Tampereen yliopisto

Aleksi Puranen

ARVONLUONTI ASIAKASORGANISAATIOLLE TIETOTURVAN KONTEKSTISTA

Kandidaatintyö
Johtamisen ja talouden tiedekunta
Helmikuu 2024

TIIVISTELMÄ

Aleksi Puranen: Arvonluonti asiakasorganisaatiolle tietoturvan kontekstista
Kandidaatintyö
Tampereen yliopisto
Teknis-taloudellinen kandidaattiohjelma
Helmikuu 2024

Tämä tutkimus tarkastelee tietoturvan roolia organisaation arvonluonnissa. Tutkimuksessa yhdistetään systemaattinen kirjallisuuskatsaus ja asiantuntijahaastattelut. Tämä kahden menetelmän strategia mahdollistaa kattavamman katsauksen siitä, miten tietoturvatoimenpiteet, etenkin sertifioinnit edistävät potentiaalista arvoa organisaatioissa, ja korostaa näkökulmaa, että tietoturvaa ei enää pidetä pelkkänä suojaustoimenpiteenä vaan mahdollistajana luottamuksen rakentamisessa, tuotemerkin maineen parantamisessa ja kilpailuedun turvaamisessa.

Tuloksena havaittiin, että tietoturvasertifikaatit, kuten ISO/IEC 27001, ovat merkittäviä indikaattoreita organisaation sitoutumisesta korkeaan tietoturvatasoon, joka lisää sen markkina-arvoa ja asiakkaiden luottamusta, koska ne ovat merkki arkaluonteisten tietojen vankasta suojaamisesta ja sitoutumisesta hyviin käytäntöihin. Lisäksi tutkimuksessa laajennetaan tietoturva-arvon taloudellista näkökulmaa aineettomiin hyötyihin, kuten asiakastyytyväisyyteen ja koettuun potentiaaliseen arvoon.

Avainsanat: tietoturva, arvonluonti, tietoturvasertifikaatti

SISÄLLYSLUETTELO

TERMIT JA KÄSITTEET

Arvo	tavaran, palvelun tai toiminnan kyky tyydyttää tarve tai tuottaa hyötyä. Voidaan jakaa vaihtoarvoon, eli arvoon, joka syntyy palvelun tai tuotteen vastaanottamisesta tuottajalta, ja käyttöarvoon, joka ilmenee palvelun tai tuotteen hyödyntämisestä. Lisäksi voidaan huomioida kontekstiarvo, joka ottaa huomioon palvelun tai tuotteen käytön kontekstin. (Haksever et al., 2004; Vargo et al., 2008)
Arvonluonti	asiakkaan hyvinvoinnin lisäämiseen tähtäävä vuorovaikutteinen prosessi, jossa asiakas ja tuottaja yhdessä luovat ja kokevat arvoa tuotteiden tai palvelujen avulla (Grönroos & Voima 2013)
Tietoturva	hallinnollisten ja teknisten toimien yhdistelmä, joka varmistaa tiedon luottamuksellisuuden, eheyden ja saatavuuden, ns. "CIA"-triadin. (Whitman & Mattord, 2016 s. 8; Kyberturvallisuuden sanasto, 2018)
Tietoturvan hallintajärjestelmä (ISMS)	toimintaperiaatteet, menettelytavat, ohjeet ja niihin liittyvät resurssit ja toiminnot, joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan (ISO, 2020).
Tietoturvasertifiointi	Ulkoisesti tarkastettu todiste tietoturvan prosessikokonaisuuden toimivuudesta
ISO/IEC 27001	Standardi, joka sisältää vaatimukset ja ohjeistukset tietoturvan hallintajärjestelmän perustamiseen, implementointiin, ylläpitoon ja jatkuvaan parantamiseen. (ISO, 2022).
Potentiaalinen arvo	tuottavan organisaation prosessit ja resurssit, joiden on mahdollista tuottaa arvoa asiakkaalle hyödyntämisen yhteydessä (Grönroos & Voima 2013)

1. JOHDANTO

Digitalisaation ja tiedon merkityksen kasvun myötä organisaatioilla on yhä suurempi tarve ylläpitää asianmukaista tietoturvan tasoa. Organisaatiot panostavat taloudellisesti tietoturvaan eri tavoin riippuen organisaation koosta ja tietoturvatarpeista. Taloudellinen panostaminen tietoturvaan on haastavaa, ja oikeiden tarpeiden tunnistaminen on vaikeaa. Usein organisaatiot investoivat liikaa tiettyyn tietoturvan osa-alueeseen, jolloin muut osa-alueet jäävät alirahoitetuiksi tai niihin ei investoida lainkaan (Safi et al., 2021).

Nykymaailmassa myös arvon ja arvonluonnin käsite on muuttunut. Perinteinen suoran rahallisen voiton tai tappion määritelmä ei riitä arvioimaan, onko tuote tai palvelu arvokas käyttäjälleen. Arvon määritelmä on laajentunut käsittämään myös aineettomia näkökohtia, kuten miten tuote vastaa asiakkaan tarpeisiin tai mitä asiakas tuntee/kokee tuotetta käyttäessään (Koskela-Huotari, 2021). Tietoturvassa arvoa on kuitenkin tutkittu lähinnä perinteisestä näkökulmasta, eli miten tietoturvainvestoinnit vaikuttavat arvoon suorassa rahassa mitattuna. Kirjallisuudessa eräässä systemaattisessa kirjallisuuskatsauksessa tarkasteltiin 37 erilaista relevanttia julkaisua tietoturvatapahtumien merkityksestä organisaation osakekurssille. Suurin osa julkaisuista (75,6 %) esitti, että tietoturvatapahtumilla on tilastollinen merkitys osakekursseihin (Georgios & Lefteris, 2016). Tämän tutkimuksen tavoitteena on laajentaa näkökulmaa siihen, miten tietoturvan arvo koetaan ja voidaanko tietoturvaa käyttää arvonluonnissa muuhunkin, kun rahallisen arvon mittaamiseen.

Tämä perinteisen arvokäsitteen laajentaminen on erityisen tärkeää tietoturvan kannalta. Digitaalisten uhkien muuttuessa yhä kehittyneemmiksi ja laajemmalle levinneiksi tietoturvan rooli arvon luomisessa ulottuu pelkkien riskien lieventämistä laajemmalle. Nykyaikaisten organisaatioiden on huomattava, että tehokkailla tietoturvastrategioilla voidaan lisätä asiakkaiden luottamusta ja tyytyväisyyttä, vahvistaa brändin mainetta ja luoda suoraa kilpailuetua. Tunnistamalla tietoturvan vaikutukset epäsuorempiin ja hankalammin mitattaviin arvoihin, organisaatiot voivat kehittää kokonaisvaltaisemman käsityksen tietoturvainvestointiensa hyödyistä.

Lisäksi tässä tutkimuksessa pyritään selvittämään, voidaanko tietoturvaa esittää osana arvolupausta. Esimerkiksi tietojen eheyden ja luottamuksellisuuden varmistaminen ei

ainoastaan suojaisi tappioilta vaan myös edistäisi asiakasuskollisuutta ja houkuttelisi uusia asiakkaita, jotka arvostavat tietoturvallisempia ratkaisuja. Lisäksi aloilla, joilla tietosuojasäännösten noudattaminen on ratkaisevan tärkeää, vankat tietoturvatoimenpiteet voivat estää kalliita oikeudellisia seuraamuksia ja maineen vahingoittumista.

Tämän tutkimuksen lähestymistapa vastaa nykyisiä liiketoimintasuuntauksia, joissa arvonluonti nähdään yhä useammin moniulotteisena, ja siihen sisältyy sekä aineellisia että aineettomia hyötyjä. Kun tämä laajempi näkökulma sisällytetään tietoturvainvestointistrategioihin, organisaatiot voivat tehdä tietoon perustuvia päätöksiä, jotka ovat linjassa niiden yleisten liiketoimintatavoitteiden kanssa, ja reagoida tehokkaammin kehittyvään digitaaliseen ympäristöön.

Yhteenvetona voidaan todeta, että tämän tutkimuksen tavoitteena on valaista arvon moniulotteisuutta tietoturvan yhteydessä, kyseenalaistaa perinteinen kustannuskeskeinen näkemys ja ehdottaa kattavampaa kehystä tietoturvan ymmärtämiseksi ja hyödyntämiseksi arvon luomisen strategisena välineenä.

1.1 Tutkimuksen tausta

Tutkimuksen tavoitteena on tutkia, miten tietoturvaa voidaan hyödyntää arvonluonnin prosessissa ja miten asiakkaat kokevat toimittajan tietoturvatilanteen vaikuttavan hankintapäätökseen. Tutkimusongelmaksi nousee kirjallisuudessa havaittu puute, eli tietoturvan vaikutusta arvonluontiin on tutkittu vähän laadullisella tasolla. Nykyinen kirjallisuus on katsonut aihetta markkina-arvon, investointien, sekä taloudellisten tietojen analyysien kautta, mutta inhimillisempi alan asiantuntijoiden katsaus ja mielipiteet aiheeseen liittyen tulevat heikosti esille.

