TURVALLISEN DIGITALISAATION TYÖKALUPAKKI YRITYSJOHTAJALLE

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa. Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Julkaisija:
Huoltovarmuusorganisaatio.
Huoltovarmuusorganisaatio on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit.

Tämä dokumentti perustuu työhön ja tuotoksiin, jotka tehtiin Digipoolin #Strategia22 projektissa.

Julkaisija: Huoltovarmuuskeskus
Kuvat: GettyImages ja Colourbox
Taitto: LM Someco Oy
Julkaisuvuosi: 2022
ISBN: 978-952-7470-17-6

Sisältö

TURVALLISEN DIGITALISAATION TYÖKALUPAKKI YRITYSJOHTAJALLE

Nykyään liki jokainen organisaatio on keskeisiltä toiminnoiltaan digifirma, koska perustoiminnot ovat digitaalisten ratkaisujen varassa. Yrityksen liiketoiminnan strategiassa onkin huomioitava digitaalinen turvallisuus, jotta yritys kykenee toteuttamaan strategiaa tehokkaasti ja hallitsemaan siihen liittyvät riskit. Digitaalisten ratkaisujen turvallisuuden on oltava yksi ylimmän johdon keskeisistä tavoitteista – johto on vastuussa yrityksen liiketoiminnasta, arvon tuotosta ja näiden turvaamisesta. Tämä opas kertoo, miten digitaalinen turvallisuus huomioidaan yrityksessä niin, että se edesauttaa liiketoimintastrategian toteutusta.

Digitaalisen turvallisuuden eli kyberturvallisuuden kehittämisessä ja toteutuksessa keskeistä on, että kokonaisuutta johdetaan keskitetysti ja johdonmukaisesti kattaen koko organisaation – digitaalinen turvallisuus on sulautettava koko yrityksen toimintaan: jokaisen liiketoimintayksikön on tunnistettava omat vastuunsa yrityksen digitaalisessa ympäristössä ja osallistuttava oman toiminnan digiturvalliseen toteutukseen. Tämän edellytyksen toteutuminen on ylimmän johdon vastuulla. Suomessa osakeyhtiölakiinkin 2006/624 § 8 on kirjattu: “Yhtiön johdon on huolellisesti toimien edistettävä yhtiön etua.” Lisäksi tietosuojan näkökulmasta yritysten toimintaa sääntelee Euroopan unionin yleinen tietosuoja-asetus GDPR, joka mahdollistaa myös huomattavat sanktiot asetuksen säännösten rikkomisesta ja tietosuojavahinkojen korvaamiseksi. On myös huomioitava, että kasvavassa määrin yrityksiä koskee toimialakohtaiset kyberturvallisuuden lakisääteiset vaatimukset. Näistä yksi keskeisistä on EU:n verkko- ja tietoturvadirektiivi (NIS-direktiivi).

Kyberhyökkäykset näkyvät yhä enemmän julkisuudessa, mikä on korostanut kyberturvallisuuden merkitystä. Digitaalisen turvallisuuden toteutumiseksi kybersuojausten lisäksi yrityksen on huomioitava digitalisaatioratkaisuissa teknologiavalintojen merkitys turvallisuuden toteutumiselle: miten teknologioiden toimivuus tai toimimattomuus vaikuttaa yrityksen liiketoimintastrategian läpivientiin. Ymmärtäessään nämä tekijät yrityksellä on mahdollisuus kyberriskit halliten kasvattaa liiketoimintaa, lisätä sijoittajien luottamusta sekä tuottaa lisäarvoa ja kasvua omistajille. Johdonmukainen digitaalisen turvallisuuden hoitaminen tukee yrityksen maineen ja riskien hallintaa sekä oikein viestittynä lisää asiakkaiden arvostusta toimintaa kohtaan. Turvallinen digiympäristö on myös osoitus vastuullisesta valinnasta digitalisaation osalta.

Tämä Digipoolin työkalupakki on laadittu yritysjohtajille helpottamaan digi- ja kyberturvallisuuden kokonaisvaltaista johtamista yrityksen hallituksessa ja johtoryhmässä. Sisällön laadinnan lähtökohtana on ollut strategialla johtaminen ja yrityksen toiminnan jatkuvuuden turvaaminen.

Taustaa ja perusteluja

Kyberrikollisuuden määrä ja maailmanlaajuiset kustannukset nousevat nopeasti, mikä johtuu hyökkäysten toteutuskustannusten alenemisesta ja suojautumistarpeen lisääntymisestä. Digitaaliset laitteet ovat lisääntyneet merkittävästi, ja niitä käytetään entistä useammasta paikasta. Yritysten ydintoiminnot ovat yhä riippuvaisempia digitaalisista järjestelmistä.

Suomeen kohdistuu jatkuvasti kybervakoilua eikä se vähene pitkälläkään aikavälillä. Kybervakoilulla hankitaan esimerkiksi tuotekehitystietoa ja yritysten toiminnan kannalta kriittistä dataa. Suomessa tällaista tietoa urkitaan erityisesti yksityisistä yrityksistä mutta myös korkeakouluista ja tutkimuslaitoksista. Mitä enemmän yhteiskunta digitalisoituu, sitä suurempaa vahinkoa voidaan saada aikaan muuttamalla dataa tai estämällä siihen pääsy. Suurin kybervaikuttamisen uhka liittyy tällä hetkellä taloudellisesti motivoituneeseen kyberrikollisuuteen,[2] esimerkiksi lunnaiden saamiseen kiristyshaittaohjelmilla.

Yrityskentästä tehty havainto siitä, että strategiat eivät riittävästi edesauta digitalisaation turvallisuuden toteuttamista, paljastaa myös kaksi syytä tilanteeseen: 1) kyberturvallisuutta käsitellään teknologisena haasteena ja hallinnollisena työnä sekä 2) useimmat digi- ja kyberturvallisuusjohtajat eivät osallistu yrityksen strategiseen päätöksentekoon.

#STRATEGIA22-projektin puolesta

Digipooli

YRITYSJOHTAJAN TYÖKALUPAKIN PERUSTEET

Yrityksen johdolla on vastuu digitalisaation turvallisesta toteuttamisesta. Johdolla on oltava riittävä digitalisaatioriskien lukutaito. Kokonaisvaltainen tilanneymmärrys luo hyvät edellytykset johtamiselle ja oikea-aikaisille päätöksille. Yrityksen liiketoimintastrategiaan on kirjattava tavoitteet kyberturvallisuuden osalta ja yrityksen on toteutettava sitä toiminnassaan.

Strategia määrittää oikean resursoinnin tason eli ne panostukset, jotka yritys on kyberturvallisuuden varmistamiseksi valmis tekemään tai kääntäen, mitä riskejä yritys on valmis ottamaan. Digi- ja kyberjohtamiseen panostaminen maksaa itsensä takaisin mm. parempana kilpailukykynä ja henkilöstön työtyytyväisyytenä. Teknologialla voimme ratkaista alle puolet kasvavista digi- ja kyberturvallisuuden haasteista, merkittävämmän osan ratkaisee se, miten turvallisuutta johdetaan ja miten sitä arjessa toteutetaan. Teknologiavalinnoillakin on merkitystä ja ne on tehtävä huomioiden teknologioiden toimintakyky ja turvallisuus pitkällä aikajänteellä sekä arvioiden yrityksen oma kyky hyödyntää teknologioita.

Osana hyvää yritysjohtamisen tapaa yrityksen toiminnan ja arvontuotannon jatkuminen on varmistettava – niin osakkeenomistajien, muiden sidosryhmien kuin henkilöstönkin kannalta. Jatkuvuus- ja kriisisuunnitelmia on tehtävä varautuen kriittisimpiin liiketoimintoihin kohdistuviin uhkiin. Varautuminen edellyttää myös häiriötilanteissa toimimisen harjoittelua, jotta liiketoiminta pääsee tilanteiden jälkeen jatkumaan mahdollisimman tehokkaasti.

Vastuullinen työnantaja panostaa henkilöstönsä osaamiseen ja digitaitoihin, joita me kaikki tarvitsemme myös jokapäiväisessä elämässämme. Henkilöstön osaamiseen panostaminen on osa oikeaa resursointia, mutta myös osa yrityksen kulttuuria, jolla on valtava merkitys liiketoimintaan kohdistuvien kyberuhkien todennäköisyyden minimoinnissa.

Digitaalisen turvallisuuden johtamisen voi määritellä noudattaen strategisen johtamisen yleisiä periaatteita (kyberjohtamisen peruspilarit). Ne voidaan kiteyttää neljään osakokonaisuuteen, joille strateginen digijohtaminen on rakennettava, jotta digi- ja kyberturvallisuus tulee osaksi organisaation jokapäiväistä johtamista.

