön. [1], [9], [14]

Näiden havaintojen perusteella voidaan todeta, että pk-yritysten tietoturvapoikkeamien juurisyyt muodostuvat useiden inhimillisten organisatoristen ja teknologisten tekijöiden yhteisvaikutuksesta. Vaikka yksittäiset tietoturvapoikkeamat vaihtelivat tutkimuksittain, juurisyyt toistuivat usein samankaltaisina. Resurssien, koulutuksen ja strategian puute altistaa pk-yritykset vakaville tietoturvauhille. Lisäksi ulkoisiin toimijoihin ja digitaaliseen riippuvuuteen liittyvät riskit korostuivat kasvavana osana yritysten tietoturvaympäristöä. Tulokset viittaavat siihen, että tietoturvapoikkeamien ehkäiseminen edellyttää sekä teknisten että organisatoristen käytäntöjen kehittämistä. Näitä torjuntatoimia tarkastellaan seuraavassa luvussa.

3.3 Torjuntatoimet pk-yrityksissä

Tutkimuskirjallisuuden perusteella pk-yritysten tietoturvapoikkeamien torjuminen edellyttää sekä organisatorisia, inhimillisiä että teknisiä ratkaisuja. Useassa tutkimuksessa korostui, että tehokas tietoturvan hallinta ei perustu yksittäisiin ratkaisuihin vaan kokonaisvaltaiseen lähestymistapaan, jossa tietoturva integroidaan yrityksen päivittäisiin käytäntöihin ja prosesseihin. Tutkimusaineistoista havaituista torjuntakeinoista rakennettiin taulukko 3.3, jossa esiintyy tehokkaiksi havaitut torjuntatoimet. Taulukossa 3.3 korostuu etenkin riskien arviointi, tietoturvaan liittyvät hallinnolliset päätökset sekä tekniset kontrollit. Taulukon perusteella torjuntatoimet voidaan jakaa kolmeen kategoriaan: organisatoriset ja strategiset torjuntatoimet (T1-T3), henkilöstöön ja toimintatapoihin liittyvät torjuntatoimet (T4-T6) sekä teknologiset ja ulkoisiin toimijoihin liittyvät torjuntatoimet (T7-T8).

Tutkimusaineistossa korostui organisatorisiin toimintatapoihin ja strategiseen tietoturvan hallintaan liittyvät torjuntatoimet. Useissa tutkimuksissa riskien arviointi osoittautui olevan erityisen tehokas torjumaan tietoturvapoikkeamien syntyä. Riskien arviointi auttoi yrityksiä käyttämään resursseja oikein ja kohdistamaan tietoturvatoimenpiteitä tehokkaasti. Lisäksi tietoturvapolitiikkojen, hallintamallien ja selkeiden toimintatapojen käyttöönotto yrityksissä paransi niiden kyberresilienssiä merkittävästi. Myös tietoturvastrategioiden luominen ja niiden integrointi osaksi yrityksen päivittäisiä käytäntöjä todettiin vähentävän tietoturvapoikkeamia. Nämä tulokset osoittavat, että tehokas tietoturvan hallinta vaati johdon sitoutumista sekä tietoturvan huomioimista osana jatkuvaa liiketoiminnan kehittämistä. [5], [18], [26]

Henkilöstön osaamiseen ja päivittäisiin toimintatapoihin liittyvät torjuntatoimet näyttäytyivät myös merkittävinä tietoturvapoikkeamien ehkäisykeinoina. Erityisesti tutkimuksissa korostui kyberturvakoulutus ja päivittäiset tietoturvakäytännöt, kuten turvalliset salasana käytännöt, ohjelmistopäivitykset sekä monivaiheinen tunnistaminen. Tutkimuksissa havaittiin, että henkilöstön jatkuva tietoturvatietoisuuden

Taulukko 3.3: Kirjallisuudessa esitetyt tietoturvapoikkeamien torjuntatoimenpiteet pk-yrityksissä.