Itse tutkimus rajataan käsittelemään, tietoturvan arvoa etenkin sertifikaattien kautta ja miten ne edistävät arvonluontia. Tietoturvatason mittaaminen sertifikaattien avulla on kiintopiste, joka ei perustu isompaan tulkinnanvaraan, tai monimutkaisimpiin tapoihin mitata tietoturvan tasoa. Näin pyritään saamaan näkökulmaa siihen, onko tietoturvallisempi organisaatio (sertifikaatin omaava) esimerkiksi houkuttelevampi yhteistyökumppani, kuin vähemmän tietoturvallinen organisaatio (ei sertifioitu). Tietoturvan arvoa, sekä arvonluontia tietoturvalla pohditaan sekä kirjallisuuteen, että asiantuntijoiden haastatteluihin perustaen.

Näiden rajausten ja tavoitteiden pohjalta on muodostettu päätutkimuskysymys, sekä sitä tukevat alatutkimuskysymykset. Kysymyksiin pyritään vastaamaan tutkimuksessa. Päätutkimuskysymykseksi on muodostettu seuraava:

P: Tuottavatko tietoturvasertifioidut organisaatiot enemmän arvoa asiakkaille?

Päätutkimuskysymyksen tueksi on valittu kaksi kappaletta apututkimuskysymyksiä, jotka edesauttavat päätutkimuskysymykseen vastaamisessa. Apututkimuskysymykset ovat seuraavat:

A1: Millä tavoin tietoturvallisemmat ratkaisut ovat arvokkaampia asiakkaille?

A2: Lisäävätkö organisaation tietoturvasertifikaatit asiakassuhteen solmimisen todennäköisyyttä?

Näiden kysymysten avulla tutkimuksessa pyritään tarjoamaan kattavampi käsitys tietoturvan roolista arvonluontiprosessissa. Perinteisten taloudellisten mittareiden lisäksi huomioon otetaan myös asiakkaiden käsitykset, markkina-asema ja strategiset edut. Tutkimuksen tavoitteena on tarjota tietoa siitä, miten organisaatiot voisivat hyödyntää tietoturvaprosesseja ns. ”pakollisen pahan” lisäksi myös kilpailuvalttina ja luoda arvoa asiakkailleen niiden avulla.

1.2 Tutkimuksen rakenne

Tutkimuksessa yhdistetään laadullinen kirjallisuuskatsaus, sekä haastattelututkimus, jota käytetään lisätiedonhankintamenetelmänä. Kirjallisuuskatsauksessa keskitytään tieteellisiin artikkeleihin, jotka käsittelevät tietoturvaa ja arvonluontia. Kirjallisuuskatsausta tuetaan teoriaosuudella, jossa pohjustetaan tietoturvaa, sekä arvonluontia. Teorian pohjalta rakennetaan haastattelurunko. Haastattelun tarve perustellaan siten, että aiheeseen liittyvä tutkimusaineisto on liian suppea riittääkseen puhtaaseen kirjallisuuskatsaukseen. Lisäksi haastattelulla pyritään tuomaan aiheeseen relevantteja asiantuntijoiden näkemyksiä ja edistää aiheeseen liittyvää syvempää pohdintaa.

Kirjallisuuskatsauksessa aineisto käydään järjestelmällisesti läpi ja niistä pyritään löytämään yhteneväisyyksiä, sekä eroavaisuuksia, jotka auttavat vastaamaan tutkimuskysymyksiin. Kirjallisuuskatsauksen tukena käytetään haastatteluista saatuja tuloksia. Näiden pohjalta muodostetaan synteesi, jossa kerätään löydetyt havainnot yhteen. Tämän jälkeen tutkimuksen tulokset kerätään yhteen, sekä arvioidaan niiden laatua. Lisäksi tutkitaan, saatiinko tutkimuskysymyksiin tyydyttävät vastaukset. Lopuksi käsitellään vielä havaitut mahdollisuudet jatkotutkimukselle.

2. METODOLOGIA

2.1 Tutkimusaineisto

Kirjallisuuskatsaus toteutetaan Finkin (2014) seitsemän kohdan mallin mukaan, eli tutkimuskysymys määritellään, hakutietokannat valitaan, hakulausekkeet valitaan, käytännön rajauskriteerit valitaan, kuten vuosihaarukka, tutkimuksen asettelut, kielet..., aineiston metodologinen laatu analysoidaan, kirjallisuuskatsaus suoritetaan, sekä tulokset kootaan yhteen. Tutkimuskysymyksien valinta ja asetus on esitetty kappaleessa 1.2. Aineistoa etsitään pääasiallisesti kahden eri aihealueen, tietoturvan ja arvonluonnin leikkauspisteestä. Tässä työssä kirjallisuutta haetaan sähköisessä muodossa Tampereen Yliopiston kirjaston tietokannasta Andor ja Googlen tietokannasta Google Scholar. Kirjallisuus rajataan vertaisarvioituihin artikkeleihin, jotka ovat enintään viisi vuotta vanhoja.

Hakusanoina käytetään avainsanoja: ”information security”, ”cybersecurity”, ”value creation”, “value proposition”, ”certification” ja “value”. Aineiston hakeminen tapahtuu yhdistelemällä avainsanoja ja rajoittamalla hakutuloksia käyttämällä boolen operaattoreita hakulausekkeessa, sekä suodattamalla tuloksia tietokantojen tarjoamilla asetuksilla, kuten julkaisuvuodet ja aineistotyyppi. Alla on käytetyt hakulausekkeet.

Hakulauseke	**Andor**	**Google Scholar**	**Yhteensä**
"Information security" AND "value"	12 630	353 000	**365 630**
("information security" OR “cybersecurity”) AND "value creation"	152	17 700	**19 092**
("information security" OR "cybersecurity") AND "competetive advantage"	0	39	**39**
"information security" AND "value" AND "certification"	435	44 700	**45 135**
"value proposition" AND ("information security" OR "cybersecurity")	25 832	8000	**33 832**

Taulukko 1. *Tietokantojen hakutulokset*

Taulukosta huomataan, että hakulausekkeiden rajaamisesta huolimatta materiaalia löytyy paljon etenkin Googlen tietokannasta. Hakutuloksia rajattiin edelleen siten, että haun suorittamisen jälkeen tietokannan tarjoamista artikkeleista käytiin läpi kaksi ensimmäistä sivua, joilta valittiin aiheeseen liittyvät materiaalit. Kirjallisuuskatsauksen materiaaleihin valittiin artikkeleita, jotka ovat vähintään vuodelta 2019. Lähdemateriaaleja etsittiin arvonluontiin, tietoturvaan, tietoturvan arvoon, kyberturvaan ja tietoturvasertifikaattien arvoon liittyen. Arvonluonnista ja tietoturvasta löytyi erikseen paljon aineistoa, mutta arvonluontiin tietoturvalla, tai tietoturvan arvoon liittyen aineistoa on suppeasti.

Valittujen kirjallisuusmateriaalien metodologista laatua ei analysoitu laajemmin. Kuitenkin artikkelien julkaisukanavat tarkistettiin täyttävän vähintäänkin julkaisufoorumin (Julkaisufoorumi, 2023) luokan 1, eli perustason laadun varmistamiseksi.

Aineiston rajauksen ja arvioinnin jälkeen, kirjallisuuskatsaukseen valittiin kaksi artikkelia. Artikkelit käsittelevät tietoturvasertifikaattien vaikutuksia organisaation talouteen. Kirjallisuuskatsaukseen valikoitui artikkeleita vuosilta 2019–2022. Valittu kirjallisuus on esitetty alla olevassa taulukossa 3.

Taulukko 2. *Kirjallisuuskatsauksen materiaali*

Tekijät	**Otsikko**	**Kuvaus**	**Julkaisukanavan jufo-luokitus (Julkaisufoorumi, 2023)**
Deane et.al (2019)	The effect of information security sertification announcements on the market value of the firm	Tutkii organisaation tietoturvasertifioinnin vaikutusta pörssikursseihin.	2, Johtava taso
Podrecca et.al (2022)	Information security and value creation: The performance implications of ISO/IEC 27001	Tutkii organisaation ISO 27001 sertifioinnin vaikutusta taloudelliseen tulokseen, sekä suhteeseen vaikuttavia taustamuuttujia	2, Johtava taso

2.2 Haastattelun toteutus

Haastattelu toteutetaan puolistrukturoituna haastatteluna. Haastatteluita varten on luotu haastattelurunko, mutta kysymysten järjestystä voidaan vaihdella. Lisäksi vastauksia ei olla sidottu vastausvaihtoehtoihin, joten haastateltava vastaa kysymyksiin omin sanoin. (Hirsijärvi & Hurme, 2008, 47) Tämä edesauttaa syvempää pohdintaa ja mahdollistaa uusien näkökulmien löytämisen. Haastateltavia on viisi kappaletta. Kolme haastatelta-

vista, joista kaksi työskentelee samassa organisaatiossa, edustavat kahta yksityisen sektorin organisaatiota. Loput kaksi haastateltavaa edustavat yhtä julkisen sektorin tutkimuslaitosta. Haastatteluista kaksi pidettiin kasvotusten, yksi puhelimitse ja kaksi Microsoft Teams- palvelun välityksellä. Haastattelut äänitettiin ja tallennettiin haastateltavan luvalla. Äänityksiä ei litteroitu täysin, vaan kysymyksistä muodostettiin taulukko, johon kunkin haastateltavan vastauksista muodostettiin synteesi ja poimittiin mahdollisesti suoria lainauksia.