I. Johtaminen

1. Ylimmän johdon kokonaisvaltainen ja luotettava digi- ja kybertilanneymmärys
2. Kattava digitaalisen turvallisuuden ja kyberturvallisuuden riskienhallinta
3. Kyberturvallisuus osana liiketoimintastrategiaa ja sen toteutusta

II. Resursointi

4. Oikeasuhtainen digi- ja kyberturvallisuuden resursointi
5. Valittujen teknologioiden toimintakyky ja turvallisuus

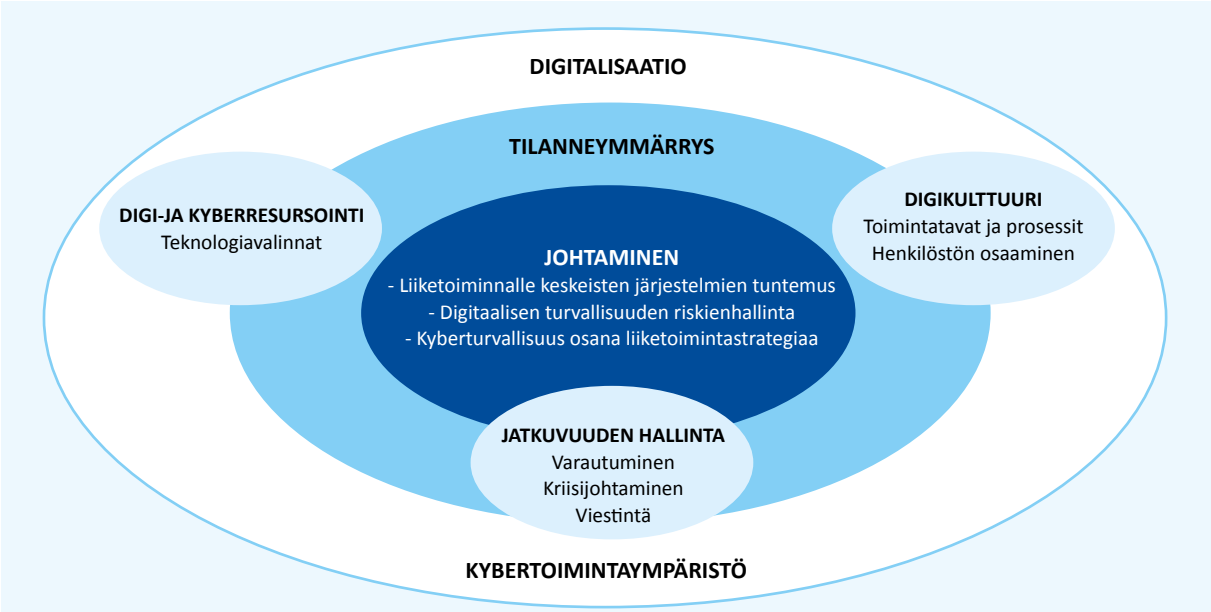
III. Jatkuvuuden hallinta

6. Digitaaliset poikkeamat huomioiva ajantasainen varautumis- ja kriisisuunnitelma
7. Suunniteltu ja harjoiteltu kriisijohtamismalli

IV. Digikulttuuri

8. Liiketoiminnan kehittämisen ja toimintaympäristön vaatimuksia vastaavat ydinprosessit ja toimintatavat
9. Kyberturvallisuuskulttuuri
10. Koko henkilöstön asianmukaiset digi- ja kybertaidot

Yrityksen johtoryhmän tehtävänä on tyypillisesti yhdessä toimitusjohtajan kanssa valmistella yhtiön strategia, liiketoimintasuunnitelmat, budjetti sekä muut hallituksen päätettävät asiat. Lisäksi johtoryhmä yleensä käsittelee yhtiön kannalta merkittävimmät operatiiviset asiat ja tekee päätökset niistä. Johtoryhmän tehtävät voidaan määritellä johtoryhmän työjärjestyksessä.



Kuva 1. Digitalisaation turvallisuuden johtamisen peruspilarit

Yrityksen strategia kertoo, kuinka yritys laajentaa markkinoitaan tai ylläpitää saavutettua markkinaosuutta ja kilpailuvalttejaan. Näihin keinoihin voivat kuulua kumppanit, tuote- ja palvelukehitys, mahdolliset yritysostot ja oma osaaminen. Yrityksen eri toimialoja ja liiketoimintoja on tarkasteltava ainakin myynnin ja markkinoinnin, viestinnän, taloushallinnon, tuotannon ja palveluiden, sidosryhmien ja asiakkuuksien, riskien ja jatkuvuudenhallinnan sekä kehittämisen näkökulmista. Liiketoiminnan laajentamisessa ja jatkuvuuden hallinnassa on keskeistä tunnistaa digitaalisen turvallisuuden merkitys strategian toteuttamisessa.

Toimitusjohtaja valitsee johtoryhmän jäsenet. Johtoryhmässä tulee olla digitaliseen turvallisuuteen liittyvää osaamista. Erikseen nimetyn digijohtajan tehtävä voi olla välivaihe, kunnes johtoryhmän jäsenillä on riittävä osaaminen. Koska kokonaisuus on johtoryhmän vastuulla, osaamisen perusteella on mahdollista jakaa vastuuta toiminnoittain tai liiketoiminta-alueittain. Kuvassa 2 on esimerkki malliksi vastuiden jakamisesta.

Kuva 2. Esimerkki johtoryhmän vastuuaiheiden jakautumisesta johtoryhmässä

KYBERTURVALLISUUDEN TYÖKALUPAKKI: TOP 10 -TOIMENPITEET

JOHTAMINEN

1. Ylimmän johdon kokonaisvaltainen ja luotettava digi- ja kybertilanneymmärrys

Operatiivinen johto vastaa siitä, että hallitukselle säännöllisesti ja ymmärrettävästi raportoidaan digi- ja kyberriskeistä, uhista ja seurannaisvaikutuksista.

Johto tuntee liiketoiminnan kannalta keskeiset digitaaliset järjestelmät ja ymmärtää mistä digitaalisista järjestelmistä liiketoimintaprosessit ovat riippuvaisia ja minkälaisia järjestelmiä tarvitaan, jotta yrityksen liiketoimintaa voidaan toteuttaa strategian mukaisesti.

2. Kattava digi- ja kyberriskianalyysi ja riskienhallintajärjestelmä

Hallitus varmistaa, että johto sisällyttää resilienssin ja kyberriskien arvioinnin liiketoimintastrategiaan ja yrityksen kokonaisriskienhallintaan sekä ottaa arvioinnin tuloksen ja resurssien kohdentamisessa syntyneen kehitysvelan huomioon budjetoinnissa.

3. Kyberjohtamisen konsepti osana liiketoimintastrategian toteutusta

Hallitus varmistaa, että yrityksen eri osat tekevät yhteistyötä arvioidakseen, ovatko ne havainneet samanlaisia uhkia koordinoidakseen reagointia tai toteuttaakseen yhteiset valvontatoimet riskin keskitetyksi käsittelemiseksi ja hallitsemiseksi. Hallitus määrittelee ja mittaa vuosittain liiketoiminnan riskinsietokyvyn suhteessa kyberresilienssiin ja varmistaa, että tämä on yrityksen strategian ja riskinottohalukkuuden mukainen.

RESURSOINTI

4. Oikeasuhtainen digi- ja kyberturvallisuuden resursointi

Digitaalisen turvallisuuden ja kyberturvallisuuden investointien hyödyt huomioidaan osana riskien hallintaa. Tunnistettujen riskien suojauksista lasketaan kustannusarviot. Suojaukseen investoidaan tai hyväksytään hallittu riski mahdollisen kyberuhan toteutumisen vaikutuksista liiketoimintaan.

5. Valittujen teknologioiden toimintakyky ja turvallisuus

Liiketoiminnan edellyttämät digitalisaation tavoitteet on määritetty yrityksen strategiassa (esim. digitalisaatioaste). Ennen tavoitteiden asettamista hallitus ja johtoryhmä käyvät läpi erilaiset kehitystä tukevat teknologiat ja järjestelmät sekä niiden kokonaiskustannusarviot. Kustannusarvioissa huomioidaan digitaalisen turvallisuuden ja kyberturvallisuuden toteutus osana investointia.

JATKUVUUDEN HALLINTA

6. Ajantasaiset varautumisen sekä jatkuvuuden- ja kriisinhallinnan suunnitelmat

Hallitus ja toimiva johto vastaavat yrityksen varautumis- ja kriisienhallintasuunnitelmista sekä toimenpiteistä, joiden ajantasaisuudesta johto raportoi säännöllisesti yrityksen hallitukselle. Suunnitelmien tulee erikseen huomioida digitaalisten järjestelmien ja kyberpoikkeamien hallinta niihin liittyvien toimien erityispiirteiden vuoksi. Kyberhyökkäykset huomioidaan osana kriisiviestintäsuunnitelmaa.

7. Suunniteltu ja harjoiteltu kriisijohtamismalli

Hallituksen ja johtoryhmän jäsenet perehdytetään kyberturvallisuuteen heidän ottaessaan tehtävänsä vastaan. Ajankohtaisista uhkista ja suojaustoimenpiteistä tiedottamiseen on prosessi. Kriisijohtamismalli huomioi viestintätarpeet monipuolisesti. Avainhenkilöt osallistuvat suunnitelman mukaisiin harjoituksiin.