Kirjoittaja, vuosi, viittaus	T1: Riskien arviointi	T2: Tietoturvapolitiikat ja hallinto	T3: Tietoturvastrategia ja suunnittelu	T4: Kyberturvakoulutus	T5: Cyber hygiene -käytännöt	T6: Tietoturvakäytäntöjen integrointi prosesseihin	T7: Tekniset kontrollit	T8: Kolmannen osapuolen riskienhallinta
Ali et al. 2022 [14]	X						X	
Awan et al. 2025 [5]	X	X	X	X			X	
Button et al. 2025 [18]		X		X				
Cartwright et al. 2025 [24]		X	X					
Dua et al. 2024 (Third-party risk) [23]	X							X
Dua et al. 2024 (Asset management) [1]	X				X		X	
El-Hajj et al. 2024 [4]	X	X					X	
Falch et al. 2022 [16]		X	X					
Hadap et al. 2025 [10]	X	X	X	X				
Huaman et al. 2021 [2]	X	X					X	
Kandpal et al. 2023 [17]	X	X					X	
Kocksch et al. 2024 [19]				X	X			
Lill et al. 2025 [21]	X	X	X	X	X		X	
Loskorikh et al. 2025 [20]				X			X	
Mkhulisi et al. 2024 [25]				X				
Ncubukezi et al. 2020 [22]					X		X	
Saban et al. 2021 [26]		X	X					
Tamimi et al. 2025 [13]				X				
Tetteh 2024 [3]	X	X						
Tsiodra et al. 2023 [9]	X						X	
Valdes-Rodriguez et al. 2024 [27]		X				X	X	

kehittäminen vähensi etenkin tietojenkalasteluun ja sosiaaliseen manipulointiin liittyviä riskejä. Esille nousi etenkin se, että tietoturvakoulutusten tulisi olla jatkuvaa eikä kertaluontoista. Nämä tulokset viittaavat siihen, että henkilöstön tietoturvaosaamisen merkitys on kriittinen osa tietoturvapoikkeamien torjuntaa. [5], [22], [27]

Viimeisenä torjuntatoimikategoriana on teknologiset ja ulkoisiin toimijoihin liittyvät torjuntatoimet. Tutkimuksissa korostuivat tekniset kontrollit kuten palomuurit, käyttöoikeuksien hallinta ja tietojärjestelmien valvonta. Näillä toimenpiteillä

voitiin vähentää erityisesti haittaohjelmiin, tietomurtoihin ja luvattomaan pääsyyn liittyviä riskejä. Ulkoisten toimijoiden riskien arviointi ilmeni myös tärkeänä torjuntatoimena, jolla vältetään kolmannen osapuolen kautta peilautuva tietoturvauhka. [2], [9], [23]

Aineiston perusteella tietoturvapoikkeamien tehokas torjuminen edellyttää useiden toisiaan tukevien toimenpiteiden yhdistämistä. Esille nousi erityisesti ihmisiin, strategioihin ja teknologisiin ratkaisuihin liittyvät torjuntatoimet. Lisäksi niiden integrointi osaksi päivittäistä toimintaa ja käytäntöjä kehittää pk-yrityksen valmiutta ennaltaehkäistä tietoturvapoikkeamia. Tuloksista voidaan päätellä, että kokonaisvaltaisen tietoturvakehyksen luominen yritykselle vaatii sen, että otetaan huomioon ihmiset, strategiat ja teknologia.

4 Pohdinta

4.1 Keskeisten havaintojen merkitys

Tämän kirjallisuuskatsauksen perusteella voidaan havaita, että pk-yritysten tietoturvapoikkeamien taustalla vaikuttavat usein samankaltaiset tekijät, eikä poikkeamat johdu yksittäisistä inhimillisistä tai teknisistä virheistä. Poikkeamien taustalla on useita yhdistyviä tekijöitä, jotka muodostavat olosuhteet, jossa tietoturvapoikkeamia pääse syntymään. Kirjallisuutta tarkasteltaessa esiin nousi inhimillisiin virheisiin, teknisiin ongelmiin sekä organisatorisiin tekijöihin liittyviä puutteita. Näiden tekijöiden toistuvuus kirjallisuudessa viittaa siihen, että pk-yritysten tietoturvapoikkeamat muodostavat rakenteellisen ilmiön, jossa useat eri puutteet kietoutuvat toisiinsa.