Alla esimerkki, miten haastattelut dokumentoitiin kirjalliseen muotoon:

Taulukko 3. *Haastatteluvastausten litterointi - esimerkki*

Haastateltava:	**Henkilö 1**	**Henkilö 2**	**Henkilö 3**
Kysymys 1:	Haastateltavan 1 vastaus tiivistettynä	Haastateltavan 2 vastaus tiivistettynä	Haastateltavan 3…
Kysymys 2:	…	…	…
Kysymys 3:	…	…	…

Osittaisen litteroinnin jälkeen haastatteluiden tallennukset poistettiin haastateltavan tietojen suojaamisen vuoksi. Haastattelumateriaalia kertyi yhteensä 2h 36min. Keskimääräisesti yksi haastattelu kesti 31min. Haastateltavat henkilöt ovat esitelty alla:

Haastateltava henkilö	**Virallinen työnimike**	**Organisaatio**
Henkilö 1 (H1)	Chief Security Officer	Osakeyhtiö 1
Henkilö 2 (H2)	Chief Information Security Officer	Osakeyhtiö 1
Henkilö 3 (H3)	Toimitusjohtaja	Osakeyhtiö 2
Henkilö 4 (H4)	Chief Information Security Officer	Tutkimuslaitos 1
Henkilö 5 (H5)	Tietoarkkitehti	Tutkimuslaitos 1

Taulukko 4. *Haastateltavat henkilöt*

Tässä tutkimuksessa haastattelulla pyritään edesauttamaan tutkimuskysymyksiin vastaamisessa sekä keräämällä syvempiä havaintoja monimutkaisista tietoturvan ilmiöistä, että kartoittamaan ovatko kirjallisuudesta poimitut havainnot ristiriidassa asiantuntijoiden lausuntojen kanssa.

Haastateltaviksi valikoitui pääasiallisesti eri johtotehtävissä toimivia tietoturva-asiantuntijoita, jotka edustavat tapauskohtaisesti sekä palvelun toimittajia, että asiakkaita. Haastateltavat toimivat lisäksi sekä julkisella, että yksityisellä sektorilla. Näin pyritään varmistamaan monipuolinen tiedonkeruu, vaikka otanta onkin jokseenkin pieni. Haastattelut itsessään toteutettiin puolistrukturoituna haastatteluina, jotka noudattavat karkeasti haastattelurunkoa. Haastattelumuoto kuitenkin mahdollistaa lisäkysymyksien kysymisen, sekä kysymysten järjestyksen vaihtamisen. Haastatteluissa käytettiin seuraavaa runkoa. Kysymyksiä ei toimitettu haastateltaville etukäteen.

2.3 Haastattelurunko

1. Nimi, virallinen työnimike ja työtehtävät?

Keskeinen teoria:

2. Miten määrittelisit tietoturvan?
3. Mitä käsite ”arvo” tarkoittaa?
4. Mitä tarkoitetaan arvonluonnilla?

Arvonluonti tietoturvan näkökulmasta:

5. Millaisessa roolissa tietoturva on organisaatiossanne / miten tietoturva on otettu huomioon strategiassa?
6. Mikä tekee tietoturvasta arvokasta? / Mistä tietoturvan arvo muodostuu?
7. Voidaanko tietoturvasta antaa arvolupausta?
8. Mihin tietoturvan arvolupaukset perustuvat?
9. Voidaanko tietoturvatasoa mitata?
10. (Miten tietoturvatasoa mitataan?)
11. Millä tavoin tietoturvatasoa voidaan mitata organisaatioissa?
12. Millä tavoin tietoturvallisemmat ratkaisut ovat arvokkaampia asiakkaalle?
13. Ovatko tietoturvasertifikaatit hyvä tapa lisätä tuotteen arvoa?
    a. Lisäävätkö sertifikaatit todennäköisyyttä saada asiakassuhteita?
    b. Vaativatko asiakkaat sertifikaatteja?
    c. Saavuttaako sertifikaateilla suoraa kilpailuetua?
14. Tunnistavatko asiakkaat tietoturvan arvon?
15. Millä seikoilla tietoturvaa voitaisiin käyttää arvonluontiin?
16. Voidaanko tietoturvaa käyttää arvonluontiin, ja jos voi niin miten?
17. Onko asiakkaalta tullut palautetta palvelusta liittyen tietoturvaan. Millaista palaute on ollut?

3. TIETOTURVA

Yksi määritelmä tietoturvalle, on hallinnolliset ja tekniset toimet, joilla varmistetaan tiedon ns. ”CIA” triadi (*eng. confidentiality, integrity and availability*), tällä tarkoitetaan luottamuksellisuutta, eheyttä ja käytettävyyttä. (Kyberturvallisuuskeskus, 2018)(Whitman & Mattord, 2016 s. 8) Lundgren & Möller, 2017)(ISO/IEC 27000) Tiedon luottamuksellisuus tarkoittaa sitä, että tieto ei ole sivullisten käytettävissä (Sanasto). Tiedon saatavuus rajoitetaan niille tahoille, joilla on oikeus hyödyntää tietoa. Mikäli tieto pääsee väärien tahojen käsiin, tiedon luottamuksellisuus on rikottu. Tiedon luottamuksellisuuden varmistamisen menetelmiä ovat esimerkiksi tiedon luokittelu, turvallinen dokumenttien ja datan varastointi, yleisten turvakäytäntöjen noudattaminen, tiedon säilyttäjien ja loppukäyttäjien kouluttaminen ja tiedon kryptaus, eli salaaminen. (Whitman & Mattord, 2016) Tiedon luottamuksellisuus on erityisen kriittistä, kun käsiteltävänä on työntekijöiden, asiakkaiden, tai potilaiden tietoja (Whitman & Mattord, 2016) Kokonaisuudessaan luottamuksellisuus on tietoturvan ominaisuus, joka varmistaa, että tietoja ei anneta tai luovuteta luvattomille henkilöille, yhteisöille tai prosesseille (Lundgren & Möller, 2017).

Tiedon eheydellä tarkoitetaan tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa (Kyberturvallisuuskeskus, 2018). Eheys on ominaisuus, joka kuvaa tarkkuutta ja kokonaisuutta. (ISO/IEC 27000) Tiedon eheys on uhattuna, jos tieto korruptoituu, tuhoutuu, tai kohtaa muuta häiriötä, joka muuttaa tiedon alkuperäistä muotoa. Tiedon korruptio voi tapahtua tiedon tallentamisen, muokkaamisen, tai siirron aikana. Näiden sisäisten uhkien lisäksi, tiedon eheyttä uhkaa myös ulkoiset tekijät, esimerkiksi tietokonevirukset. (Whitman & Mattord, 2016) Eheys on ominaisuus, joka kuvaa tiedon tarkkuutta ja kokonaisuutta (Lundgren & Möller, 2017).

Tiedon saatavuus tarkoittaa, että tieto on hyödynnettävissä ja saatavilla haluttuna aikana (Kyberturvallisuuskeskus, 2018). Käyttäjillä ja järjestelmillä tulee olla pääsy tietoon, joka on hyödyllisessä muodossa. Saatavuus toimii yhdessä luottamuksellisuuden kanssa, joten tieto tulee olla saatavilla vain sille oikeutetuille tahoille. (Whitman & Mattord, 2016)

Nykyajan tarpeet tekevät CIA-määritelmästä itsessään riittämättömän määrittelemään koko tietoturvaa. Tämä johtuu rajatusta määritelmästä ja jatkuvassa muutoksessa olevasta toimintoympäristöstä. Jotta tietoturvan nykytilanne saadaan paremmin määriteltyä, lisätään määritelmään CIA-triadin ominaisuuksien lisäksi vielä seuraavat ominai-

suudet ja prosessit: yksityisyys, tunnistettavuus, todentaminen, valtuutus ja vastuuvelvollisuus. (Whitman & Mattord, 2016) Yksityisyydellä tarkoitetaan, että dataa käytetään vain datan omistajan sallimin tavoin. Tunnistettavuudella tarkoitetaan järjestelmän kykyä tunnistaa käyttäjä, joka yrittää päästä käsiksi tietoihin. Todennuksella tarkoitetaan järjestelmän kykyä varmistaa, että tunnistautuva käyttäjä on se, kuka hän väittää olevansa. Todennuksen jälkeen valtuutusprosessi määrittelee, kuinka laajaan tietomäärään käyttäjällä on luku- ja muokkausoikeus. Vastuuvelvollisuudella tarkoitetaan sitä, että järjestelmä yhdistää jokaisen aktiviteetin johonkin käyttäjään, automatisoituun prosessiin, tai järjestelmään. (Whitman & Mattord, 2016)

Vaihtoehtoinen tietoturvan määritelmä on ”*Appropriate Access*” AA-malli, joka pyrkii huomioimaan paremmin inhimilliset, organisatoriset, kulttuurilliset, käytännölliset ja lainsäädännölliset tietoturvaongelmat. Missä CIA- triadia käytetään yleisenä tietoturvan määritelmänä, sekä ns. ”tarkistuslistana” tietoturvan nykytilasta, AA-malli pyrkii vain määrittelemään tietoturvan konseptina. (Lundgren & Möller, 2017) AA-malli määrittelee tietoturvan jonkin turvattavan objektin, toimijan ja sidosryhmän välisenä suhteena (Lundgren & Möller, 2017). Yleinen AA-mallin määritelmä on ”Objekti O on turvallinen sidosryhmälle H, jos ja vain jos: jokaisella toimijalla A ja jokaisella O:n osalla P, A:lla on juuri sopiva pääsy P:hen suhteessa sidosryhmään H” (Lundgren & Möller, 2017). AA-mallin määritelmä kuvaa absoluuttista tietoturvaa, eli tilaa, jossa jokin objekti on täysin tietoturvattu. Lundgren & Möller (2017) kritisoivat, että perinteinen CIA- malli on riittämätön määritelmä tietoturvalle. Kuitenkin CIA määritelmä, tai jokin siihen perustuva laajempi malli, joka käyttää CIA-määritelmää pohjanaan on yleisesti eniten käytössä oleva perusmääritelmä tietoturvalle.