DIGIKULTTUURI

8. Vaatimuksiin vastaavat ydinprosessit ja toimintatavat

Ydinprosessit ja toimintatavat on johdettu strategiasta priorisoiden, ja ne vastaavat liiketoiminnan kehittämisen ja toimintaympäristön vaatimuksiin. Ydinprosessit ja toimintatavat toimitusketjuissa on varmistettu siten, että sopimukset vastaavat kunkin toimitusketjun kriittisyyttä.

9. Kyberturvallisuuskulttuuri

Hallitus ja johtoryhmä luovat edellytykset avoimelle kyberturvallisuuskulttuurille. Tietoturvallisia käytäntöjä arvostetaan ja niiden merkitys ymmärretään osana yrityksen turvallisuuden ja liiketoiminnan jatkuvuuden hallintaa.

10. Koko henkilöstön asianmukaiset digi- ja kybertaidot

Yrityksen tavoitteiden saavuttamiseen ja riskien hallitsemiseen tarvittavat taidot on määritelty. Yrityksen henkilöstö koulutetaan tietoturvataidoissa ja taitoja testataan säännöllisesti.

YRITYSJOHTAJAN TOIMENPIDEKORTIT

Kortti koostuu kahdesta osiosta, joista ensimmäisessä on aihealueeseen johdattelevia kysymyksiä ja toisessa listaus toimenpiteistä, joita yritysjohdon tulisi ainakin ottaa huomioon digitalisaation strategisessa johtamisessa ja ohjaamisessa.

Toimenpidekorttien laadinnassa on hyödynnetty World Economic Forumin julkaisua ”Advancing Cyber Resilience Principles and Tools for Boards”.

Kortti 1: Ylimmän johdon kokonaisvaltainen ja luotettava digi- ja kybertilanneymmärrys

Ohjaavat kysymykset

- Onko yrityksellä käytössä prosessi, jolla varmistetaan, että hallitus ja johtoryhmä saavat kattavat tiedot digitaalisesta turvallisuudesta päätöksenteon tueksi?
- Onko hallitus vastuuttanut yrityksestä oikeat henkilöt, jotta digi- ja kyberturvallisuutta ja sen edistymistä voidaan hallita digitalisaatiotavoitteiden mukaisesti?
- Miten digitalisaation turvallisuuden kehitystä seurataan ja ylläpidetään?
- Tunteeko ylin johto strategian tavoitteiden riippuvuudet digitaalisista ratkaisuista?

Tehtävälista, varmistettavat asiat

- **Liiketoiminnot on priorisoitu** (huomioiden tuki kriittiselle kansalliselle infrastruktuurille tai muille kansallisille eduille, joilla vastataan yhteiskunnan asettamiin vaatimuksiin).
- Ylin johto tuntee liiketoiminnan kannalta **keskeiset digitaaliset järjestelmä**t. Johto ymmärtää, miten tekniset järjestelmät, prosessit tai resurssit edistävät tavoitteiden saavuttamista sekä luovat kilpailuetua.
- Operatiivinen johto vastaa siitä, että hallitukselle raportoidaan ymmärrettävästi digi- ja kyberriskeistä, uhista ja seurannaisvaikutuksista. Raportti on pysyvä asialistakohta hallituksen kokouksissa.
- Yrityksellä on selkeä toimintamalli, miten tilannekuvan kolme eri tasoa saadaan tehokkaasti käyttöön (tasot: strateginen, riskien hallinta ja operatiivinen).
- Hallitukselle annetaan tarvittavat tiedot yrityksen ulkopuolisista näkökulmista (osakkeenomistajat, sääntely, asiakkaat ja muut yhteiskunnalliset toimijat), jotta hallitus voi suhteuttaa digi- ja kyberriskit ympäristöön.
- Digiturvallisuudesta ja kyberturvallisuudesta vastaavalla johtajalla on pääsy hallitukseen ja johtoryhmään, riittävä toimivalta, aiheen hallinta, kokemus ja resurssit tehtävien hoitamiseksi.
- Hallitus varmistaa, että organisaatiosta tehdään vuosittain virallinen riippumaton digi- ja kyberturvallisuuskatselmus.

Kortti 2: Kattava digi- ja kyberriskianalyysi ja riskienhallintajärjestelmä

Ohjaavat kysymykset

- Miten johto päättää, mitkä riskit hyväksytään ja mitkä suojataan?
- Saavatko hallituksen ja johtoryhmän jäsenet säännöllisen päivityksen liiketoiminnan digi- ja kyberkypsyydestä, kyberriskeistä ja keskeisten uhkien torjumiseksi toteutetuista suojaustoimenpiteistä?
- Onko digitalisaation ja kyberturvallisuuden raportointi hallitukselle tasoltaan oikea ja heijastaako se nykyistä ja mahdollista tulevaa tilannetta suhteessa strategiaan, sen toimeenpanoon ja liiketoimintaan?
- Miten hallitus ja johtoryhmä määrittelevät yrityksen resilienssiä koskevan strategian ja siihen liittyvät riskit/riskitasot?

Tehtävälista, varmistettavat asiat

- Yrityksellä on prosessi, jossa digitalisaatioon ja kyberturvallisuuteen liittyvien riskien arviointi on sidottu osaksi liiketoimintariskien arviointia.
- Riskiraportointi hallitukselle on tasoltaan oikea ja se tuottaa tietoa nykyisestä sekä tulevasta tilanteesta.
- Hallitus tunnistaa digi- ja kyberriskien todellisen vaikutuksen liiketoimintaan kuten liiketoiminnan häiriöt tai vaikutuksen tuotteen/palvelun laatuun tai yrityksen maineeseen.
- Yritys kykenee hallitsemaan muutokset, jotka digi- ja kyberturvallisuuden suunniteltuun liiketoimintaan, tai teknologiavalintoihin tehdään.
- Yrityksen toimintaa arvioidaan tai auditoidaan sisäisesti ja ulkoisesti.
- Yritys on sertifioitu kilpailuedun edistämiseksi ja vastuullisuuden osoittamiseksi.
- Yritys viestii riskeistä ja niiden seurauksista omalle henkilöstölleen ja sopimuskumppaneilleen.

Kortti 3: Kyberjohtamisen konsepti osana liiketoimintastrategian toteutusta

Ohjaavat kysymykset

- Tekevätkö yrityksen eri osat keskinäistä yhteistyötä (esim. muiden liiketoiminta-yksiköiden kanssa) arvioidakseen, ovatko ne havainneet samanlaisia uhkia ja koordinoidakseen reagointia tai toteuttaakseen yhteiset valvontatoimet riskin keskitetyksi käsittelemiseksi ja hallitsemiseksi?
- Onko hallitus tyytyväinen siihen, että yritys pystyy tehokkaasti hallitsemaan kyberturvallisuuden haavoittuvuuksia ja vaadittuja päivityksiä, joita voi tulla eteen liiketoiminnan tai suunniteltujen teknologiamuutosten seurauksena?

Tehtävälista, varmistettavat asiat

- Varmista, että (liiketoimintojen kehittämisen edellyttämien) uusien teknologia- ja järjestelmäinvestointien yhteydessä arvioidaan suunnitelmallisesti, miten kyberturvallisuus toteutetaan (esim. miten uusi toteutus sovitetaan järjestelmäarkkitehtuuriin ja ylläpidetään). Siten strategiaa toteutettaessa kyberturvallisuus ensisijaisesti tukee yrityksen liiketoimintaa ja turvallisuudesta tulee sisäänrakennettu osa päätöksentekoa.
- Tunnista ja huomioi toimintaympäristön muutosten vaikutukset omalle liiketoiminnalle ja turvallisuudelle.
- Käytä hyväksi havaittuja ja liiketoiminnan turvallisuutta edistäviä vakioituja ja standardoituja toimintatapoja.
- Valitse ja hallitse liiketoiminnan kehittämistä hyödyttäviä teknologioita perustellusti.
- Ota huomioon kyberturvallisuuden kattava rakentaminen, joka edellyttää toimenpiteitä yrityksen strategisella, operatiivisella ja teknillisellä/taktisella tasolla.

Kortti 4: Oikeasuhtainen digi- ja kyberturvallisuuden resursointi

Ohjaavat kysymykset

- Kuinka suuri osuus vuotuisista toiminta-menoista käytetään yrityksen jatkuvuuden hallintaan, ja miten tämä vertautuu itse-asetettuihin tavoitteisiin, alan normeihin tai toimialan keskiarvoon?
- Onko yrityksellä kohdennettua budjettia digitalisaatioon ja turvallisuuteen ja kuka/ketkä sen omistaa?
- Onko yrityksellä muita talousarvioita, jotka edistävät yrityksen liiketoiminnan ja turvallisuuden jatkuvuutta?