Voidaan arvioida, että pk-yritysten tietoturvan erityinen haavoittuvuus on niiden toimintaympäristö. Resurssipuutteet, vähäinen henkilöstömäärä ja hajanaiset toimintamallit heikentävät yritysten mahdollisuutta rakentaa systemaattisia tietoturvakäytäntöjä. Tämän seurauksena yksittäiset virheet vaikuttavat pk-yrityksissä paljon laajemmin kuin suurissa organisaatioissa, joissa on hajautettu vastuita ja toimintamekanismeja monimuotoisemmin.

Tutkimukset [19], [21], [26], osoittivat myös, että tietoturvapoikkeamia ei voida katsoa pelkästään teknisinä ongelmina. Poikkeamilla voi olla merkittäviä vaikutuksia liiketoimintaan, asiakassuhteisiin sekä taloudelliseen vakauteen. Näin ollen tietotur-

vapoikkeamia voidaan pitää myös liiketoimintariskeinä ja niiden torjuminen tulee ottaa huomioon osana liiketoiminnan kehittämisstrategiaa. Nämä havainnot korostuivat erityisesti tutkimuksissa [3], [4], jossa tietoturvapoikkeamat johtivat yrityksen strategisen operaation ulkopuolelle esimerkiksi mainehaittaan tai asiakasluottamuksen heikentymiseen.

Kokonaisuutena tutkimuskirjallisuus osoitti, että pk-yritysten tietoturvapoikkeamien torjunta edellyttää laajaa ymmärrystä liiketoimintastrategiasta, teknisistä ongelmista ja ihmisten toimintatavoista sekä siitä, miten nämä vaikuttavat toisiinsa. Tämä muodostui kirjallisuuskatsauksen keskeisimmäksi havainnoksi.

4.2 Juurisyiden ja torjuntatoimien välinen yhteys

Tarkasteltaessa kirjallisuutta havaittiin, että tietoturvapoikkeamien juurisyillä ja tehokkaimmilla torjuntatoimilla oli selkeä yhteys. Tämä näkyi erityisesti inhimillisiin virheisiin ja osaamispuutteisiin liittyvissä juurisyissä, jotka pystyttiin yhdistämään johdonmukaisesti torjuntatoimiin, mitkä liittyivät henkilöstön koulutukseen ja tietoturvatietoisuuden korostamiseen. Tästä on perusteltua päätellä, että tehokkain tapa torjua tietoturvapoikkeamia on kohdistaa toimenpiteitä suoraan taustalla vaikuttaviin juurisyihin.

Tulosten perusteella voidaan päätellä, että tekniset kontrollit ovat välttämättömiä, mutta niiden vaikutus voi jäädä vähäiseksi jos niitä ei tueta riittävällä osaamisella ja oikeanlaisilla toimintamalleilla. Esimerkiksi tietojenkalastelussa tekniset kontrollit vähentävät riskiä, mutta lopullinen vaikutus riippuu siitä, miten hyvin henkilöstö on koulutettu tunnistamaan tietojenkalasteluyrityksiä.