3.1 ISO/IEC Tietoturvasertifiointi

Organisaatiot voivat halutessaan hakea sertifiointia todisteena jonkin prosessikokonaisuuden toimivuudesta. Tietoturvan hallinnan prosesseihin on olemassa ISO/IEC ISMS standardiperhe. Standardiperhe on jaettu neljään osaan, jotka ovat: sanastostandardi, vaatimusmäärittelyt, ohjeelliset standardit, ja sektorikohtaiset ohjeelliset standardit. (ISO, 2018 27000) Pääasiallisesti organisaatiot pyrkivät hankkimaan vaatimusstandardin ISO/IEC 27001 sertifioinnin. Itse sertifiointi saadaan ulkoisen tarkastajan (tahon) todetessa, että organisaatio täyttää riittävät vaatimukset (kontrollit) sertifikaatin myöntämiseen (ISO, 2022iso.org a).

ISO/IEC 27001 standardi on organisaation kannalta strateginen päätös. Se sisältää vaatimukset ja ohjeistukset tietoturvan hallintajärjestelmän *(eng. information security management system / ISMS)* perustamiseen, implementointiin, ylläpitoon ja jatkuvaan

parantamiseen. Tämä tietoturvallisuuden hallintajärjestelmä pyrkii siihen, että tietoturvan CIA triadi toteutuu. ISO/IEC kuvailee ISO/IEC 27001 standardin hyötyjä organisaatiolle seuraavasti: standardi kattaa tietojen suojaamisen paperisessa-, pilvi- ja digitaalisessa muodossa, parantaa vastustuskykyä kyberhyökkäyksiä kohtaan, tarjoaa keskitetyn viitekehyksen joka turvaa kaiken tiedon, varmistaa organisaatiolaajuisen suojan teknologiaan perustuvia riskejä kohtaan, edesauttaa kehittyviin tietoturvauhkiin vastaamista, vähentää tehottomaan puolustusteknologiaan liittyviä kustannuksia, ja suojaa tiedon luottamuksellisuutta, eheyttä ja käytettävyyttä (ISO, 2022).

3.2 Tietoturvan hallintajärjestelmä

Erityyppiset ja erikokoiset organisaatiot keräävät, käsittelevät, tallentavat ja välittävät tietoa, ja ne pitävät sitä kriittisenä voimavarana. Näihin toimintoihin liittyy luontaisia riskejä tietovaroille, kuten hyökkäysuhkia, virheitä ja muita odottamattomia onnettomuuksia. Tietoturva on elintärkeää näiden varojen suojaamiseksi ja niiden saatavuuden, luottamuksellisuuden ja eheyden varmistamiseksi. (ISO, 2020) Järjestelmän tietoturvallisuudesta voidaan sanoa: ”Tietojärjestelmä S on turvallinen sidosryhmälle H, jos ja vain jos: jokaisella toimijalla A ja jokaisella S:n osalla P, A:lla on juuri sopiva pääsy S:ään suhteessa sidosryhmään H” (Lundgren & Möller, 2017). Järjestelmien turvaus onkin välttämätöntä liiketoiminnan tehokkuuden ja lainsäädännön noudattamisen kannalta. Tietoturvallisuuden hallintaan kuuluu asianmukaisten valvontatoimien toteuttaminen ja uusien riskien jatkuva käsittely seurannan, arvioinnin ja parantamisen avulla. (ISO, 2020)

Tietoturvan hallintajärjestelmä ”koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista ja toiminnoista, joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan” (ISO, 2020). Se on systemaattinen lähestymistapa, jolla perustetaan, toteutetaan, käytetään, seurataan, arvioidaan, ylläpidetään ja parannetaan tietoturvaa liiketoiminnan tavoitteiden mukaisesti. Se perustuu riskinarviointeihin ja organisaation riskinsietokykyyn, ja siihen kuuluu asianmukaisten valvontatoimien soveltaminen tietovarallisuuden suojaamiseksi. (ISO, 2020)

Tietoturva keskittyy tietojen luottamuksellisuuteen, saatavuuteen ja eheyteen. Siihen kuuluu erilaisten uhkien hallinta ISMS:n puitteissa toteutettavien asianmukaisten valvontatoimien avulla. Siihen kuuluvat politiikat, prosessit, menettelyt ja tekniset ratkaisut, joilla varmistetaan, että organisaation tietoturva- ja liiketoimintatavoitteet saavutetaan. Näiden valvontatoimien integrointi liiketoimintaprosesseihin on ratkaisevan tärkeää.

ISMS:n johtamiseen kuuluu organisaation prosessien ohjaaminen ja parantaminen tietovarallisuuden suojaamiseksi. Siihen kuuluu tietoturvapolitiikkojen, -menettelyjen ja -ohjeiden laatiminen ja toteuttaminen koko organisaatiossa. Johtamisrakenteet vaihtelevat organisaation koon ja monimutkaisuuden mukaan.

Johtamisjärjestelmä tarjoaa puitteet organisaation tavoitteiden saavuttamiselle ja kattaa organisaatiorakenteen, toimintatavat, vastuualueet ja resurssit. Tietoturvan yhteydessä sillä varmistetaan asiakkaiden ja sidosryhmien turvallisuusvaatimusten täyttäminen, säännösten noudattaminen ja tietovarantojen hallinta organisaation tavoitteiden mukaista jatkuvaa parantamista varten.

4. ARVO JA ARVONLUONTI

4.1 Arvo käsitteenä

Arvon suoranainen määritelmä on haastavaa tämän monitahoisen- ja tulkinnallisen luonteen vuoksi. Arvo on yleinen alan termi, jota käyttävät sekä akateemikot, että alan muut toimijat, mutta usein on silti epäselvää, mitä arvolla tarkoitetaan eri yhteyksissä. (Jussila, Kärkkäinen, Helander…)

Porter (1985) määrittää arvon yksinkertaisesti summana, minkä asiakas on valmis maksamaan tuotteesta tai palvelusta. Haksever et. al (2004) taas määrittelevät arvon artikkelissaan tavaran, palvelun tai toiminnan kyvyksi tyydyttää jokin tarve, tai tuottaa hyötyä henkilölle tai oikeushenkilölle. Arvo voidaankin määritellä jakamalla se karkeasti vaihtoarvoon *(value in exchange)* ja käyttöarvoon *(value in use)*. (Haksever et al., 2004; Vargo et al., 2008)

Vaihtoarvo määritellään arvoksi, joka syntyy kun palvelu, tai tuote vastaanotetaan tuottajalta ja vastaanottaja tarjoaa tuottajalle jonkin hyödykkeen (Vargo & Lusch, 2008). Vaihtoarvo itsessään on transaktionallista, ja kuvaakin käytännössä rahan vaihtoa johonkin palveluun / tuotteeseen.

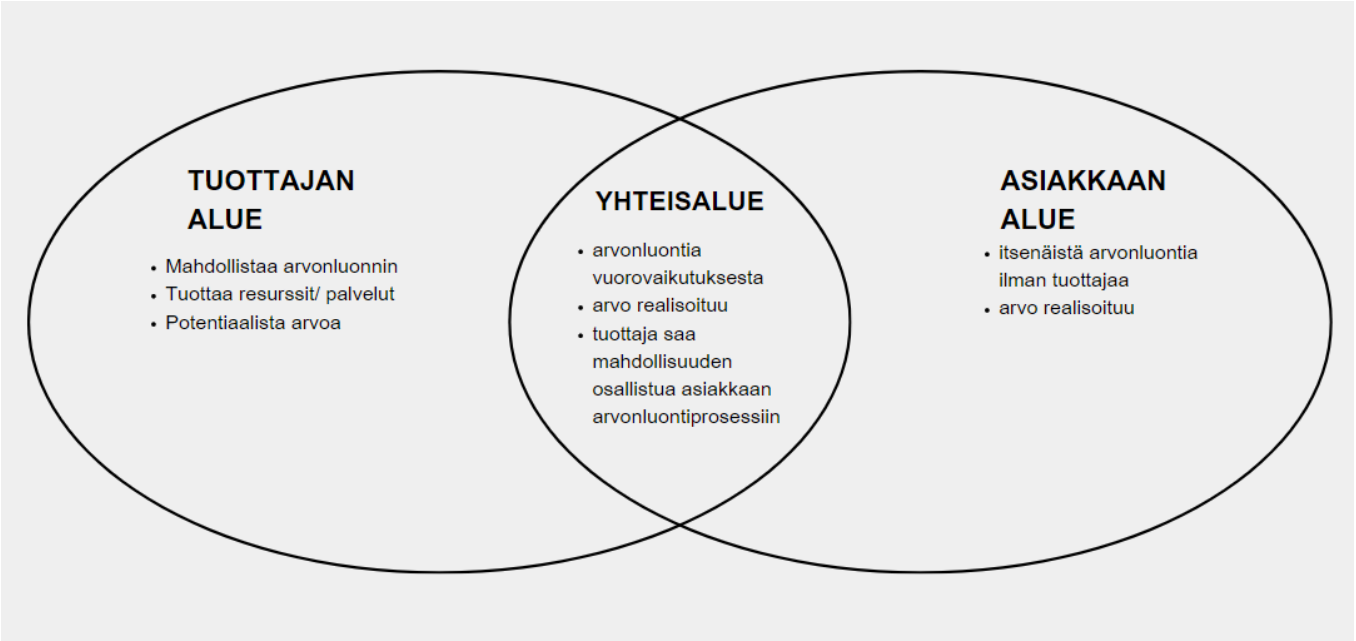
Käyttöarvo taas on arvo, joka syntyy, kun jotakin palvelua, tai tuotetta hyödynnetään. Arvoa yhteisluodaan tässä tapauksessa. Tuotteen tai palvelun kehittäjä soveltaa omaa osaamistaan, kun taas asiakas käyttää omia resurssejaan edesauttamaan kehittäjää luomaan lisää arvoa (tavallisesti rahanvaihdon yhteydessä). Käyttöarvon tueksi voidaan nostaa lisäksi kontekstiarvo *(value in context)*, joka ottaa huomioon kontekstin, missä sidosryhmä, tai henkilö käyttää palvelua, tai tuotetta. (Vargo et al., 2008) Yleistasolla voidaan sanoa arvon olevan jotain, joka tekee jostain asiasta ”parempaa” (Grönroos, 2011).