Tehtävälista, varmistettavat asiat

- Yrityksellä on digitalisen turvallisuuden vaikutukset huomioiva prosessi kokonaisbudjetin muodostamisessa.
- Hallituksella on kyky ymmärtää digi- ja kyberturvallisuusriskien vaikutuksia ja sitä, miten riskit voivat olla erilaisia suhteessa yrityksen tavoitteisiin riskien ja kyberturvallisuus-toimenpiteiden operatiivisten kustannusten/vaikutusten tasapainottamisessa.
- Mahdollisen kybervakuutuksen kustannukset on huomioitava.
- Digitalisaation ja digitaalisen turvallisuuden investointien hyödyt ovat suhteessa toisiinsa.

Kortti 5: Valittujen teknologioiden toimintakyky ja turvallisuus

Ohjaavat kysymykset

- Onko yrityksen strategiassa määritetty tavoitteet digi- ja kyberteknologian hyödyntämisestä liiketoiminnassa ja yrityksen hallinnossa?
- Onko yrityksellä käytössä prosessi digitaalisten järjestelmien resilienssin arvioimiseksi sellaisten kolmansien osapuolten kanssa, jotka voivat hallita tieto- tai teknologiaresursseja?

Tehtävälista, varmistettavat asiat

- Digitalisaation tavoitteet on määritetty (esim. yrityksen digitalisaatioaste). Ennen tavoitteiden asettamista on käyty läpi erilaiset teknologiat, niiden mahdollisuudet ja käyttöön liittyvät kyberuhat ja muut riskit (esim. alustapalvelut, pilvipalvelut, tekoäly, 5G, teollinen internet jne.).
- Digitalisaation kohteena olevat liiketoimintaprosessit, hallinnolliset prosessit sekä tuotteet ja palvelut on määritetty.
- Yrityksessä on määritetty tietoteknisen ympäristön osat, jotka ovat kriittisiä liiketoiminta-tavoitteiden saavuttamiseksi.
- Yrityksessä on suunnitelma teknologioiden käyttämisestä toiminnan kehittämisessä ja teknologioiden käyttöönotosta.
- Varmistettu, että valittu teknologia tukee liiketoiminnan kehitystä digi- ja kyberturvallisesti.
- Laadittu edellä mainittua määritystä vastaavat turvallisuus- ja kumppanuussopimukset.
- Ohjaavat prosessit tuottavat yritykselle strategian, riskienhallinnan, toimintaympäristö-analyysin ja resurssit sekä toteuttavat muutosten hallintaa.
- Hallinnolliset prosessit tukevat yrityksen päätöksentekoa ja viestintää muita prosesseja korkeammalla tasolla.

Kortti 6: Ajantasaiset varautumisen, jatkuvuuden- ja kriisinhallinnan suunnitelmat

Ohjaavat kysymykset

- Onko yrityksellä käytössä liiketoiminnan jatkuvuussuunnitelmat ja toipumissuunnitelmat sisältäen viestinnän, tietoturvaiskujen torjunnan ja häiriöiden torjunnan?
- Miten digitaaliset järjestelmät (esim. tekniset ratkaisut) on suojattu?
- Miten turvallisuus (esim. auditointi, tunkeutumistestaus) on todennettu?

Tehtävälista, varmistettavat asiat

- Vastuu suunnitelmista on yrityksen johtoryhmällä.
- Hallitus varmistaa, että johto tukee sietokyvystä tai digi- ja kyberturvallisuudesta vastaavaa johtajaa laatimalla, toteuttamalla, testaamalla ja parantamalla jatkuvasti toipumissuunnitelmia.
- Suunnitelmien on oltava yhdenmukaisia kaikilla yrityksen liiketoiminta-alueilla, jotka edellyttävät suorituskyvyn säännöllistä seurantaa ja raportointia hallitukselle.
- Suunnitelmiin sisältyy riittävä ja monipuolinen johdon edustus sen varmistamiseksi, että keskeiset näkökulmat ja tarpeet otetaan huomioon (esim. laki, myynti ja markkinointi, mediasuhteet, hallitussuhteet, sijoittajasuhteet, toimitilojen hallinta, yritysturvallisuus jne.).
- On nimetty henkilö, joka tuntee lakien vaatimukset eri lainkäyttöalueilla, joilla yritys toimii, ja sen miten nämä vaatimukset sisällytetään suunnitelmiin.
- Suunnitelmat huomioivat digitaalisesti riippuvaisiin liiketoimintoihin kohdistuvat mahdolliset poikkeamat uhat.

Kortti 7: Suunniteltu ja harjoiteltu kriisijohtamismalli

Ohjaavat kysymykset

- Saavatko hallituksen tai johtoryhmän jäsenet riittävän perehdytyskoulutuksen digitalisaatioon ja kyberturvallisuuteen ottaessaan vastaan uuden tehtävän?
- Onko yrityksellä säännöllinen koulutus- ja harjoitusohjelma, jolla heidän tietonsa ja taitonsa viimeisimmistä turvallisuus-tapahtumista päivitetään?
- Viestiikö johto hallitukselle mahdollisista fyysisistä, toiminnallisista, ihmisiin liittyvistä, oikeudellisista ja/tai mainehaitoista, jotka voivat seurata kybertapahtumasta?
- Tiedottaako johto hallitukselle nykyisistä toimialakohtaisista uhkista/uhkamalleista/suuntauksista/toimenpiteistä, mukaan lukien kolmansiin osapuoliin (esim. toimittajiin) liittyvät riskit?
- Miten julkisia sisältöjä hallitaan niin, että ne eivät luo uhkia yrityksen suuntaan?

Tehtävälista, varmistettavat asiat

- Yrityksen toimintamalli ja tehtävät ovat hallituksen hyväksymät.
- Kriisinjohtamisorganisaatio on koulutettu ja säännöllisesti harjoitettu, koulutuksen ja harjoittelun painopiste on määritelty esimerkiksi riskianalyysin perusteella.
- Organisaatiolla on jatkokoulutus- ja harjoitussuunnitelma.
- Yritys harjoittelee aktiivista tiedonjakoa niin teknisesti kuin hallinnollisesti. Harjoitukset sisältävät tekniset ensitoimet, poikkeamasta ilmoittamisen, henkilöstön ohjeistamisen ja ulkoisen viestinnän.
- Toiminta on budjetoitu.
- Yrityksessä on viestitty selkeästi organisaation tärkeimmistä tavoitteista ja varmistettu, että nämä prioriteetit ohjaavat myös digi- ja kyberturvallisuustoimenpiteitä.
- Yrityksellä on sisäisen ja ulkoisen viestinnän suunnitelma, joka kattaa erilaiset kriisi-tilanteet.
- Viestinnän roolit on nimetty ja tehtävien hoitajat harjoitettu.
- Yrityksen viestintä eri kanavissa on säännöllistä.
- Maineenhallinta on huomioitu viestintäsuunnitelmassa.

Kortti 8: Vaatimuksiin vastaavat ydinprosessit ja toimintatavat

Ohjaavat kysymykset

- Onko yrityksellä käytössä liiketoiminnan kehittämiseen prosessit ja toimintatavat, joilla voidaan tunnistaa myös tieto- ja teknologiaresursseja?
- Onko yrityksen liiketoiminnan ja yrityksen hallinnon ydinprosessit määritetty ja priorisoitu?
- Onko keskeiset yhteistyötahot/ulkoistukset/alihankkijat/sopimustahot tunnistettu?
- Mitä ulkoistussopimuksissa on sovittu tieto-turvasta, jatkuvuudenhallinnasta, turvalli-suussopimuksista?
- Vastaavatko toimitusketjun sopimusten turvallisuusvaatimukset toiminnon kriitti-syyttä liiketoiminnalle?
- Miten asiakastietoja hallitaan oman maineen ja asiakkaan/sidosryhmän kannalta?

Tehtävälista, varmistettavat asiat

- Yrityksen liiketoiminnalliset tavoitteet ohjaavat liiketoimintaprosessin toimintoja.
- Toimintojen alihankintasopimusten on turvallisuuden osalta varmistettu vastaavan toiminnon kriittisyyttä organisaatiolle.
- Operationaaliset prosessit ovat kehitetty turvallisiksi asiakkaille tehtävien tuotteiden ja palveluiden toteuttamiseksi.
- Tukiprosessit mahdollistavat operationaaliset prosessit, esimerkiksi henkilöstöresurssien, järjestelmien tai kirjanpidon avulla.
- Yritys- ja liiketoimintaostot ja niihin liittyvät kyberriskit ovat hallinnassa. (Cyber Due Diligence merkittävissä tapauksissa, jos dataa ja/tai järjestelmiä siirtyy oston mukana.)