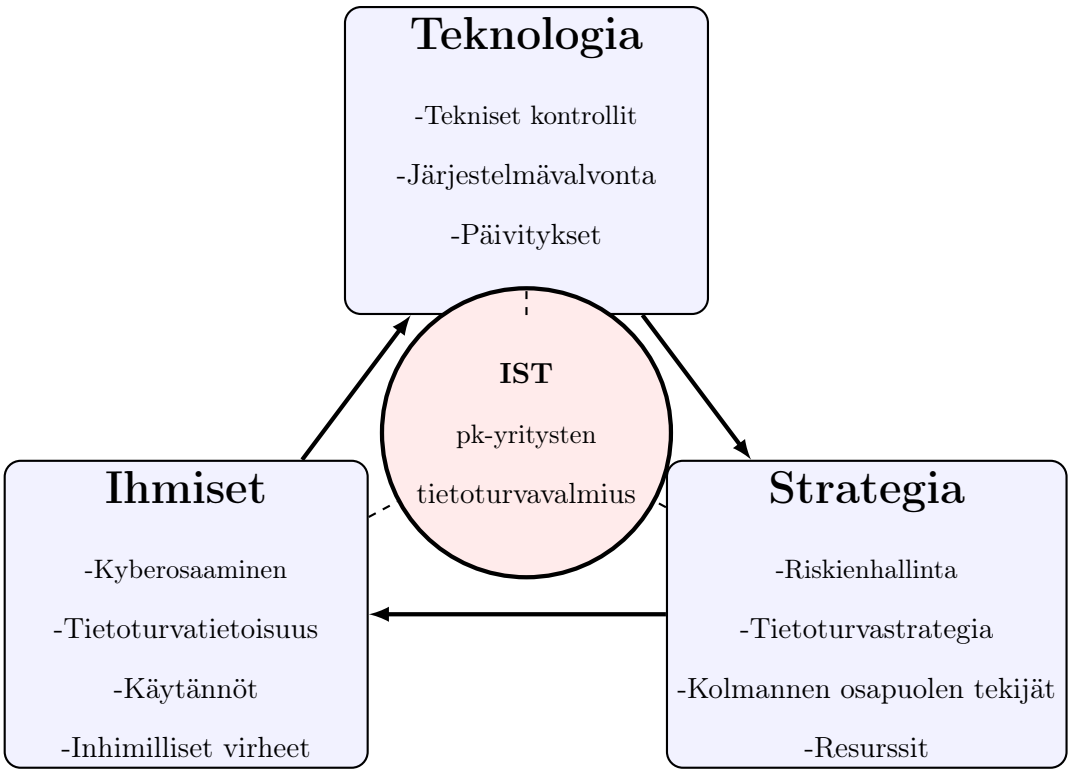
Vastaavasti resurssien puutteeseen ja riskienhallintaan liittyvissä tutkimuksissa [5], [10], [24], nousi esille strategisempi näkökulma. Näissä tapauksissa tehokkaimmiksi torjuntatoimiksi nousi riskien ennakointiin ja selkeään vastuun jakamiseen liittyvät torjuntatoimet. Näin ollen on havaittavissa, että tietoturvapoikkeamien ehkäi-

sy liittyy olennaisesti myös siihen, miten tietoturva on organisoitu osaksi yrityksen päätöksentekoa ja johtamista.

Tästä voidaan päätellä, että tietoturvapoikkeamia voidaan välttää kohdistamalla torjuntatoimet suoraan juurisyihin systemaattisesti ja ennakoiden. Tämä nostaa esiin kokonaisvaltaisen ja ennaltaehkäisevän tietoturvamallin pk-yrityksille.

4.3 IST-malli pk-yrityksille

Edellä mainittujen havaintojen perusteella tässä kirjallisuuskatsauksessa luotiin IST-malli (kuva 4.1), jonka tarkoituksena on selkeyttää pk-yritysten tietoturvapoikkeamien torjuntaa jakamalla juurisyyt ja torjuntatoimet kolmeen ulottuvuuteen: ihmiset, strategia ja teknologia.



Kuva 4.1: IST-malli pk-yritysten tietoturvavalmiuden keskeisistä osa-alueista

Ihmiset-ulottuvuudella kuvataan toimintatapoihin, inhimillisiin virheisiin ja koulutuksen puutteeseen liittyviä ongelmia. Kirjallisuudessa tämä näkyi erityisesti puutteellisena kyberosaamisena ja tilanteina, jossa työntekijä ei kyennyt tunnistamaan poikkeavaa toimintaa ajoissa. Tämä ulottuvuus korostaa inhimillisyyden osuutta tietoturvapoikkeamien torjumisessa. Vaikka teknisellä tasolla tietoturva olisi riittävä, ihmiset ovat kuitenkin keskiössä ja osaamisen täytyy olla sellaisella tasolla, että tietoturvallisuus toteutuu myös käytännön tasolla.

Strategia-ulottuvuudella puolestaan kuvataan yrityksen riskienhallintaa, resurssien kohdentamista ja johtamista. Strateginen ulottuvuus nousi kirjallisuudessa esiin etenkin silloin, kun yrityksillä ei ollut selkeitä toimintatapoja tai tietoturvakäytäntöjä. Kun tietoturva kyetään ottamaan suoraan osaksi yrityksen liiketoimintaa, eikä sitä pidetä irrallisena teknisenä osana pystytään ennaltaehkäisemään tietoturvapoikkeamia tehokkaasti.