4.2 Arvonluonti

Arvonluonti on keskeinen käsite markkinoinnin ja liiketoimintastrategian alalla. Viime vuosien siirtymä tuotekeskeisestä logiikasta *(eng. goods-dominant logic)* palvelukeskeiseen logiikkaan *(eng. service-dominant logic)* on johtanut siihen, että on arvioitu uudelleen sitä, miten arvoa luodaan, koetaan ja toimitetaan. (Grönroos, 2011)

Arvonluonnissa on pohjimmiltaan kyse asiakkaan hyvinvoinnin lisäämisestä ja siitä, että asiakkaat ”voivat paremmin” eri tavoin. Tämä hyvinvoinnin lisäys voi ilmetä eri tavoin, riippuen palvelukohtaamisen konteksteista. (Grönroos & Voima, 2013)

Nykyaikainen käsitys arvonluonnista perustuu arvon yhteisluonnin konseptiin. Kun tuotekeskeisessä logiikassa keskitytään arvon tuottamiseen, palvelukeskeisessä logiikassa painotetaan enemmän käyttöarvoa. (Vargo & Lusch, 2004) Nykyisellään arvonluonti vaatii asiakkaan panosta. Asiakas kokee käyttöarvoa ja arvioi sitä kokemuksellisessa ja pitkäkestoisessa prosessissa. (Grönroos & Voima, 2013) Voidaankin ajatella arvonluonnin tapahtuvan kolmella alueella: tuottajan alueella, asiakkaan alueella, sekä näiden leikkauspisteessä, eli yhteisalueella (Grönroos & Voima, 2013).



Kuva 1. *Arvonluonnin alueet (mukaillen Grönroos & Voima 2013)*

Tuottajan alue tarjoaa resurssit ja palvelut, joita potentiaalisesti käytetään asiakkaan toimesta. Pääpaino on sellaisten tuotteiden tai palvelujen tuottamisessa, joilla oletetaan olevan arvoa asiakkaille. Tuottajan alueella arvo on vielä potentiaalista. Alueiden leikkauspisteissä tapahtuu arvon yhteisluontia, missä tuottaja ja asiakas ovat vuorovaikutuksessa ja vaikuttavat toistensa prosesseihin. Yhteisellä alueella sekä palveluntarjoaja että asiakas osallistuvat aktiivisesti arvonluontiprosessiin, ja vuorovaikutus voi vaikuttaa merkittävästi asiakkaan kokemukseen ja käsitykseen arvosta. Asiakkaan alueella arvoa luodaan itsenäisesti ilman tuottajan suoraa osallistumista. Asiakkaat voivat luoda ja luovat arvoa tuotteen tai palvelun ostamisen jälkeen, usein tavoilla, joita tuottaja ei ole tarkoittanut tai ennakoinut. Tällä alueella korostetaan asiakkaan omien resurssien, prosessien ja kontekstien merkitystä arvon luomisessa. Itse arvo realisoituu potentiaalisesta arvosta konkreettiseksi arvoksi yhteisalueella ja asiakkaan alueella. (Grönroos

2013) Interaktio on siis keskeisessä roolissa arvon yhteisluonnissa. Tämä vuorovaikutus muuntaa arvonluonnin asiakkaan itse kokeman sijaan dialogiseksi prosessiksi, jossa tuottajalla on mahdollisuus vaikuttaa asiakkaan arvonluontiprosessiin positiivisesti, tai negatiivisesti. (Grönroos, 2013)

Tässä tutkimuksessa arvonluonnin prosessia tarkastellaan tietoturvasertifioinnin kautta. Tietoturvasertifioinnit, kuten ISO/IEC 27001, määrittelevät prosessit, miten organisaatiot hallinnoivat ja turvaavat tietovarantojaan. Arvonluonnin näkökulmasta näitä sertifiointeja voidaan pitää toimintoina, jonka avulla organisaatiot paitsi suojaavat omaa omaisuuttaan myös lisäävät asiakkailleen tarjoamiensa palvelujen potentiaalista arvoa tuottajan alueella. Tietoturvasertifioinnin puitteissa arvonluonti keskittyy tuottajan alueelle, jossa *”palveluntarjoaja mahdollistaa (esim. tuottaa ja toimittaa) asiakkaan arvonluontia resursseilla/prosesseilla, joita käytetään ja jotka koetaan asiakkaan piirissä”* (Grönroos & Voima 2013).

5. TIETOTURVA ARVONLUONNIN NÄKÖKULMASTA

Vaikka negatiivisten tietoturvatapahtumien vaikutuksia on tutkittu kattavasti (Georgios & Lefteris 2016), kirjallisuudessa on perehdytty vain niukasti proaktiivisten tietoturvatoimien vaikutuksiin. Näissä tapauksissa ISO 27001 sertifiointia on käytetty mittarina proaktiivisista toimista, jonka jälkeisvaikutuksia on sittemmin havainnoitu osakekurssien ja taloudellisen suorituskyvyn avulla.

5.1 ISO/IEC 27001- sertifikaatin arvo organisaatiolle kirjallisuudessa

Deane et.al (2019) keskittyvät ISO 27001 -sertifiointia koskevien tiedotteiden vaikutusta organisaation osakekurssiin. Tutkimus suoritettiin tapahtumatutkimuksena, jossa analysoitiin 111 julkista ilmoitusta jonkin organisaation onnistuneesta ISO 27001 sertifioinnista. Otokset kerättiin vuosilta 2005–2015 ja analyysi pohjautui epänormaaliin tuottoon, eli todellisen tuoton ja markkinamalleihin perustuvan odotetun tuoton erotukseen julkaisupäivän ympärillä. Tutkimuksessa otettiin myös kantaa siihen, miten toimiala, yrityksen koko ja tiedotuksen ajoitus (ennen tai jälkeen vuoden 2013, joka kategorisoidaan tutkimuksessa merkittäväksi vuodeksi tietoturvatapahtumien suhteen) saattavat vaikuttaa markkina-arvoon. (Deane et.al 2019)

Tutkimuksessa havaittiin, että ISO 27001 -sertifiointia koskeviin ilmoituksiin liittyy keskimäärin positiivisia epänormaaleja tuottoja. Vaikutuksen huomattiin myös vaihtelevan toimialakohtaisesti, rahoitusalalla ja valmistavassa teollisuudessa positiivinen vaikutus oli merkittävämpi. Myös pienemmillä yrityksillä oli suurempia positiivisia epänormaaleja tuottoja kuin suuremmilla yrityksillä, ja vuoden 2013 jälkeiset ilmoitukset reagoivat positiivisemmin, mikä heijastaa tietoturvauhkien ja -hallinnan kehittyvää tilannetta. (Deane et.al 2019) Tulokset viittaavat siihen, että osakkeenomistajat arvostavat investointeja kvantifioitaviin tietoturvainvestointiin, ja ne voivat nostaa yrityksen markkina-arvoa (Deane et.al 2019).