Kortti 9: Kyberkulttuuri

Ohjaavat kysymykset

- Onko varmistettu, että työntekijät kokevat voivansa vaikuttaa yrityksen digitalisaatioon ja kyberturvallisuuteen, ja että heillä on mahdollisuus tuoda esiin näihin liittyviä epäkohtia?
- Ovatko hallituksen ja johtoryhmän jäsenet sitoutuneet digi- ja kyberturvallisuutta koskeviin päätöksiin, noudattavatko he itse niitä ja tuovatko he esiin tehottomia käytäntöjä yhteistyössä työntekijöiden kanssa?
- Onko varmistettu, että organisaatiossa puhutaan avoimesti ja myönteisesti henkilöstölle siitä, miksi digi- ja kyberturvallisuus on tärkeää?

Tehtävälista, varmistettavat asiat

- Hallituksen ja johtoryhmän tehtäviin kuuluu kyberturvallisuuskulttuurin luominen ja kehittäminen.
- Kyberkulttuuri koostuu digitalisaatioon liitetyistä toimintatavoista, työmoraalista, yhteisistä säännöistä ja ehdoista sekä työntekijöiden välisistä vuorovaikutustavoista.
- Digitalisaation ja kyberturvallisuuden tuomat muutokset on käsitelty hyvässä hengessä, mukaan lukien yhteiset tavoitteet, työtehtävät ja vastuualueet sekä pelisäännöt ja toimintatavat.
- Yrityksen henkilöstö tietää, miten ja kenelle epäkohdista tai poikkeamista voi raportoida. He kokevat, että heitä kannustetaan raportointiin, eivätkä he pelkää negatiivisia seurauksia raportoidessaan epäkohdista tai poikkeamista.
- Turvallisuuspoikkeamien raportointiin kannustetaan nopean reagoinnin mahdollistamiseksi.
- Henkilöstö kokee voivansa kyseenalaistaa toimintamalleja rakentavalla tavalla ja pääsevänsä hyödyntämään kykyjään, taitojaan ja luovuuttaan.
- Henkilöstön näkemyksiä hyödynnetään aidosti digi- ja kyberturvallisuuskäytäntöjen suunnittelussa ja muutoksessa.
- Henkilöstö ymmärtää digi- ja kyberturvallisuuden tärkeyden ja merkityksen organisaatiolle. Yrityksessä otetaan huomioon oppiva ja kehittyvä työyhteisö, kannustetaan aktiivisuuteen ja sujuvaan yhteistyöhön.
- Epäonnistumisten sijaan raportoinnissa ja sisäisessä viestinnässä keskitytään onnistumisiin (kerrotaan esimerkiksi moniko raportoi tietojenkalastelusähköposteista eikä sitä moniko lankesi niihin).
- Annetaan aikaa sosiaaliselle kanssakäymiselle.

Kortti 10: Koko henkilöstön asianmukaiset digi- ja kybertaidot

Ohjaavat kysymykset

- Saavatko yrityksen uudet työntekijät riittävän perehdytyskoulutuksen yrityksen digitalisiin järjestelmiin ja digitaaliseen turvallisuuteen?
- Onko yrityksellä säännöllinen koulutus- ja harjoitusohjelma, jolla henkilöstön tietoja ja taitoja päivitetään viimeaikaisista uhkista ja suuntauksista (tilanneymmärryksen kehittyminen)?

Tehtävälista, varmistettavat asiat

- Yrityksen tavoitteiden saavuttamiseen ja riskien hallitsemiseen tarvittavat taidot on määritelty.
- Työtehtävien vaatimat valmiudet ja osaamistasot on määritelty koulutussuunnittelun pohjaksi.
- Työntekijöille on koulutettu oman työtehtävän mukainen osaaminen yrityksen digitaalisten järjestelmien sietokyvystä.
- Koulutusohjelma varmistaa säännöllisen tietojen ja taitojen ylläpidon ottaen huomioon muuttuvan toimintaympäristön asettamat vaatimukset.
- Koulutusohjelma sisältää yrityksen jatkuvuuden toimintamallit sekä teknologioiden käytön ja poikkeustilanteiden toimintamallit.
- Osaaminen mitataan, testataan tai arvioidaan muutoin säännöllisesti, esimerkiksi harjoituksilla.

Liite 1:

KÄSITTEET

1. Digitalisaatio, kyberturvallisuus

Digitalisaatiossa tietoa ja tietotekniikkaa hyödynnetään toiminnan muuttamiseen tai uuden mahdollistamiseen. Esimerkiksi, kun verovelvollisen täyttämä veroilmoitus korvattiin veroviranomaisen kokoamalla veroehdotuksella, kyse oli digitalisaatiosta.

Kyberturvallisuus on tiedon, laitteistojen, verkostojen, ohjelmistojen ja käyttäjien luottamuksellisuuden, eheyden ja saatavuuden turvaamista, joka on ylläpitäjien ja käyttäjien yhteistoimintaa.

Esimerkiksi tärkeiden dokumenttien säilyttäminen kassakaapissa on tietoturvaa, kun taas näiden tärkeiden dokumenttien säilyttämisen tietokoneella on kyberturvaa (ja samalla tietoturvaa).

2. Tilannekuva ja -ymmärrys

Yrityksen toimintaympäristötietoisuus ja toimintaympäristön ymmärtäminen ovat edellytyksiä oikea-aikaisille johtamistoimenpiteille, joilla turvataan liiketoiminnan menestys myös kybertoimintaympäristön muuttuessa. Liiketoiminnan suunnittelua ja toimeenpanoa varten voidaan muodostaa kybertilannekuva, jonka sisältö ja tarve vaihtelevat suuresti eri johtamistasojen ja toimijoiden välillä, joten ei ole mahdollista määritellä yksiselitteistä kaikkiin tilanteisiin ja kaikkien kokoluokkien yrityksille sopivaa kybertilannekuvaa.

Kybertilannekuva ei muodostu ainoastaan teknisestä tilannekuvasta. Parhaimmillaan kybertilannekuvassa on kyetty onnistuneesti yhdistämään teknisten tietojen lisäksi uhkatiedot ja yleinen tilanne. Tärkeimpänä elementtinä toimii kuitenkin ihminen, joka kykenee koostamaan tiedoista selkeän kokonaisuuden ja tekemään siitä järkeviä johtopäätöksiä.

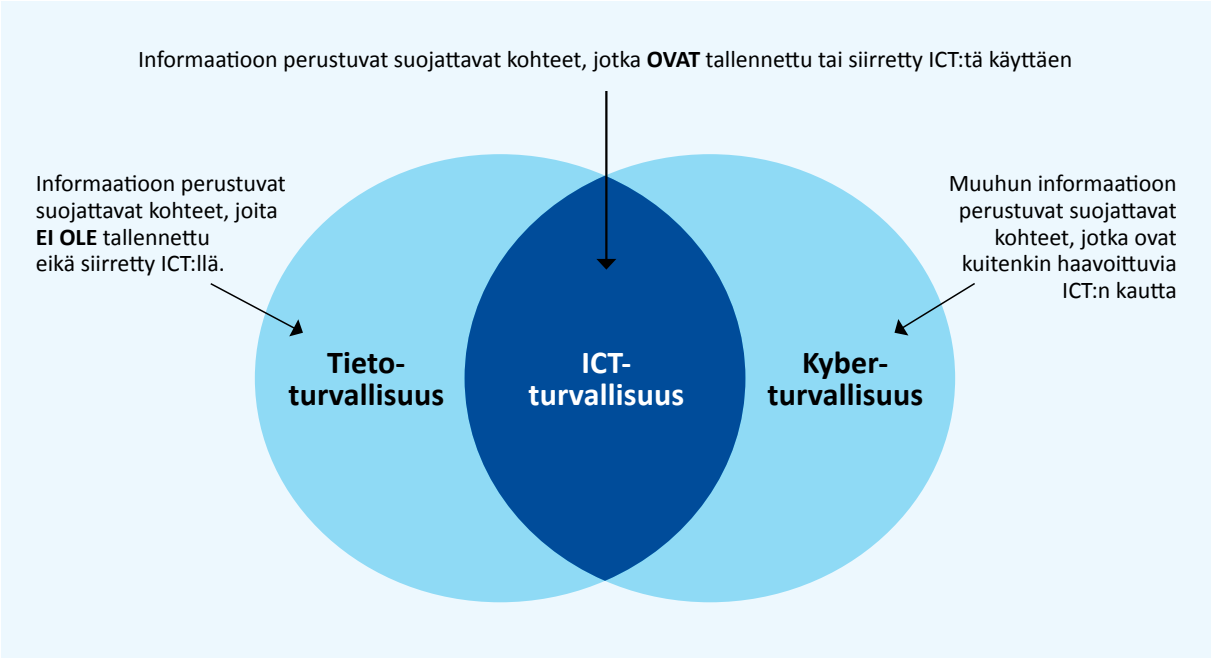
Tilannekuvatasot, tilannekuvan merkitys

1. Strateginen tilannekuva
   Mahdollistaa yritysjohdon tilannetietoisuuden kasvattamisen ja ylläpitämisen.

2. Digitaalisten ja kyberriskien tilannekuva
   Mahdollistaa riskiperustaisen päätöksenteon ja johtamisen. Antaa perusteet jatkuvuuden suunnittelulle ja liiketoiminnan jatkuvuudelle.