Teknologia-ulottuvuus kattaa tekniset kontrollit ja järjestelmän valvontaan liittyvät riskit. Kirjallisuus osoitti, että teknologisilla ratkaisuilla on suuri merkitys tietoturvapoikkeamien torjumisessa, mutta se ei yksinään riitä jos muut ulottuvuudet ovat puutteellisia.

IST-mallin keskeinen tulkinta on se, että pk-yritysten tietoturvapoikkeamat syntyvät usein näiden kolmen ulottuvuuden rajapinnoissa. Kun kaikki ulottuvuudet tukevat toisiaan, on yrityksillä erinomaiset valmiudet torjua tietoturvapoikkeamia. Vastaavasti puute yhdessäkin ulottuvuudessa heikentää yrityksen tietoturvaa merkittävästi. IST-malli auttaa hahmottamaan pk-yritysten tietoturvaa isona kokonaisuutena ja kokoaa kirjallisuudesta tehdyt havainnot selkeäksi malliksi.

4.4 Käytännön merkitys pk-yrityksille

Tämän työn havainnolla on käytännön merkitystä pk-yrityksille erityisesti tietoturvan kehittämisen näkökulmasta. Kirjallisuuden perusteella pk-yritysten tulisi katsoa tietoturvaa kokonaisuutena eikä irrallisina toimenpiteinä.

IST-malli auttaa hahmottamaan pk-yritysten tietoturvallisuuden ulottuvuuksia. Mallin avulla voidaan tarkastella esimerkiksi henkilöstön osaamista, vastuiden jakoa ja teknisten kontrollien riittävyyttä ja näin ollen kehittää tietoturvaa laaja-alaisesti.

Tämä on erityisen merkittävää pk-yrityksille niiden resurssirajoitteiden vuoksi. IST-mallin avulla resurssit voidaan kohdistaa tehokkaasti oikeisiin juurisyihin ja samalla vähentää tilanteita, jossa resursseja käytetään turhaan teknisiin ratkaisuihin ilman, että niiden taustalla oleviin inhimillisiin ja strategisiin riskeihin on puututtu.

Tämä kaikki tukee sitä, että pk-yrityksen tietoturva tulee sitoa osaksi liiketoimintastrategiaa ja johtamista. Kun tietoturvalliset toimintatavat on integroitu osaksi yrityksen joka päiväistä toimintaa, tietoturvallisuudesta tulee pitkäjänteistä ja kustannustehokasta.

4.5 Työn luotettavuus ja rajoitteet sekä jatkotutkimusehdotukset

Tämän työn luotettavuutta vahvistaa se, että kirjallisuuskatsaus on toteutettu käyttämällä tutkimusaineistona vertaisarvioituja tutkimuksia kolmesta eri hakukannasta. Näin ollen oli mahdollista rakentaa laaja kuva pk-yrityksiin kohdistuvista tietoturvapoikkeamista, niiden juurisyistä ja torjuntatoimista.

Työllä on kuitenkin myös rajoitteita. Ensinnäkin tutkimuskenttä osoittautui osittain rajalliseksi, sillä tietoturvapoikkeamia käsiteltiin hieman eri määritelmin tutkimusten välillä. Toisena rajoitteena oli se, että useassa tutkimuksessa pk-yrityksiä

tarkasteltiin osana laajempaa yritysjoukkoa, jolloin pk-yritysten ominaispiirteet eivät nousseet esille.

Myös aineiston rajaus vaikutti muodostuneeseen kuvaan. Tutkimusaineistoa valittaessa ulkopuolelle jäi väistämättä tutkimuksia, jotka olisivat hyödyttäneet tätä kirjallisuuskatsausta. Tutkimusten välillä oli myös eroja yritysten toimialojen välillä, mikä vaikuttaa tämän kirjallisuuskatsauksen yleistettävyyteen.

IST-malli on tämän työn pohjalta muodostettu synteesi, jonka on tarkoitus jäsentää tutkimuksen havaintoja. Sitä ei ole testattu empiirisesti, minkä vuoksi sen käytännön toimivuutta ei voida todentaa täysin varmaksi. Tästä huolimatta malli tarjoaa teoriaan perustuvan viitekehyksen, joka on kirjallisuuteen perustuva.