Podrecca et.al (2022) taas keskittyvät enemmän organisaation taloudelliseen suorituskykyyn ja sisäisiin hyötyihin ISO 27001- sertifiointiprosessin aikana. Tutkimuksessa analysoitiin sekä ISO 27001 -sertifioinnin vaikutusta organisaation taloudelliseen suorituskykyyn, että toimialan ja organisaation ominaispiirteitä, jotka vaikuttavat ISO 27001 -

sertifioinnin ja taloudellisen suorituskyvyn välisiin suhteisiin. Tutkimuksessa analysoitiin 143 yhdysvaltalaisesta pörssiyhtiöstä koostuvaa aineistoa käyttäen pitkäaikaista tapahtumatutkimusta ja pienimmän neliösumman regressioanalyysiä. Painopisteinä olivat yhtiöiden kannattavuus, tehokkuus ja myynti. (Podrecca et.al 2022)

Kannattavuuden osalta sertifioitu organisaatio suoriutuu jatkuvasti paremmin kuin sertifioimaton. Ero on tilastollisesti merkitsevä ja positiivinen, ja se on erityisen huomattava vuosien t + 1 ja t + 2, t ja t + 2, t-2 ja t + 1 sekä t-2 ja t + 2 välillä, missä t = sertifikaatin myöntämisvuosi. (Podreccca et.al 2022)

Työn tuottavuuden osalta tulokset ovat samalla linjalla. Sertifioitujen organisaatioiden työn tuottavuus on kasvanut merkittävästi, erityisesti ajanjaksoilla t + 1 - t + 2, t - t + 2 ja t-2 - t + 2. Nostettakoon mielenkiintoiseksi havainnoksi se, että tuottavuus paranee eniten vuonna t + 2. Tämä viittaa siihen, että yritykset saavat merkittävimmät hyödyt työn tuottavuuden kannalta vasta sen jälkeen, kun ne ovat omaksuneet ja sisäistäneet ISO/IEC 27001 -standardiin liittyvät uudet käytännöt. (Podrecca et.al 2022)

Myyntituloksen analyysi taas antaa hieman erilaisen kuvan. Tässä tapauksessa merkittäviä positiivisia muutoksia havaitaan lähinnä sertifiointiprosessin aikana eikä niinkään sen jälkeen. Myynnin paraneminen on merkittävää väleillä t-2 ja t-1, t-2 ja t, t-2 ja t+1 sekä t-2 ja t+2. Myynti siis kasvaa itse prosessin aikana, eikä niin merkittävästi sen jälkeen. Artikkelissa ilmiölle esitetään kaksi mahdollista syytä: ensiksi ISO 27001 saattaa olla asiakkaiden asettama edellytys yhteistyön aloittamiselle. Toiseksi asiakkaan ja toimittajan väliset odotetut hyödyt saattavat alkaa muodostua jo ennen virallista sertifiointia. (Podrecca et.al 2022)

5.1.1 Tietoturvasertifioinnin implikaatiot potentiaaliseen arvoon

Sisäisten prosessien näkökulmasta ISO 27001 -sertifiointi näyttäisi toimivan yhtenä mahdollistajana organisaatioiden toiminnan tehokkuuden ja työn tuottavuuden parantamisessa. Kuten Podrecca et al. (2022) toteavat, sertifiointiprosessiin liittyy tilastollisesti merkittäviä parannuksia kannattavuudessa ja työn tuottavuudessa erityisesti sertifiointia seuraavina ajanjaksoina. Tämä voisi viitata siihen, että ISO 27001 -standardien sisäistäminen edistää jatkuvan parantamisen kulttuuria, jossa organisaatioita kannustetaan jalostamaan prosessejaan ja optimoimaan resurssien kohdentamista parempien tulosten saavuttamiseksi. Sertifiointi ei ainoastaan merkitse vakiintuneiden tietoturvakäytäntöjen noudattamista, vaan se myös käynnistää organisaatiomuutoksia, jotka joh-

tavat parempaan suorituskykyyn kannattavuuden ja tuottavuuden osalta. (Podrecca et al., 2022)

Asiakkaiden näkökulmasta ISO 27001 -sertifioinnilla näyttäisi olevan rooli käsitysten ja luottamuksen muodostumisessa. Sertifiointi on merkki organisaation sitoutumisesta jatkuvaan auditointiin ja korkeiden tietoturvanormien ylläpitämiseen. Tämä on erityisen tärkeää aikana, jolloin tietomurrot ja tietoturvauhat ovat sekä kuluttajien että yritysten yleisiä huolenaiheita. Podrecca et al. (2022) havaitsema odotettu myynnin paraneminen sertifiointiprosessin aikana korostaa ISO 27001 -sertifioinnin merkitystä asiakkaiden luottamuksen lisäämisessä ja liiketoimintakumppanuuksien edistämisessä. Se osoittaa, että markkinat pitävät ISO 27001 -sertifiointia arvokkaana voimavarana jo ennen sertifiointiprosessin muodollista päättymistä, mikä korostaa odotuksia asiakkaiden ja toimittajien keskinäisistä hyödyistä, jotka johtuvat tehostetuista tietoturvatoimenpiteistä.

ISO 27001 -sertifiointi tuo myös lisäarvoa vaikuttamalla myönteisesti markkinoiden arvostukseen, kuten Deanen et al. (2019) havainnot osoittavat. ISO 27001 -sertifioinnin julkistamisen ja positiivisen epänormaalin tuoton välinen yhteys viittaa siihen, että sijoittajat tunnistavat tietoturvaan tehtävien investointien arvon. Lisäksi sertifiointia pidetään strategisena investointina, joka voi lisätä yrityksen markkina-arvoa, mikä kuvastaa tietoturvan kasvavaa merkitystä. Vuoden 2013 jälkeinen myönteinen markkinareaktio osoittaa edelleen, että tietoturvainvestointien tietoisuus ja arvostus ovat lisääntyneet vastauksena kehittyviin kyberuhkiin. (Deane et al., 2019)

Ainakin voidaan siis sanoa, että itse ISO 27001 sertifiointi, sekä siihen johtava prosessi kasvattavat organisaation potentiaalista arvoa tuottajan alueella. Sertifiointi vaikuttaa kattavasti organisaation sisäisiin prosesseihin, joiden tehostaminen ja parantaminen taas epäsuorasti

5.2 Haastatteluaineiston analyysi

Jokaisella haastateltavalla oli hieman eri käsitys siitä, miten tietoturva voitaisiin määritellä ja mitä se kattaa. H1 käsittää sen kattavana prosessina, jonka tarkoituksena on suojella tietoja uhkilta liiketoiminnan jatkuvuuden varmistamiseksi ja riskien minimoimiseksi, huomioiden sekä reaktiivisen, että proaktiivisen lähestymisen. H3 laajentaa tätä näkemystä sisällyttämällä siihen fyysiset näkökohdat ja korostaa, että tietoturva ylittää digitaaliset rajat ja kattaa myös organisaation fyysisiä varantoja. H3 lisäksi mainitsee CIA- triadin toteutumisen. H4:n määritelmä tuo esiin oikeudellisen ja vaatimustenmukaisuuden ja korostaa tietojen suojaamista lakisääteisten velvoitteiden ja organisaa-

tion etujen mukaisesti. H5:n määritelmä keskittyy enemmän luvattoman levittämisen estämiseen, korostaen tiedon tarkoituksenmukaista hyödyntämistä. H2´:n mukaan tietoturva kiteytetään liiketoiminnallisten tavoitteiden suojelijaksi, jolloin se liitetään suoraan organisaation strategisiin tavoitteisiin.

Käsitys arvosta esiintyi kenties kaikista monimuotoisemmin, joka puoltaa myös teoriaa siltä osalta, ettei käsite ole yksiselitteinen. Huomioitavaa on se, että haastateltavat sisällyttivät itse tietoturvan vastaukseen, mitä luultavimmin johtuen siitä, että haastattelu muuten käsitti tietoturvaa. H1 liittää arvon asiakastyytyväisyyteen ja liiketoiminnan menestykseen ja pitää tietoturvaa asiakkaiden luottamuksen ja siten myös markkinamenestyksen edistäjänä. H3:n näkemys arvosta, joka koostuu aineellisista ja aineettomista hyödykkeistä, korostaa tietoturvan organisaatiolle ja sen sidosryhmille tuomia monitahoisia etuja. H5 ja H2 pohtivat syvällisemmin arvon muodostumiseen vaikuttavia sisäisiä ja ulkoisia tekijöitä ja esittävät, että tuotteen tai palvelun ja siten myös sen perustana olevan tiedon merkitys määräytyy kysynnän ja sen kyvyn tyydyttää tiettyjä tarpeita tai toiveita perusteella.

Kaikki osallistujat tunnustivat yksimielisesti tietoturvan strategisen roolin, mikä korostaa sen merkitystä pelkkää teknistä toteutusta tärkeämpänä. Tietoturva on liiketoimintastrategian peruspilari (H1), liiketoimintojen luonteen kannalta olennainen (H3), tiedon eheyden säilyttämisen, sekä mainehaittojen minimoimisen kannalta kriittinen (H4) ja elintärkeä organisaation tavoitteiden saavuttamisen kannalta (H5 ja H2). Tämä yksimielisyys kuvastaa sitä, että tietoturva nähdään strategisena voimavarana, joka on olennainen osa nykyaikaisten organisaatioiden toimintaa. Tietoturvan roolin korostaminen operatiivisten tarpeiden tukemisessa, uhkilta suojautumisessa ja liiketoimintatavoitteiden mahdollistamisessa kertoo sen keskeisestä asemasta organisaation suunnittelussa ja strategiassa.

Tietoturvan arvo koettiin monitahoiseksi. H1 korostaa tietoturvan arvon merkitystä erityisesti luottamuksen luomisessa uusiin asiakkaisiin, esimerkiksi osoittamalla organisaation sitoutumisen asiakastietojen suojaamiseen (H1). H3 laajentaa tätä käsitystä toteamalla, että tietoturva lievittää asiakkaiden tietosuojaan liittyviä pelkoja, mikä voi johtaa joissakin ääritapauksissa jopa suoraan rahalliseen arvoon vähentämällä tietomurtojen riskejä ja niihin liittyviä kustannuksia (H3). H2 taas näkee tietoturvan arvon seuraavasti: *”Tietoturvan päätehtävä on turvata pääliiketoiminta. Oikeastaan muuta tehtävää ei ole. Arvo tulee sitä kautta, että pääliiketoiminta on mahdollistettu.”* (H2). H4 korostaa tietoturvan hyödyllisyyttä ja suojaavaa roolia etenkin maineen säilyttämisessä, mikä on ratkaisevan tärkeää organisaation toiminnallisen menestyksen ja uskottavuuden kannalta (H4). H5 katsoo arvoa myös potentiaalisen mainehaitan kannalta: *”Ilman riittävää*

tietoturvaa organisaatiolle voi aiheutua merkittäviä toiminnallisia ja maineeseen liittyviä riskejä" (H5). H1 pohti myös siltä kannalta, että yli-investoiminen tietoturvaan ei kannata: *"Tietoturvalla voidaan myös tärvätä bisnescase, jos mennään kustannustasolla liian korkealle. Ei siis kannata mennä tietyn tietoturvatason yli, lainsäädäntö asettaa tietyt vaatimukset, jonka päälle laitetaan vielä kerros suojausta, jotta päästään riittävän hyvälle tasolle. Tästä yli meneminen on usein tehotonta."* (H1).

Haastattelussa tietoturvan mittaamiseksi H1 ehdottaa, että auditointi- ja vaatimustenmukaisuuskriteerien laatiminen voi auttaa mittaamaan tietoturvan tasoa organisaatiossa, esimerkiksi ISO 27001 standardin mukaisesti (H1). H3, H2, ja H4 mainitsevat myös ISO 27001 -standardin, joka tarjoaa suoria mittareita arviointiin (H4, H3, H2). H3 tuo myös esille esimerkiksi service-desk vasteajan mittaamisen yhtenä potentiaalisena keinona.

Mitä taas tulee ISO 27001 sertifiointiin, H1, H2, H3 ja H4 pitävät sertifiointeja hyödyllisinä, koska ne tarjoavat puitteet toiminnalle ja toimivat osoituksena organisaation sitoutumisesta tietoturvakäytäntöihin (H1, H2, H3, H4). Sertifikaatteja ei pidetä ainoastaan joidenkin asiakkaiden vaatimuksena vaan myös markkinointivälineenä, joka voi parantaa organisaation mainetta ja kilpailuasemaa (H1, H2). Sertifikaattien tehokkuus arvojen välittämisessä asiakkaille vaihtelee kuitenkin, ja H3 totesi, että asiakkaat vaativat usein turvallisuustasoa, joka ylittää pelkän sertifioinnin (H3).

Haastateltavien arviot asiakkaiden käsityksestä tietoturvan arvosta vaihtelevat. H1 ja H2 kertovat, että asiakkaat ovat muuttumassa vaativammiksi, vaativat todisteita turvatoimista ja tunnustavat hyvin turvallisten ratkaisujen arvon (H1, H2). H2 laajentaa vielä, kertoen, että: *"Snowden-casen jälkeen yleinen tietoisuus on noussut ja asiakkaat ovat asian päällä."* (H2). H3 tuo taas esille, että asiakkaiden yleinen ymmärrys tietoturvan arvosta saattaa olla puutteellinen (H3).

Mitä taas tulee yleisesti tietoturvan arvoon, H1 tuo esille, että tietoturva on harvoin ensisijainen syy järjestelmän hankkimiseen, mutta on kuitenkin oltava riittävällä tasolla. Tässä pohdinnassa tuotiin myös esille se, että potentiaalista arvoa tulee mainehaittojen minimoinnissa (H1). H4 ja H2 taas näkevät tietoturvan potentiaalisena myyntivaltina, erityisesti silloin, kun se vastaa asiakkaan arvoja ja vaatimuksia turvallisista ja luotettavista ratkaisuista (H4, H2). H2 pohtii näkökulmaa, missä arvoa voisi tulla lisää, mikäli tietoturvatasoa *"nostetaan selkeästi kilpailijoiden yläpuolelle"* (H2). Haastateltavat kokevat kuitenkin, että tietoturvasertifiointi voi olla hyvä tapa nostaa palvelun arvoa. Lähinnä siten, että sertifikaatilla voidaan ”kuitata” monet tietoturvakysymykset ja usein näin päästään kilpailijoiden edelle (H1, H2, H3). H3 toteaa myös, että tietoturvasertifi-

ointi on ollut suoraan strateginen investointi, joka mahdollisti uusien asiakassuhteiden solmimista ja on tuottanut suoraa liikevoittoa (H3).

5.3 Tietoturva osana organisaation potentiaalista arvoa

Edellä mainittujen tutkimusten ja haastattelujen antamien näkemysten pohjalta tässä osassa syvennytään vastaamaan syvällisemmin esitettyihin tutkimuskysymyksiin, jotka koskevat tietoturvasertifioinnin tuomaa lisäarvoa asiakkaiden näkökulmasta.

5.3.1 A1: Millä tavoin tietoturvallisemmat ratkaisut ovat arvokkaampia asiakkaille?

Vaikka tietoturva itsessään ei välttämättä ole pääasiallinen syy tehdä jokin hankinta, tietoturvalliset ratkaisut vaikuttaisivat olevan arvokkaampia asiakkaille. Tietoturvan osalta asiakkaan on noudatettava lainsäädännöllisiä vaatimuksia, jotka asettavat tietoturvan minimitason. Mahdollisen haitallisen tietoturvatapahtuman sattuessa mainehaitta voi kuitenkin olla suuri, vaikka lainsäädännön asettamat vaatimukset olisivatkin täytetty. Tässä tapauksessa tietoturva on ainakin sillä tavoin merkityksellinen, että suojatuimmilla ja ulkoisesti arvioiduilla prosesseilla mainehaitta voidaan minimoida. (H1) Maine- ja imagohaitat olivatkin hyvin yleinen teema haastatteluissa. Neljä viidestä haastateltavasta toivat mainehaittojen minimoinnin esille tietoturvan arvoa pohtiessa.

5.3.2 A2: Lisäävätkö organisaation tietoturvasertifikaatit asiakassuhteen solmimisen todennäköisyyttä?

Ainakin kirjallisuudesta huomataan, että myynnin kannalta kasvua tapahtuu etenkin sertifiointiprosessin aikana. Tätä pohdittiin muutamalta kannalta: joko asiakkaat vaativat sertifiointia yhteistyökumppanuuteen, tai sertifioinnista odotetut hyödyt näkyvät jo prosessin aikana. (Podrecca et.al 2022) On myös mahdollista, että sertifiointia seuraava mahdollinen positiivinen osakekurssin nousu (Deane et.al 2019) vaikuttaa positiivisesti organisaation imagoon, ja siten on houkuttelevampi yhteistyökumppani. Haastateltavista H1, H2, ja H3 toivat esille joidenkin asiakkaiden vaativan sertifiointia, jotta yhteistyö voitaisiin aloittaa. H1 korostaa tässä tapauksessa myös asiakkaiden kasvanutta tietoisuutta tietoturvasta: *” Asiakkaat eivät enää oleta, että tietoturva-asiat ovat kunnossa. Usein heillä on tarkat omat kriteeristöt ja mittaristot, jotka toimittajalla on oltava kunnossa. Tässä tapauskessa usein esimerkiksi sertifikaatti edesauttaa tässä asiakassuhteen solmimista.”*(H1). Saman organisaation toinen haastateltava kommentoi sa-

maa aihetta: *”Sertifikaattia (ISO 27001) voidaan käyttää ainakin markkinoinnissa, mutta tietoturva menee kuitenkin vaan tiettyyn tasoon asti, ei ole pelkästään ainoana myyntivalttina. Tuote ratkaisee loppuviimeksi.”* (H2). Julkisella sektorilla sertifioinnilla näyttäisi olevan pienempi merkitys: *”Jos katsoo valtion puolesta, valtionhallinta ja lait antaa kriteerit ja raamit tietoturvatasolle. Perusfundamentaalit tulee laista ja tiedonhallintalautakunta antaa suosituksia, joita tulee ottaa huomioon. Ei niinkään katsota sertifikaatteja.” (H4).*

Näyttäisi siltä, että tietoturvasertifioinnilla mahdollistetaan ainakin joitakin asiakkuuksia, jotka asettavat sen vaatimukseksi. Tietoturvasertifiointi voidaan siis nähdä yhtenä tekijänä, joka kasvattaa asiakassuhteen solmimisen todennäköisyyttä. Sertifikaatit toimivat luottamuksen signaalina, joka vakuuttaa potentiaaliset asiakkaat organisaation sitoutumisesta jatkuvaan kehitykseen ja arviointiin tietoturvan osalta.

5.3.3 P: Ovatko tietoturvasertifioidut organisaatiot arvokkaampia asiakkaille?

Tietoturvasertifioidut organisaatiot lisäävät omaa potentiaalista arvoaan usealla eri tasolla. Sertifioinnit voivat lisätä organisaation taloudellista suorituskykyä tuottavuuden, kannattavuuden ja myynnin osalta (Podrecca et.al 2022), parantaa markkinoiden ja sijoittajien näkemyksiä yrityksestä (Deane et.al 2019), sekä lisätä asiakasluottamusta.