3. Operatiivinen tilannekuva
   Päivittäis- ja kriisijohtamisen perusta.

Tilannekuvalähteitä: Kaupalliset analyysi- ja kuvapalvelut, ICT-palvelukumppanien verkostot, omat sensoriverkot, Kyberturvallisuuskeskuksen tilannekuvapalvelut ja SOC-palvelut



Kuva: Tietoturvallisuuden, ICT-turvallisuuden ja kyberturvallisuuden määrittely

Kybertoimintaympäristö

Yrityksen kybertoimintaympäristö on alati muuttuva. Toimintaympäristö voidaan tyypittää kolmella eri tavalla:

- turbulentti ympäristö, jossa muutoksien lukumäärä on suuri ja ennustettavuus on heikko, tilanne on kaoottinen

- dynaaminen ympäristö, jossa esiintyy lukumääräisesti paljon muutoksia, mutta muutokset ovat enemmän tai vähemmän ennustettavissa aikaisempien tapahtumien ja kokemusten perusteella

- vakaa ympäristö, jossa muutoksia on vain muutamia, ja ne voidaan ennustaa aikaisempien kokemuksien perusteella.

3. Johtaminen

Kyberturvallisuuden strateginen johtaminen

Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista[8]. Alla olevassa kuvassa on esitetty kyberturvallisuuden johtamisen yleinen periaate.

Hallituksen vastuu

Osakeyhtiölain mukaisesti hallitus huolehtii yhtiön hallinnosta ja toiminnan asianmukaisesta järjestämisestä (yleistoimivalta). Osana hyvää hallintoa hallitus vastaa digitalisaatioon liittyvästä digi- kybersietokyvyn valvonnasta. Hallitus voi siirtää ensisijaista valvontatoimintaa olemassa olevalle valiokunnalle (esim. tarkastus- tai riskivaliokunnalle). Hallituksen on arvioitava, onko nykyisillä hallituksen jäsenillä tarvittavat tiedot, taidot ja kokemus digitalisaation tehokkaaseen johtamiseen ja valvontaan sekä edellyttävätkö tietopuutteet uusien jäsenten valintaa hallitukseen.

Toimitusjohtajan vastuu

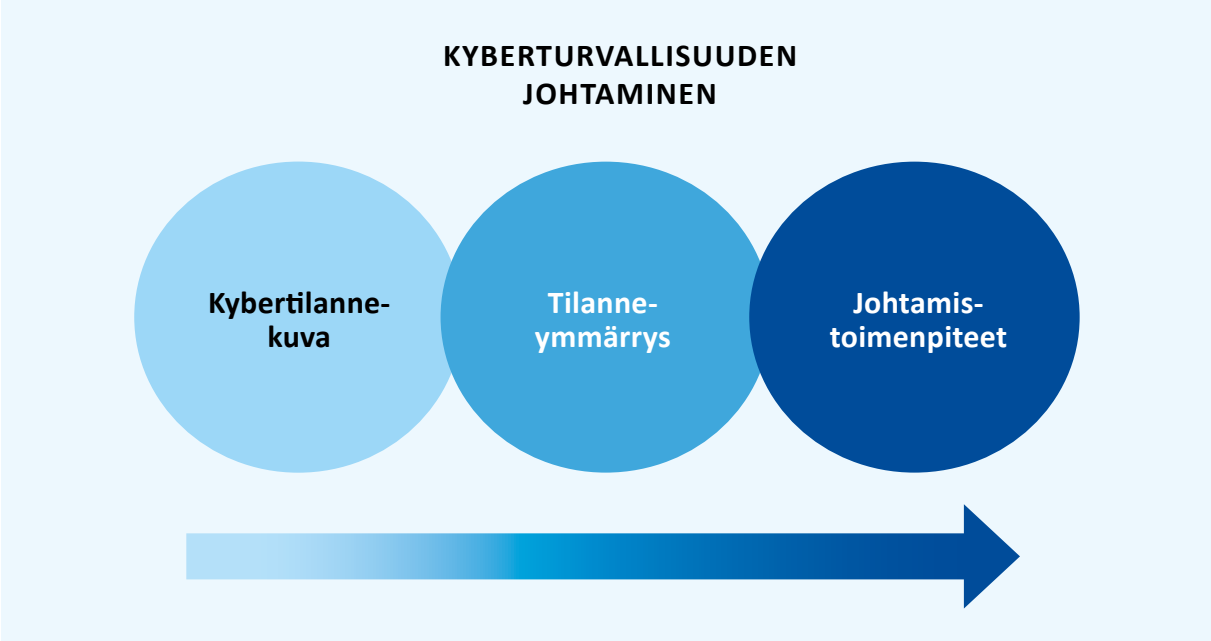
Toimitusjohtaja hoitaa yhtiön juoksevaa hallintoa hallituksen antamien ohjeiden ja määräyksien mukaisesti. Hänen on annettava hallitukselle ja sen jäsenelle tiedot, jotka ovat tarpeen hallituksen tehtävien hoitamiseksi.

Johtoryhmän tehtävät digitalisaation turvallisuuteen liittyen:

1. Pitää oma ja yrityksen tilannetietoisuus (tilannekuva) ajan tasalla.
2. Varmistaa, että digitalisaation ja kyberturvallisuuden hallintasuunnitelma (tapahtumat, riskit) on olemassa.
3. Ymmärtää rooli(t) poikkeavien tapahtumien hallinnassa oman vastuualueen osalta.
4. Osallistua harjoituksiin.
5. Kannustaa hyvään turvallisuuskulttuuriin.

Viestintästrategia

Viestintästrategia tukee organisaation ylätason strategian tavoitteiden toteutumista. Se sisältää samat arvot, kohderyhmät ja tavoitteet sekä ottaa huomioon organisaation haasteet ja toimintaympäristön. Strategian perusteella tehdään valintoja: mitä asioita tai tuotteita haluamme saattaa kohderyhmiemme tietoon, minkälaista viestiä, kieltä ja kanavia käytämme sekä kenen suulla viestintää käytännössä tehdään. Viestintästrategia sisältää kriisiviestinnän perusteet ja toimintatavat.



4. Strategia

Strategia on pitkän ajan toimintaan liitetty suunnitelma, jota organisaatio kehittää ja noudattaa parantaakseen tuotteiden ja palveluiden tuotantoa huomioiden samalla toimintaympäristön uhkat ja mahdollisuudet. Strategian päämääränä markkinoilla on saavuttaa kilpailuetua suhteessa kilpailijoihin. Jokaisella yrityksellä on omat lähtökohtansa strategiaan.

Digi- ja kyberturvallisuuden strategisella suunnittelulla tulee varmistaa, että yrityksen ylin johto ymmärtää, miten teknologiat auttavat liiketoimintatavoitteiden saavuttamisessa sekä millainen sietokyky organisaatiolla on kestää toiminnasta ja teknologiasta johtuvia tappioita. Osallistava suunnittelu on keino sitouttaa yritysjohtoa digi- ja kyberturvallisuuden huomioimiseen strategiassa.

Riskienhallinta

Hallitus varmistaa, että yrityksen johto yhdistää resilienssin ja digi- ja kyberriskien arvioinnin yleiseen liiketoimintastrategiaan, yrityksen riskienhallintakokonaisuuteen sekä budjetoinnin ja resurssien kohdentamiseen.

5. Tavoitteet

Resilienssi, sietokyky

ISO 2007 standardia mukaillen on tavoite yrityksen organisaation, henkilöstön, järjestelmän, tietoverkon, toimenpiteiden ja prosessin kyky sietää liiketoimintakatkon tai häiriön aiheuttamat seuraukset ja jatkaa toimintaa hyväksyttävällä minimitasolla.

Jatkuvuuden hallinta

ISO 22301 standardia mukaillen on tavoitteena se, että liiketoiminnan jatkuvuuden hallintajärjestelmä turvaa organisaation ja yrityksen kyvyn jatkaa toimintaansa häiriötilanteessa. Sen avulla tunnistetaan toiminnan haavoittuvat osa-alueet ja pystytään arvioimaan uhkien vaikutukset sekä suunnittelemaan ja toteuttamaan toimintatavat häiriötilanteiden varalle. Liiketoiminnan jatkuvuuden hallintajärjestelmän rakentamisessa ja toteuttamisessa voidaan käyttää standardia ISO 22301. Siinä määritellään vaatimukset, jotka koskevat hallintajärjestelmän toteuttamista, ylläpitämistä ja parantamista. Vaatimukset soveltuvat kaikenlaisille ja -kokoisille organisaatioille tai niiden osille niin yksityisellä kuin julkisellakin puolella.