Jatkotutkimuksissa olisi tarpeen tarkastella IST-mallia empiirisesti. Erityisen mielenkiintoista olisi arvioida mallin ulottuvuuksien painoarvoa eri toimialojen välillä. Lisäksi olisi perusteltua tutkia sitä, miten eri torjuntatoimet vaihtelevat eri toimintaympäristöissä ja arvioida tarkemmin sitä, että nouseeko jokin niistä toistuvasti esille tehokkuudellaan.

5 Yhteenveto

Tässä tutkielmassa tarkasteltiin pienten ja keskisuurten yritysten tietoturvapoikkeamia sekä niiden keskeisiä juurisyitä ja tehokkaimpia torjuntatoimia. Tutkimuksen tavoitteena oli luoda laaja kokonaiskuva siitä, millaiset tietoturvapoikkeamat korostuvat pk-yrityksissä, mistä ne yleisimmin johtuvat ja millaisilla torjuntakeinoilla niitä voidaan ehkäistä tehokkaasti. Näihin kysymyksiin pyrittiin vastamaan kolmen tutkimuskysymyksen avulla hyödyntäen ajankohtaisia ja vertaisarvioituja tieteellisiä tutkimuksia.

Ensimmäinen tutkimuskysymys tarkasteli mitkä ovat yleisimmät tietoturvapoikkeamat pk-yrityksissä. Kirjallisuuden perusteella yleisimmiksi osoittautuivat tietojenkalasteluyritykset, tietomurrot, haittaohjelmat, luvaton pääsy, sosiaalinen manipulointi, kolmannen osapuolenkautta tapahtuvat hyökkäykset sekä järjestelmien haavoittuvuuksiin liittyvät poikkeamat. Poikkeamia esiintyi vaihtelevasti eri tutkimusten välillä, mutta etenkin tietojenkalasteluyritykset, tietomurrot sekä luvaton pääsy nousi toistuvasti esille. Tulokset osoittavat, että pk-yritysten tietoturvapoikkeamat kohdistuvat sekä henkilöstöön että teknisiin järjestelmiin minkä vuoksi niiden vaikutukset vaikuttavat laajasti yritysten liiketoimintaan, asiakassuhteisiin ja operatiiviseen toimintaan.

Toinen tutkimuskysymys käsitteli tietoturvapoikkeamien keskeisiä juurisyitä. Kirjallisuuden perusteella merkittävimmiksi juurisyiksi nousi inhimilliset virheet, kyberosaamisenpuute, resurssipuute, cyber hygiene -puutteet, kolmannen osapuo-

len riskit, puutteellinen riskienhallinta, puutteellinen tietoturvastrategia sekä puutteet teknisissä kontrolleissa. Tarkastelu osoitti, että juurisyyt esiintyvät harvoin toisistaan irrallisina, vaan useista tekijöistä koostuvasta kokonaisuudesta. Erityisesti inhimilliset virheet ja organisatoriset puutteet korostuivat yleisimpinä juurisyinä ja havaittiin, että taustalla vaikutti usein monesta pienestä asiasta koostuva yhdistelmä.

Kolmannessa tutkimuskysymyksessä tarkasteltiin tehokkaimpia torjuntatoimia tietoturvapoikkeamiin. Kirjallisuuden perusteella keskeisimmiksi torjuntatoimiksi nousi riskien arviointi, tietoturvapolitiikat ja hallinto, kyberturvakoulutus, cyber hygiene -käytännöt, tekniset kontrollit, kolmannen osapuolen riskien hallinta sekä tietoturvakäytäntöjen integrointi prosesseihin. Kirjallisuus osoitti, että torjuntatoimien tehokkuus nousi erityisesti silloin, kun niitä kohdistettiin suoraan taustalla vaikuttavaan juurisyyhyn systemaattisesti ja ennaltaehkäisevästi. Tämän perusteella tietoturvapoikkeamien torjunta pk-yrityksissä täytyy ennen kaikkea olla jatkuvaa ja moniulotteista.