Tietoturvasertifikaatit, kuten ISO 27001, ovat tärkeitä indikaattoreita organisaation kyvystä hallita tietoturvauhkia ja suojata asiakastietoja. Asiakkaille tämä merkitsee luottamuksen rakentumista, sillä sertifiointi todistaa organisaation sitoutuneen tietoturvan ylläpitämiseen ja jatkuvaan parantamiseen. Tämä on erityisen arvokasta aikana, jolloin tietoturvaloukkaukset yleistyvät mediassa, ja asiakkaat ovat yhä tietoisempia tietoturvauhkista. Lisäksi sertifiointi voi toimia kilpailuetuna, kun asiakkaat vertailevat tarjolla olevia palveluntarjoajia. Jotkut asiakkaat vaativat suoraan sertifiointia, joka suoraan sulkee pois osan kilpailijoista. Toiset asiakkaat taas esittävät listan tietoturvavaatimuksista, joka on usein kuitattavissa, tai ainakin helposti vastattavissa, mikäli organisaatio on suorittanut vaikkapa ISO 27001 sertifikaatin.

Haastattelut ja tutkimukset tukevat näkemystä, että tietoturvasertifiointi on investointi, joka voi tuottaa lisäarvoa niin organisaatiolle itselleen kuin sen asiakkaille. Asiakkaat arvostavat yhä enemmän tietoturvan korkeaa tasoa, joten palvelun käytön aikana myös koettu käyttöarvo voi olla korkeampi, mikäli tietoturvataso on korkea.

Voidaankin todeta, että tietoturvasertifioidut organisaatiot ovat arvokkaampia asiakkaille, sillä ne tarjoavat lisäturvaa, luottamusta ja vahvistavat asiakassuhteita. Sertifiointi

heijastaa organisaation sitoutumista parhaisiin tietoturvakäytäntöihin ja osoittaa potentiaalisille asiakkaille, että organisaatio ottaa tietoturvan vakavasti. Tämä sitoutuminen voi johtaa parempaan asiakastyytyväisyyteen, vahvempiin asiakassuhteisiin ja lopulta organisaation arvon kasvuun.

6. YHTEENVETO

6.1 Päätelmät

Katsaus tietoturvan roolista potentiaalisena arvonluojana korostaa ISO 27001 -sertifioinnin merkittävää panosta sekä organisaation taloudelliseen suorituskykyyn että sen markkina-arvoon. Tutkimukset osoittavat, että sertifiointiin liittyvät ilmoitukset tuottavat keskimäärin positiivisia epänormaaleja tuottoja, mikä viittaa siihen, että markkinat tunnistavat ja arvostavat tietoturvaan tehtyjä investointeja. Lisäksi sertifiointi näyttäisi tuovan sisäisiä hyötyjä organisaatioille, parantaen niiden kannattavuutta, tehokkuutta ja myyntiä pitkällä aikavälillä.

Tämän lisäksi haastatteluaineisto tukee näkemystä, että tietoturva on strateginen voimavara, joka tukee liiketoimintatavoitteita ja edistää asiakkaiden kokemaa luottamusta. ISO 27001 -sertifioinnin havaittiin myös lisäävän asiakassuhteen solmimisen todennäköisyyttä, toimien luottamuksen signaalina ja mahdollistaen ainakin jonkin tason kilpailuetua markkinoilla.

Näiden havaintojen perusteella voidaan päätellä, että ISO 27001 -sertifiointi on merkittävä investointi organisaatioille, jotka pyrkivät parantamaan tietoturvaa ja samalla kasvattamaan potentiaalista arvoaan. Sertifiointi ei ainoastaan vahvista organisaation tietoturvakäytäntöjä, vaan myös luo perustan jatkuvalle parantamiselle ja innovaatiolle tietoturvan hallinnassa. Lisäksi se rakentaa luottamusta asiakkaiden ja sijoittajien keskuudessa, mikä on erityisen tärkeää nykyhetkessä, jolloin tietoturvauhat ovat yhä kasvava huolenaihe.

Kokonaisuudessaan tutkimustulokset ja haastattelut osoittavat, että tietoturvasertifioinnilla on keskeinen rooli organisaation potentiaalisen arvon kasvattamisessa. Se ei ainoastaan paranna organisaation tietoturvaa, vaan myös edistää sen strategisia tavoitteita ja parantaa kilpailuasemaa. Tämän vuoksi organisaatioiden tulisi pitää ISO 27001 -sertifiointia mahdollisuutena vahvistaa liiketoimintansa perustaa ja rakentaa kestävämpiä asiakassuhteita tietoturvan avulla.

6.2 Työn arviointi ja mahdolliset jatkotutkimukset

Tämän kandidaatintyön lähestymistapa arvonluontiin tietoturvan kontekstissa on tieteen näkökulmasta melko rajallisesti tutkittu aihepiiri. Työssä yhdistettiin teoreettinen viitekehys ja empiirinen aineisto tavalla, joka valaisee tietoturvan roolia arvonluonnissa organisaatioille. Rajallisen kirjallisuusmateriaaliin pohjustuva kirjallisuuskatsaus yhdistettiin lopulta asiantuntijahaastatteluihin, mikä antaa monipuolisemman näkemyksen tutkittavasta aiheesta.

Työssä olisi voinut käsitellä tarkemmin tutkimusmenetelmien rajoitteita ja niiden mahdollista vaikutusta tulosten tulkintaan, lisäksi prosessi ei välttämättä ollut kovinkaan hyvin kuvattu. Lisäksi, vaikka haastattelut tarjoavat arvokasta tietoa, niiden rajoitettu määrä ja valikoima saattavat vaikuttaa tulosten yleistettävyyteen. Tietoturvan asiantuntijoita haastatellessa esiin saattaa tulla vinoumia oman työn merkityksellisyyden ja arvon kannalta. Tulevaisuudessa voisi olla hyödyllistä laajentaa tutkimuksen otantaa ja harkita kvantitatiivisen aineiston lisäämistä tasapainottamaan tuloksia. Haastatteluun voisi ottaa esimerkiksi useampia operatiivisia johtajia, jotka eivät niinkään työskentele tietoturvan kanssa päivittäin.

Toisaalta työ tarjoaa oivalluksia organisaatioille, jotka pyrkivät hyödyntämään tietoturvaa strategisena välineenä arvonluonnissa. Tämän työn tulokset korostavat tietoturvasertifikaattien merkitystä ja niiden vaikutusta organisaation arvoon sekä asiakassuhteisiin, mikä on erittäin relevanttia nykyisessä liiketoimintaympäristössä. Jatkotutkimukset voisivat keskittyä syvemmin tietoturvan eri näkökulmien vaikutuksiin arvonluonnissa ja tutkia käytännönläheisemmin, miten erilaiset organisaatiot voivat hyödyntää tietoturvaa kilpailuedun saavuttamiseksi.

LÄHTEET

Deane, J.K., Goldberg, D.M., Rakes, T.R. & Rees, L.P., 2019. The effect of information security certification announcements on the market value of the firm. Information Technology Management, 20, ss.107–121.

Fink, A., 2014. Conducting research literature reviews: from the Internet to paper. 4th ed. Thousand Oaks, CA: Sage.

Georgios, S. & Lefteris, A., 2016. The impact of information security events on the stock market: A systematic literature review. Computer Security, 58, ss.216–229.

Grönroos, C., 2011. Value co-creation in service logic: A critical analysis. Marketing Theory, 11(3). https://doi.org/10.1177/1470593111408177

Grönroos, C. & Voima, P., 2013. Critical Service Logic: making sense of value creation and co-creation. Journal of the Academy of Marketing Science, 41, ss.133-150.

Haksever, C., Chaganti, R. & Cook, R., 2004. A Model of Value Creation: Strategic View. Journal of Business Ethics, 49, ss.291–305.

Hirsijärvi, S. & Hurme, H., 2008. Tutkimushaastattelu - Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

International Federation of Accountants (IFAC), 2020. Understanding Value Creation. New York: International Federation of Accountants.

International Organization for Standardization (ISO), 2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto (ISO/IEC 27001:2020). [Standardi]. Geneva: International Organization for Standardization.

ISO, 2022. "ISO/IEC 27001 and related standards". Saatavilla: https://www.iso.org/isoiec-27001-information-security.html [Luettu 13.11.2022].

Julkaisufoorumi, 2023. Julkaisukanavahaku. Saatavilla: https://www.tsv.fi/julkaisufoorumi/haku.php [Luettu 29.1.2022].

Koskela-Huotari, K., 2021. Arvo, arvonluonti ja arvolupaukset. Saatavilla: https://www.oulu.fi/sites/default/files/events/ModuServ%20ty%C3%B6paja_011012.pdf [Luettu 29.1.2022].

Kyberturvallisuuskeskus, 2018. Kyberturvallisuuden Sanasto. Helsinki: Sanastokeskus TSK ry.

Lundgren, B. & Möller, N., 2017. Defining Information Security. Science and Engineering Ethics, 25, ss.419–441.

Safi, R., Browne, G.J. & Jalali Naini, A., 2021. Mis-spending on information security.

Vargo, S.L. & Lusch, R.F., 2004. Evolving to a New Dominant Logic for Marketing. Journal of Marketing, 68(1), ss.1–17.

Vargo, S.L. & Lusch, R.F., 2007. Service dominant logic: continuing the evolution. Journal of the Academy of Marketing Science, 36, ss.1–10.

Vargo, S.L., Maglio, P.P. & Akaka, M.A., 2008. On value and value co-creation: A service systems and service logic perspective. European Management Journal, 26, ss.145–152.

Walter, A., Ritter, T. & Gemünden, H.G., 2001. Value Creation in Buyer-Seller Relationships: Theoretical Considerations and Empirical Results from a Supplier's Perspective. Industrial Marketing Management, 30, ss.365–377.

Whitman, M.E. & Mattord, H.J., 2016. Management of Information Security. 6th ed. Boston: Cengage Learning.