Kilpailuetu – arvon tuottaminen

Kilpailuetu on yrityksen suhteellinen etu kilpailijoihinsa ja potentiaalisiin kilpailijoihinsa nähden jossain liiketoiminnan menestykseen vaikuttavassa kyvyssä, toimintatavassa tai muussa menestystekijässä. Menestyneimmät yritykset tunnistavat digitaalisen teknologian liiketoiminnalle tuomia mahdollisuuksia ja myös hyödyntävät niitä aktiivisesti (esim. mobiiliteknologiat ja sosiaalinen media, analytiikka). Digitaalisuutta strategisesti hyödyntävät yritykset menestyvät taloudellisesti yleensä hyvin ja tuottavat arvoa yritykselle.

Digitaalisen ja kyberturvallisuuden kustannusvaikuttavuuden arviointi

Digitaalisen ja kyberturvallisuuden kustannusvaikuttavuuden arviointi perustuu riskiarviointeihin sekä toiminnallisiin indikaattoreihin. Riskiarviointeihin sisältyy jokaisen merkittävän riskin arviointi myös digitaalisen turvallisuuden näkökulmasta kuvaamalla kvantitatiivisesti riskin todennäköisyys ja vaikutus sekä suojaustoimien vaikutuksia riskiin. Tavoitteena on riskianalyysin perusteella kohdistaa digitaalisen ja kyberturvallisuuden investoinnit olennaisten riskien torjumiseen. Toiminnallisten indikaattoreiden avulla mitataan tavoitteita, joiden synnyttämiä hyötyjä ei voida arvioida euromääräisesti.[10] Voidaan arvioida esimerkiksi asiakkaiden luottamuksen menetystä, jonka seurauksena asiakkaat siirtyvät kilpailijalle. Poikkeamatilanteista aiheutuvat menetykset voidaan jaotella seuraavasti: taloudelliset menetykset, operationaaliset vaikutukset, vaikutukset asiakkaisiin ja vaikutukset henkilöstöön.

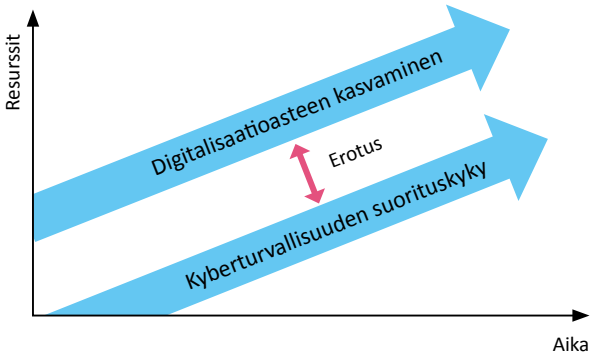
6. Tehokkuus

Digitalisaatioaste

Digitalisaatioasteella ymmärretään yleensä digitaalisten palveluiden saatavuutta ja käyttöastetta valituilla palvelualueilla. Astetta määritetään mittareilla, joita ovat esimerkiksi käyttömäärät ja käyttöasteet eri sovellusten osalta.

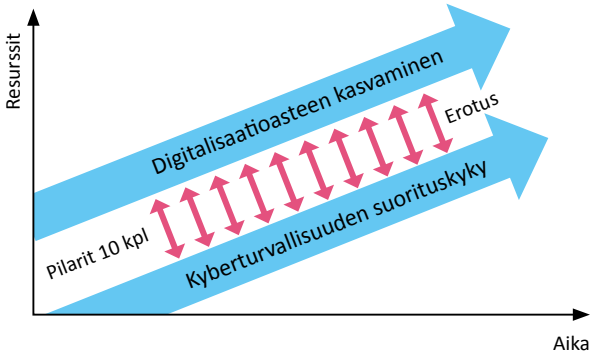
Kehitysvelka

Yrityksen digitalisaation kehitysvelka muodostuu digitalisaatioasteen kasvamisen ja siihen liittyvän kyberturvallisuuskyvyn ajallisena erotuksena. Jos erotus ajan kuluessa pienenee, yritys saavuttaa paremman suhteellisen kyberturvallisuuden. Jos erotus kuitenkin kasvaa, kyberturvallisuus ei kykene vastaamaan digitalisaation kehitykseen. Erotuksen kasvaminen vaatii investointeja turvallisuuden kasvattamiseen.



Kehitysvelan arviointi

Kehitysvelkaa voidaan arvioida esimerkiksi hyödyntäen aiemmin esitettyä pilarimallia. Jokainen pilari arvioidaan asteikolla 0–5 (0=paras tulos) ja pisteet lasketaan yhteen. Mitä pienempi summa, sitä pienempi kehitysvelka on. Useamman ajallisesti peräkkäisen arvioinnin jälkeen voidaan laskea erotuksen suunta. Tämän perusteella johtoryhmä voi tarkentaa yrityksen resursseja tarvittavaan suuntaan. Digitalisaation hyödyt jäävät saavuttamatta, jos kehitysvelka on liian suuri.



7. Liiketoiminnan jatkuvuuden hallinta

Jatkuvuussuunnitelma ja toimeenpano

Hallitus varmistaa, että johto tukee sietokyvystä/digi- ja kyberturvallisuudesta vastuussa olevaa johtajaa laatimalla, toteuttamalla, testaamalla ja parantamalla jatkuvasti jatkuvuussuunnitelmia. Niiden on yhdenmukaisesti koskettava yrityksen kaikkia liiketoiminta-alueita. Tämä edellyttää, että toimitusjohtaja (tai nimetty vastuujohtaja) seuraa suorituskykyä ja raportoi siitä säännöllisesti hallitukselle.

Harjoittelu

Hallitus varmistaa, että yrityksessä järjestetään yrityksen digi- ja kyberturvallisuuteen liittyviä harjoituksia. Johtoryhmä osallistuu harjoituksiin itse rooliensa mukaisesti. Johtoryhmä raportoi havainnoista ja muutosesityksistä hallitukselle.

Liite 2:

TOIMENPIDESUOSITUKSIA ERI YRITYSTYYPEILLE

TYYPPI	1	2	3	4
KOKOLUOKKA	Mikro - PK-yritys	Mikro - PK-yritys	Konserni - suuryritys	Konserni - suuryritys
YMPÄRISTÖ	Vakaa/dynaaminen	Turbulentti/ dynaaminen	Vakaa	Dynaaminen/ turbulentti
DIGITALISAATIOASTE	Matala	Korkea	Matala	Korkea
TUOTETYYPPI	Markkinoihin sopeutuvat	Yksilölliset tuotteet, vakaat palvelut	Standardit tuotteet, tai palvelut, massatuotteet	Asiakaskohtaiset tuotteet tai palvelut
1. Ylimmän johdon kokonaisvaltainen ja luotettava digi- ja kybertilanneymmärrys	Yhteisen tilannekuvanäkymän perusteella tehdään johdonmukaisesti toimenpiteitä.			
2. Luotettava ja uskottava digi- ja kyberriskianalyysi ja riskienhallintajärjestelmä	Digi- ja kyberriskien hallinta on määritelty koko organisaatiolle.	Digi- ja kyberriskien hallintaa seurataan systemaattisesti ja kehitetään jatkuvasti osana koko organisaation riskienhallintaa.	Digi- ja kyberriskien hallintaa seurataan systemaattisesti ja kehitetään jatkuvasti osana koko organisaation riskienhallintaa.	Digi- ja kyberriskien hallintastrategia on osa muuta riskienhallintastrategiaa.
3. Strategisen kyberjohtamisen konsepti osana liiketoimintastrategiaa	Konsepti on laadittu osaksi liiketoimintastrategiaa.			
4. Oikeasuhtainen digi- ja kyberturvallisuuden resursointi	Kriittisten palveluiden resursointi on suunniteltu kaikille kriittisille resursseille koko organisaatiossa.	Kriittisten palveluiden resurssointi on järjestetty johdon seurantaan ja niiden yhteys yhteiskuntaan on selvä koko organisaatiossa.	Kriittisten palveluiden resurssointi on järjestetty johdon seurantaan ja niiden yhteys yhteiskuntaan on selvä koko organisaatiossa.	Ylimmällä johdolla on vastuu riittävien resurssien turvaamisesta kriittisten palveluiden tuottamiseen, ja päätöksenteko on valtuutettu asianmukaisesti ja tehokkaasti.
5. Oikeat ja innovatiiviset teknologiavalinnat ja niiden toimintakyky	Valinnat tukevat digitalisaatiota ja ovat kyberturvalliset sekä toimintakykyiset.			
6. Kokonaisvaltainen ja ajantasainen varautuminen ja jatkuvuuden hallinnan suunnitelma	Jatkuvuuden suunnittelu on määritelty koko organisaatiolle.	Jatkuvuuden suunnittelua tehdään järjestelmällisesti ja kehitetään riskilähtöisesti.	Jatkuvuuden suunnittelua tehdään järjestelmällisesti ja kehitetään riskilähtöisesti.	Organisaatio harjoittelee säännöllisesti toipumista erilaisista poikkeamista, häiriöistä ja onnettomuuksista sekä parantaa suunnitelmia harjoituksien perusteella.
7. Hyvin koulutettu ja harjoitettu kriisijohtamisorganisaatio, sekä kriisiviestintäsuunnitelma	Turvallisuushenkilöstön tieto- ja taitovaatimukset on määritelty johdonmukaisesti koko organisaatiolle. Digi- ja kyberturvallisuustiedon kerääminen ja jakaminen on suunniteltu koko organisaatiolle ja sidosryhmille.	Turvallisuushenkilöstöä, arviointeja ja koulutusohjelmia kehitetään säännöllisesti. Digi- ja kyberturvallisuustietoa kerätään, analysoidaan ja jaetaan johdonmukaisesti koko organisaatiolle ja sidosryhmille.	Turvallisuushenkilöstöä, arviointeja ja koulutusohjelmia kehitetään säännöllisesti. Digi- ja kyberturvallisuustietoa kerätään, analysoidaan ja jaetaan johdonmukaisesti koko organisaatiolle ja sidosryhmille.	Koulutus- ja harjoitustoiminnalla johto ja turvallisuushenkilöstö perehdytetään ennalta vakaviinkin kyberturvallisuuspoikkeamiin ja -skenaarioihin. Ylläpidetään suhteita sisäisten ja ulkoisten toimijoiden kanssa tietojen keräämiseksi ja jakamiseksi kyberturvallisuudesta, uhista ja haavoittuvuuksista tavoitteena pienentää riskejä ja vahvistaa toimintakykyä.
8. Vaatimukset täyttävät ydinprosessit ja toimintatavat	Yrityksen ydinprosessit ja toimintatavat vastaavat liiketoiminnan kehittämisen ja toimintaympäristön vaatimuksiin. Ne on toimeenpantu ja niitä ylläpidetään liiketoiminnan tai toimintaympäristön muuttuessa.			
9. Koko henkilöstön asianmukaiset digi- ja kybertaidot ja osaaminen	Henkilöstön tieto- ja taitovaatimukset on määritelty johdonmukaisesti koko organisaatiolle.	Henkilöstöä, arviointeja ja koulutusohjelmia kehitetään säännöllisesti.	Henkilöstöä, arviointeja ja koulutusohjelmia kehitetään säännöllisesti.	Koulutus- ja harjoitustoiminnalla henkilöstö perehdytetään ennalta turvallisuuspoikkeamiin ja ylläpidetään tiedot ja taidot.
10. Ylimmän johdon hyväksymä, joustava ja kehittyvä digikulttuuri	Yrityksen johtaminen tukee kulttuurin kehittymistä täysimääräisesti.			