Tutkielmassa muodostettiin IST-malli, missä koottiin kirjallisuuden perusteella tehdyt havainnot yhdeksi kokonaisuudeksi. Mallissa tietoturvapoikkeamien taustatekijöitä tarkastellaan kolmen ulottuvuuden kautta. Ihmiset- ulottuvuus käsittelee inhimillisiä virheitä ja osaamisen puutteeseen liittyviä virheitä. Strategia -ulottuvuus käsittelee riskien hallintaa ja organisatorisia käytäntöjä. Teknologia -ulottuvuus puolestaan kuvaa yrityksen teknisiä kontrolleja, sekä järjestelmien haavoittuvuuksia. Todettiin, että tietoturvapoikkeamat syntyvät erityisesti näiden ulottuvuuksien rajapinnoissa. Vastaavasti kun kaikki ulottuvuudet tukevat toisiaan yrityksille muodostuu toimiva ja tehokas tietoturva.

Kokonaisuutena tämä kirjallisuuskatsaus osoittaa, että pk-yritysten tietoturvapoikkeamien ehkäisy edellyttää laaja-alaista ja systemaattista lähestymistapaa. Tietoturva ei usein näyttäydy vain teknisenä ongelmana vaan osana yrityksen päivittäis-

tä toimintaa, riskien hallintaa ja strategista päätöksentekoa. Tämän vuoksi tietoturvan kehittäminen vaatii henkilöstön osaamista, selkeitä toimintamalleja ja riittäviä teknisiä kontrolleja.

Lähdeluettelo

[1] S. Dua, P. Shah ja E. G. AbdAllah, ”Navigating the Digital Landscape: Enhancing Small and Medium Business’s Security through Asset Management and Data Classification”, *Proceedings - Swiss Conference on Data Science, SDS*, s. 55–61, 2024. DOI: 10.1109/SDS60720.2024.00016.

[2] N. Huaman et al., ”Proceedings of the 30th USENIX Security Symposium”, 2021, s. 1235–1252, ISBN: 978-1-939133-24-3. url: https://www.usenix.org/system/files/sec21-huaman.pdf.

[3] A. K. Tetteh, ”Cybersecurity needs for SMEs”, *Issues in Information Systems*, vol. 25, s. 235–246, 1 2024. DOI: 10.48009/1_iis_2024_120.

[4] M. El-Hajj ja Z. A. Mirza, ”ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool”, vol. 13, 19 lokakuu 2024, ISSN: 2079-9292. DOI: 10.3390/electronics13193910.

[5] M. Awan ja A. Alam, ”Cybersecurity Threats and Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study”, vol. 15, 12 joulukuu 2025. DOI: 10.3390/admsci15120481.

[6] Euroopan komissio. ”The new SME definition: User guide and model declaration”, viitattu 14. huhtikuuta 2026. url: https://publications.europa.eu/resource/cellar/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1.0007.01/DOC_1.

[7] Euroopan unionin neuvosto. ”Pk-yritysten tukeminen”, Euroopan unionin neuvosto, viitattu 14. huhtikuuta 2026. url: https://www.consilium.europa.eu/fi/policies/support-to-small-and-medium-sized-enterprises/.

[8] Tilastokeskus. ”Mikä on pk-yritysten vaikutus talouteen – määritelmällä on väliä”, Tilastokeskus, viitattu 14. huhtikuuta 2026. url: https://stat.fi/tietotrendit/artikkelit/2023/mika-on-pk-yritysten-vaikutus-talouteen-maaritelmalla-on-valia.

[9] M. Tsiodra, S. Panda, M. Chronopoulos ja E. Panaousis, ”Cyber Risk Assessment and Optimization: A Small Business Case Study”, *IEEE Access*, vol. 11, s. 44 467–44 481, 2023, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3272670.

[10] M. K. Hadap, A. K. Mehta, G. Narsimlu, P. Jawarkar, V. Kaluvala ja A. K. Chaturvedi, ”An Empirical Study on the Economic Impact of Cybersecurity Breaches and Computer Fraud on SMEs”, vol. 31, s. 93–97, 2 2025, ISSN: 2217-8961. DOI: 10.63278/1340.

[11] Suomi.fi-sanastot, *Tietoturvapoikkeama*, https://sanastot.suomi.fi/terminology/ths/concept/concept-36, Viitattu 17.4.2026, 2024.

[12] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton ja J. Sweetnam, ”Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events”, National Institute of Standards ja Technology (NIST), NIST Special Publication 1800-26, 2020. viitattu 17. huhtikuuta 2026. url: https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html.

[13] S. A. Tamimi, ”Towards Beyond Technology: Reviewing Human Error (HE) as the Primary Reason of Cyber Security Breaches”, teoksessa *2025 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)*, 2025, s. 1–6. DOI: 10.1109/ACDSA65407.2025.11166279.

[14] A. B. A. Ali, R. K. Ayyasamy, R. Akbar, V. A. Ponnusamy ja L. E. Heng, "Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME)", teoksessa *2022 IEEE 5th International Symposium in Robotics and Manufacturing Automation (ROMA)*, 2022, s. 1–6. DOI: 10.1109/ROMA55875.2022.9915696.

[15] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024", European Union Agency for Cybersecurity, tekninen raportti, 2024. DOI: 10.2824/0710888.

[16] M. Falch, H. Olesen, K. E. Skouby, R. Tadayoni ja I. Williams, "Cybersecurity Strategies for SMEs in the Nordic Baltic Region", *Journal of Cyber Security and Mobility*, vol. 11, s. 727–753, 6 2022. DOI: 10.13052/jcsm2245-1439.1161.

[17] S. Kandpal, S. Bhatt, L. Mohan, A. Patwal ja P. Kumar, "Cyber Security Implementation Issues in Small to Medium-sized Enterprises (SMEs) and their Potential Solutions: A Comprehensive Analysis", teoksessa *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, s. 1–5. DOI: 10.1109/ICCCNT56998.2023.10307363.

[18] D. J. Button, J. Ophoff, A. Irons ja S. McDonald, "Mind the gap: exploring perceptions of cyber security in the SME context", *Information and computer security*, helmikuu 2025, ISSN: 2056-4961. DOI: 10.1108/ICS-02-2025-0047.

[19] L. Kocksch ja T. E. Jensen, "The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small-and Medium-Sized Enterprises", *Proceedings of the ACM on human computer interaction*, vol. 8, CSCW2, CCW2 marraskuu 2024. DOI: 10.1145/3686893.

[20] G. Loskorikh, E. Shebeshten, O. Koval, K. L. Bagrii ja N. Valkova, "Risks of cyberattacks on accounting: Analysis of modern threats and preventive

measures", *Sustainable Engineering and Innovation*, vol. 7, s. 493–506, 2 2025. DOI: 10.37868/sei.v7i2.id574.

[21] B. Lill, C. Sauerwein, N. Mexis ja K. Langner, "A Comprehensive Review of Information Security Research regarding SMEs and Future Directions", *Journal of Cyber Security and Mobility*, vol. 14, s. 1245–1288, 5 2025. DOI: 10.13052/jcsm2245-1439.1459.

[22] T. Ncubukezi, L. Mwansa ja F. Rocaries, "Review of the Current Cyber Hygiene in Small and Medium-sized Businesses", 2020, s. 160–165, ISBN: 978-1-913572-21-1. DOI: 10.23919/ICITST51030.2020.9351339.

[23] S. Dua, P. Shah ja E. G. AbdAllah, "Managing Third Party Risk for Small and Medium Enterprises", 2024, s. 209–214, ISBN: 979-8-3315-2720-4; 979-8-3315-2719-8. DOI: 10.1109/FiCloud62933.2024.00039.

[24] A. Cartwright ja E. Cartwright, "Underinvestment in cyber security: Quantifying cyber security behavior in UK businesses", helmikuu 2025, ISSN: 0047-2778. DOI: 10.1080/00472778.2025.2549068.

[25] N. Mkhulisi, S. Dube ja F. Radebe, "Towards a Conceptual Framework for Cybersecurity Skill Requirements in Small and Medium-Sized Enterprises", teoksessa *2024 4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, 2024, s. 408–415. DOI: 10.1109/IMITEC60221.2024.10851058.

[26] K. A. Saban, S. Rau ja C. A. Wood, "SME executives' perceptions and the information security preparedness model", vol. 29, s. 263–282, 2 2021, ISSN: 2056-4961. DOI: 10.1108/ICS-01-2020-0014.

[27] Y. Valdes-Rodriguez, J. Hochstetter-Diez, M. Dieguez-Rebolledo, A. Bustamante-Mora ja R. Cadena-Martinez, "Analysis of Strategies for the Integration of Security Practices in Agile Software Development: A Sustainable

SME Approach", vol. 12, s. 35 204–35 230, 2024, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2024.3372385.