Liite 3:

ESIMERKKEJÄ YRITYKSEN KÄYTTÖÖN TARKOITETUISTA OHJEISTA TAI OPPAISTA

Kyberturvallisuus ja yrityksen hallituksen vastuu, Traficomin julkaisuja 2/2020.
(Opas perustuu NCSC-UK:n julkaisuun Cyber Security Toolkit for Boards)

Pienyritysten kyberturvallisuusopas, Kyberturvallisuuskeskus, Traficomin julkaisuja 228/2020.
(Opas perustuu Australian kyberturvallisuusviranomaisen tuottamaan materiaaliin Small Business Cyber Security Guide.)

Advancing Cyber Resilience Principles and Tools for Boards, World Economic Forum 2017.

Cyber Security Toolkit for Boards, National Cyber Security Centre, UK.

SFS (2021) ISO/IEC 27000 Tietoturvallisuuden standardisarja,
https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

Katakri 2020 -Tietoturvallisuuden auditointityökalu viranomaisille. Traficomin julkaisusarja 232/2020.

Kybermittari. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

LÄHTEET

1 Boone, A. (2017). Cyber-security must be a C-suite priority. Computer Fraud & Security, 2017(2), 13–15.

2 Kansallisen turvallisuuden katsaus 2021, Suojelupoliisi. https://supo.fi/kyberuhkat.

3, 5 Matthew Doan (2019). Companies need to rethink what cybersecurity leadership is? Boston Consulting Group, https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is.

4 Cybergovernance role board interview. (2018) Teknologiayritys Kaiser Permanenten teknologiariskijohtajan George DeCesaren haastattelu, https://www.bcg.com/en-nor/publications/2018/cybergovernance-role-board-interview-kaiser-permanente-george-decesare.

6 Ayman Al Issa, Tucker Bailey, Jim Boehm ja David Weinstein (2021). Enterprise cybersecurity aligning third parties and supply chains. McKinsey, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/enterprise-cybersecurity-aligning-third-parties-and-supply-chains.

7 Aapo Cederberg, Strategic cyber leadership is needed to address current security challenges. Cyberwatch Magazine 2021/3.

8 Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen, Kyberturvallisuuden strateginen johtaminen Suomessa, Maaliskuu 2018, Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 28/2018.

9 Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

10 Digitaalisen turvallisuuden kustannus-vaikuttavuusarviointi julkisessa hallinnossa, selvitystyön raportti 1.6.2020, Valtiovarainministeriö.

Työssä käytetyt kirjallisuuslähteet

Tämä opas perustuu tuotoksiin, jotka toteutettiin Huoltovarmuusorganisaation Digipoolin projektissa #Strategia22. Projektin toteuttajana oli Cyberwatch Finland Oy.
https://www.digipooli.fi/fi/ajankohtaista/uutinen/strategia22-projekti-havainnot-ja-tuotokset

Accenture, Cyber threat intelligence report 2021,
https://www.accenture.com/fi-en/insights/security/cyber-threat-intelligence-report-2021.

Alashi S. A., Badi D. H. (2020) The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations, Department of Information Science, King Abdulaziz University, Jeddah, Saudi Arabia.

Andrews, K. R. (1997). A reader in the resource-based perspective. Foss, N. J. (toim.), (pp. 52-59). New York, NY, United States: Oxford University Press.

Fujitsu, Customer-first security: What it is and best practices for success, Fujitsu_Customer_First_Security_Whitepaper123.pdf, fujitsu.com.

Garcia-Granados, F (2020) Cybersecurity Knowledge Requirements for Strategic Level Decision Makers, Conference Paper, Tallinn University of Technology.

Hill, A & Hill, T (2009) Manufacturing operations strategy. Palgrave Macmillan.

Leena Hiltunen, Metodina kyselytutkimus, Jyväskylän Yliopisto, 2009.

IBM, IBM Security Strategy, Risk and Compliance Services, https://www.ibm.com/downloads/cas/GKN51N92

Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

Johnson, G., Scholes, K. & Whittington, R. (2008). Exploring corporate strategy (8. ed.). Harlow; Munich: Prentice Hall Financial Times.

Kansallinen turvallisuusviranomainen, Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille, Traficomin julkaisusarja, ISSN 2669-8757, verkkojulkaisu.

Kim, J. (2017). Cyber-security in government: reducing the risk. Computer Fraud & Security, 2017(7), 8–11.

KPMG, Kyberturva kohtaa fyysisen maailman turvallisuuden, 2021, https://home.kpmg/fi/fi/blogs/home/posts/2021/05/kyberturva-kohtaa-fyysisen-maailman-turvallisuuden.html, sekä https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut/teknologiakonsultointi/tietoturva.html

Kyberturvallisuuskeskus, Kyberturvallisuus ja yrityksen hallituksen vastuu, (alkuperäinen Cyber Security Toolkit for Boards, NCSC, 2019, ncsc.gov.uk), Kyberturvallisuuskeskus 2/2020, kyberturvallisuuskeskus.fi

Kyberturvallisuuskeskus, Pienyritysten kyberturvallisuusopas, Traficomin julkaisuja 228/2020. (Opas perustuu Australian kyberturvallisuusviranomaisen tuottamaan materiaaliin Small Business Cyber Security Guide.)

Kasey Panetta, 5 Security Questions Your Board Will Inevitably Ask, Gandner 12.6.2020a, varsinainen raportti Sam Olyaei ja Jeffrey Wheatman, 19.7.2019, https://www.gartner.com/smarterwithgartner/5-security-questions-board-will-definitely-ask/

Kasey Panetta, The 15-Minute, 7-Slide Security Presentation for Your Board of Directors, Gardner 18.6.2020b, https://www.gartner.com/smarterwithgartner/the-15-minute-7-slide-security-presentation-for-your-board-of-directors

Posthumus, S., von Solms, R. (2004). A framework for the governance of information security. Computers & Security, Volume 23, Issue 8, 2004, 638-646.

SFS (2021) ISO/IEC 27000 Tietoturvallisuuden standardisarja, https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

von Solms, B. (2001). Corporate Governance and Information Security. Computers & Security, Volume 20, Issue 3, 2001, 215-218.

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371–376.

Jussi Tammelin, Tietoturvastrategian ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa, Jyväskylän yliopisto, 2021, pro gradu.

TietoEVRY, An Introduction to Cybersecurity, https://www.tietoevry.com/en/services/Cybersecurity/cybersecurity-guidebook

Jiri Vidgren, Kyberturvallisuus yritysstrategiassa, 2019, Jyväskylän yliopisto, Tietojärjestelmätiede, kandidaatintutkielma.

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI