HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

STRATEGIA22

TURVALLISEN DIGITALISAATION TYÖKALUPAKKI YRITYSJOHTAJALLE

31.3.2022

Digipooli ja Cyberwatch Oy

Sisällys

TURVALLISEN DIGITALISAATION TYÖKALUPAKKI YRITYSJOHTAJALLE

Viime vuosina ei pelkästään elinkeinoelämä, vaan koko yhteiskunta on panostanut laajasti digitaalisiin ratkaisuihin. Valtavassa kehitysinnossa ei aina ole muistettu huolehtia myös digitaalisesta turvallisuudesta. Kyber- ja kokonaisturvallisuuden tulisi kuitenkin aina olla uusissa hankkeissa mukana alusta lähtien ja organisaatioiden tulisi systemaattisesti kehittää omaa kyberkulttuuriaan.

Yrityksen digitalisaatioratkaisuissa on syytä keskittyä ensin niiden strategisiin perusteisiin, paremman kokonaistilannekuvan ymmärtämiseen, sekä toimintatapoihin ja prosesseihin. Vasta sen jälkeen on aika katsoa, mitä digiteknologiaa ja -palveluja yritys tarvitsee. Näiden tekijöiden perusteellisen ymmärryksen ja toimeenpanon jälkeen on mahdollisuus kasvattaa liiketoimintaa, lisätä sijoittajien luottamusta, sekä tuottaa lisäarvoa ja kasvua omistajille.

Kyberrikollisuuden määrä ja maailmanlaajuiset kustannukset nousevat nopeasti, mikä johtuu hyökkäysten toteutuskustannusten alenemisesta ja suojautumistarpeen lisääntymisestä. Pandemian aikana digitaalisten laitteiden määrä on lisääntynyt merkittävästi ja niitä käytetään entistä useammasta paikasta. Samalla yritysten ydintoiminnot ovat entistä riippuvaisempia digitaalisista järjestelmistä.

Digitaalisessa turvallisuudessa pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuden takaamiseen. Uhat pyritään tunnistamaan ja ehkäisemään, sekä varautumaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisissä toiminnoissa. Digitaaliseen turvallisuuteen kuuluvat (julkisen hallinnon viitekehyksen) mukaisesti riskien hallinta ja käsittely, toiminnan jatkuvuuden hallinta ja varautuminen, tietoturvallisuus ja tietosuoja, sekä kyberturvallisuus.

Digitaalisten ratkaisujen turvallisuus tulee olla ylimmän johdon keskeinen tavoite, sillä johto on lopulta vastuussa kaikesta, mitä yrityksessä tapahtuu. Digiturvallisuutta tulee johtaa koko organisaation laajuisesti, keskitetysti ja johdonmukaisesti. Liiketoimintayksiköille on annettava selkeät vastuut ja tehtävät oman digiturvallisuutensa toteuttamisesta. Ylimmän johdon tulee priorisoida digi- ja kyberturvallisuus osaksi liiketoimintayksikön omia ydintoimintoja .[1] Samanaikaisesti liiketoiminnan kanssa on seurattava digitalisaation kehitysvelkaa, jota kertyy kehittyvien toimintojen ja järjestelmien, sekä niiden kyberturvallisuuden välille.

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.

Yrityksille digitalisaation tuoma riski on nykyään kaikkialla. Monilla yrityksillä on edelleen haasteena tehdä kyberturvallisuudesta ennakoiva osa strategiaa, toimintaa ja kulttuuria ja nähdä se enemmän mahdollisuutena, kuin uhkana. Perimmäinen syy on kaksitahoinen: 1) Kyberturvallisuutta käsitellään teknologisena haasteena ja hallinnollisena työnä, sekä 2) useimmat digi- ja kyberturvallisuusjohtajat eivät osallistu yrityksen strategiseen päätöksentekoon. Nykypäivän johtajien on kyettävä sulauttamaan turvallisuus koko yrityksen toimintaan, reagoimaan nopeasti uhkiin ja vaikuttamaan muihin johtajiin[3]. Yritykselle on kehitettävä

uskottava turvallisuuskulttuuri, joka päivittyy jatkuvasti. Lisäksi digi- ja kyberturvallisuus on oltava pysyvästi hallituksen ja johtoryhmän agendalla.

Yrityksen ylimmän johdon tulee olla sitoutunut ja vastuullinen kyberturvallisuuden kehittämisessä. Suomessa Osakeyhtiölakiin 2006/624 § 8 on kirjattu: “Yhtiön johdon on huolellisesti toimien edistettävä yhtiön etua”. Tämän lisäksi tietoturvallisuuden näkökulmasta yritysten toimintaa velvoittaa muun muassa Euroopan Unionin GDPR-säännöstö, joka ohjaa yritysjohdon sitoutumista tietosuojan ja -turvallisuuden toteuttamiseen myös sanktioilla.

Digitalisaation turvallisuuteen kuuluu oleellisena osana riskienhallinta. Digi- ja kyberriskit ovat osa korkean tason strategisia ja liiketoimintariskejä, joita tulee käsitellä yhtenä kokonaisuutena, ei erillisinä huolen aiheina[4]. Digi- ja kyberriskit ovat kuin mitkä tahansa muut merkittävät liiketoimintariskit, jotka voivat vaikuttaa strategiaan, talouteen ja teknologiavalintoihin. Myös liiketoimintaketjujen hallinta ja niiden suojaaminen, kumppanuussopimukset ja kybervakuutukset ovat tarvittaessa otettava huomioon liiketoimintamallia toteutettaessa.

Kaikkien yritysten tulisi harkita strategiansa rakentamisessa liiketoiminnan jatkuvuutta, brändin suojausta, vaatimustenmukaisuutta ja kasvua. Liiketoimintakonteksti ohjaa strategisia valintoja; kannattaa miettiä tekijöitä, kuten sääntelypainetta, riskialttiutta ja mitä asiakkaat arvostavat.

Koska digi- ja kyberturvallisuus ei voi toimia tyhjiössä, yritysjohtajien on kannustettava oikeita sidosryhmiä tekemään tiivistä yhteistyötä keskenään – keskeistä on ekosysteemiajattelu. Vaikka organisaatiot tarvitsevat digitaitoja, kuten verkkoturvallisuutta, uhkatiedustelua ja tapahtumiin reagointia, niiden ei pitäisi olla mittapuu, joilla digijohtajia mitataan. Digi- ja kyberjohtajissa on arvostettava myös teknisiä valmiuksia, mutta liiketoimintajohtajien on itse otettava avainrooli liiketoimintastrategian lisäksi myös teknologiapäätöksissä ja riskienhallinnassa[5].

Viimeaikaiset kyberhyökkäykset ovat tehneet monista digi- ja kyberturvallisuushaasteista jopa aiempaa selkeämpiä. Yksi huomioista on, että yritysten turvallisuus on yhtä riippuvainen maailmanlaajuisesta digiekosysteemistä, kuin vain läheisten yritysten ja organisaatioiden toimista. Kyberturvallisuuden korkea "hygienia" – digisuojauksen hoito, tiukkuus ja perusteellisuus – on ratkaisevan tärkeää. Tasaisen korkean kyberhygienian ylläpitämiseksi koko yrityksessä, mukaan lukien uudet investoinnit ja yhteistyökumppanit, tarvitaan läpinäkyvyyttä ja avointa viestintää[6]. Yrityksen hallituksella ja operatiivisella johdolla tulee olla ajantasainen ja ennakoinnin mahdollistava kybertilannekuva, sekä kokonaisvaltainen ymmärrys yrityksen digi- ja kyberturvallisuuden tasosta. Strategisen tason digi- ja kyberturvallisuuden johtaminen korostuu.

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

#STRATEGIA22-projektin puolesta

Digipooli

YRITYSJOHTAJAN TYÖKALUPAKIN PERUSTEET

Strategisen digi- ja kyberjohtamisen voi määritellä noudattaen strategisen johtamisen yleisiä periaatteita. Ne voidaan kiteyttää kymmeneen osakokonaisuuteen, jotka ovat peruspilareita, joille strateginen digijohtaminen on rakennettava. Ne osoittavat, että digi- ja kyberturvallisuus on oltava ylimmän johdon agendalla ja kiinteä osa jokaisen yrityksen ja organisaation jokapäiväistä johtamista.

Vastuu on jakamaton ja johdolla on oltava joka hetki riittävä digitalisaatioon liittyvien riskien lukutaito. Tämä ei tarkoita, että jokaisen on oltava tekninen asiantuntija, mutta kokonaisvaltainen tilanneymmärrys luo hyvät edellytykset johtamiselle ja oikea-aikaisille päätöksille.

Digi- ja kyberjohtamiseen panostaminen maksaa varmasti itsensä takaisin paremman kilpailukyvyn ja henkilöstön työtyytyväisyyden kautta. Teknologialla voimme ratkaista alle puolet kasvavasta digi- ja kyberturvallisuuden haasteista. Ihminen nousee keskiöön, vastuullinen työnantaja panostaa osaamiseen ja digitaitoihin, joita me kaikki tarvitsemme myös jokapäiväisessä elämässämme.

Tämä työn pohjana olevat strategisen kyberjohtamisen peruspilarit[7] voidaan ryhmitellä neljään osa-alueeseen:

I. Johtaminen

1. Ylimmän johdon kokonaisvaltainen ja luotettava digi- ja kybertilanneymmärrys
2. Luotettava ja uskottava digi- ja kyberriskianalyysi ja riskienhallintajärjestelmä
3. Strateginen kyberjohtamisen konsepti osana liiketoimintastrategiaa

II. Resursointi

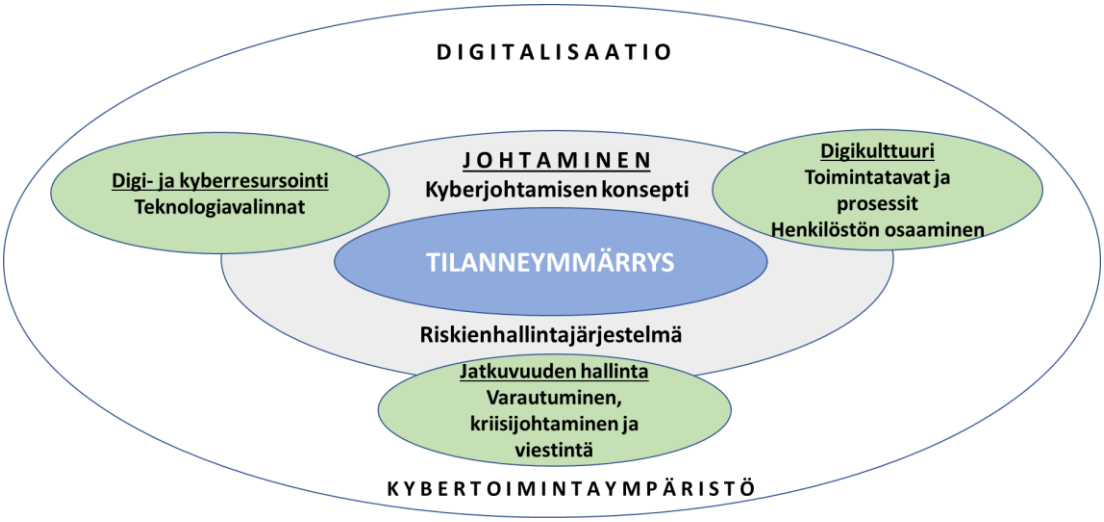
4. Oikeasuhtainen digi- ja kyberturvallisuuden resursointi
5. Oikeat ja innovatiiviset teknologiavalinnat ja niiden toimintakyky

III. Jatkuvuuden hallinta

6. Kokonaisvaltainen ja ajantasainen varautuminen ja jatkuvuuden hallinnan suunnitelma
7. Hyvin koulutettu ja harjoitettu kriisijohtamisorganisaatio, sekä kriisiviestintäsuunnitelma

IV. Digikulttuuri

8. Ydinprosessit ja toimintatavat vastaavat liiketoiminnan kehittämisen ja toimintaympäristön vaatimuksiin
9. Koko henkilöstön asianmukaiset digi- ja kybertaidot, sekä osaaminen
10. Ylimmän johdon hyväksymä, joustava ja kehittyvä digi- ja kyberkulttuuri

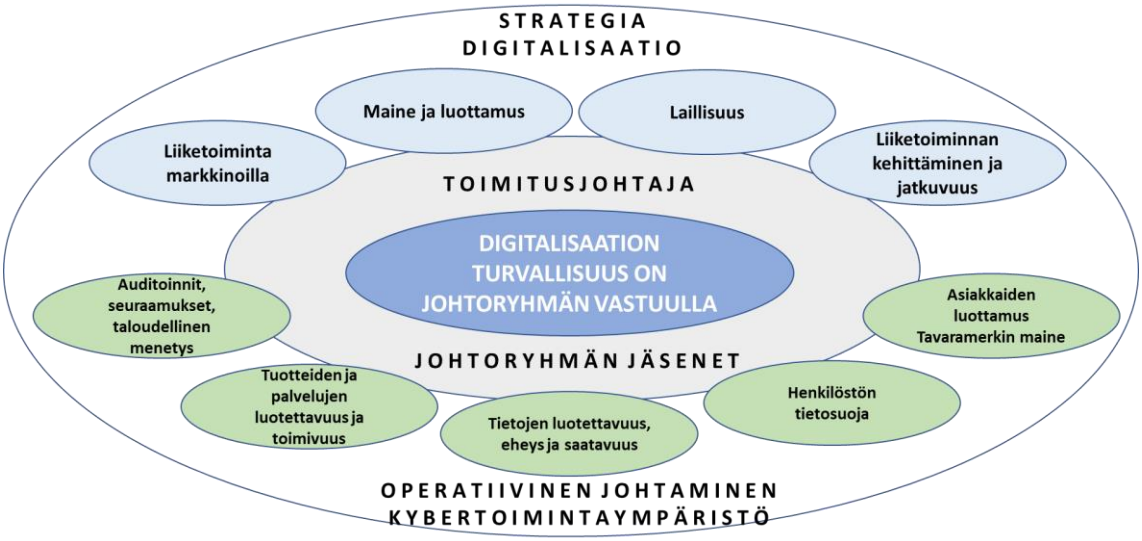


Kuva 1. Digitalisaation johtamisen neljä jalkaa ja turvallisuuden peruspilarit

Yrityksen johtoryhmän tehtävänä on tyypillisesti yhdessä toimitusjohtajan kanssa valmistella yhtiön strategia, liiketoimintasuunnitelmat, budjetti, sekä muut hallitukselle päätettäväksi menevät asiat. Lisäksi johtoryhmä yleensä päättää ja käsittelee yhtiön kannalta merkittävimmät operatiiviset asiat. Johtoryhmän tehtävät voidaan määritellä tarkemmin johtoryhmän työjärjestyksessä.

Liiketoiminnan laajentamisessa ja jatkuvuuden hallinnassa on keskeistä tunnistaa digitaalisen turvallisuuden rooli strategian toteuttamisessa. Strategia yleensä kertoo, kuinka yritys laajentaa markkinoitaan, tai ylläpitää saavutettua markkinaosuutta ja kilpailuvalttejaan, joihin kuuluvat kumppanit, sekä tuote- ja palvelukehitys, että mahdolliset yritysostot ja oma osaaminen. Yrityksen eri toimialoja ja liiketoimintoja tulee tarkastella ainakin myynnin ja markkinoinnin, viestinnän, taloushallinnon, tuotannon ja palveluiden, sidosryhmien ja asiakkuuksien, riskien ja jatkuvuudenhallinnan, sekä kehittämisen näkökulmista.

Toimitusjohtaja valitsee johtoryhmän jäsenet. Tässä yhteydessä olisi eduksi, että useammalla henkilöllä olisi digitalisaation turvallisuuteen liittyvää osaamista. Erikseen nimetyn digijohtajan tehtävä voi olla välivaihe, kunnes kaikilla johtoryhmän jäsenillä on riittävä osaaminen digitaalisesta turvallisuudesta. Koska kokonaisuus on johtoryhmän vastuulla, osaamisen perusteella on mahdollista jakaa vastuuta toiminnoittain, tai liiketoiminta-alueittain. Kuvassa 2 on esitetty mahdollisuuksia vastuiden jakamiseksi.



Kuva 2. Esimerkki johtoryhmän vastuuaiheiden jakautumisesta johtoryhmässä

KYBERTURVALLISUUDEN TYÖKALUPAKKI YHDELLÄ SIVULLA

1. ***Ylimmän johdon kokonaisvaltainen ja luotettava digi- ja kybertilanneymmärrys***

   Operatiivinen johto vastaa siitä, että hallitukselle raportoidaan ymmärrettävä arvio digi- ja kyberriskeistä, uhista ja seurannaisvaikutuksista pysyvänä asialistan kohtana hallituksen kokouksissa.

2. ***Luotettava ja uskottava digi- ja kyberriski-analyysi ja riskienhallintajärjestelmä***

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

3. ***Strateginen kyberjohtamiskonsepti osana liiketoimintastrategiaa***

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

4. ***Oikeasuhtainen digi- ja kyberturvallisuuden resursointi***

   Hallituksella on kyky ymmärtää digi- ja kyberturvallisuusriskien vaikutuksia ja sitä, miten ne voivat olla erilaisia suhteessa yrityksen eri tavoitteisiin riskien ja digiturvallisuustoimenpiteiden operatiivisten kustannusten/vaikutusten tasapainottamisessa. Digi- ja kyberturvallisuuden investointien hyödyt on mitoitettu.

5. ***Oikeat ja innovatiiviset digiteknologiavalinnat ja niiden toimintakyky***

   Digitalisaation tavoitteet on määritetty yrityksen strategiassa (esim. digitalisaatioaste). Ennen tavoitteiden asettamista on käyty läpi erilaiset kehitystä tukevat teknologiat, jonka jälkeen on määritetty tavoitteet niiden hyödyntämisestä liiketoiminnan ja hallinnon osalta.

6. ***Digivarautumisen ja jatkuvuuden hallinnan suunnitelma***

   Hallitus varmistaa, että johto tukee sietokyvystä tai digi- ja kyberturvallisuudesta vastuujohtajaa laatimalla, toteuttamalla, testaamalla ja parantamalla jatkuvasti toipumissuunnitelmia. Niiden on oltava yhdenmukaistettu koskien yrityksen kaikkia liiketoiminta-alueita, joka edellyttää suorituskyvyn seurantaa ja raportointia säännöllisesti hallitukselle.

7. ***Hyvin koulutettu ja harjoitettu kriisijohtamisorganisaatio, sekä -viestintä***

   Hallituksen ja johtoryhmän jäsenet saavat perehdytyksen digi- ja kyberturvallisuuteen ottaessaan tehtävän vastaan, ja heitä päivitetään säännöllisesti viimeaikaisista uhkista ja tapahtumista. Henkilöt osallistuvat suunnitelman mukaisiin harjoituksiin.

8. ***Vaatimukset täyttävät ydinprosessit ja toimintatavat***

   Ydinprosessit ja toimintatavat vastaavat liiketoiminnan kehittämisen ja toimintaympäristön vaatimuksiin.

9. ***Koko henkilöstön asianmukaiset digi- ja kybertaidot, sekä osaaminen***

   Yrityksen tavoitteiden saavuttamiseen ja riskien hallitsemiseen tarvittavat taidot on määritetty. Koulutusohjelma varmistaa säännöllisen tietojen ja taitojen ylläpidon ottaen huomioon muuttuvan toimintaympäristön asettava vaatimukset. Koulutuksen taso arvioidaan säännöllisillä harjoituksilla.

10. ***Joustava ja kehittyvä digi- ja kyberkulttuuri***

    Hallitus ja johtoryhmä yhdessä varmistavat, että yrityksessä on ja kehittyy hyvä digi- ja kyberkulttuuri koostuen digitalisaatioon liitetyistä toimintatavoista, työmoraalista, yhteisistä säännöistä ja ehdoista sekä työntekijöiden välisistä vuorovaikutustavoista.

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	Markkinoiden kilpailun mukaan	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 resurssointi on suunniteltu kaikille kriittisille resursseille koko organisaatiossa.	Kriittisten palveluiden resurssointi on järjestetty johdon seurantaan ja yhteiskunnan yhteyteen johdonmukaisesti koko organisaatiossa.	Kriittisten palveluiden resurssointi on järjestetty johdon seurantaan ja yhteiskunnan yhteyteen johdonmukaisesti 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

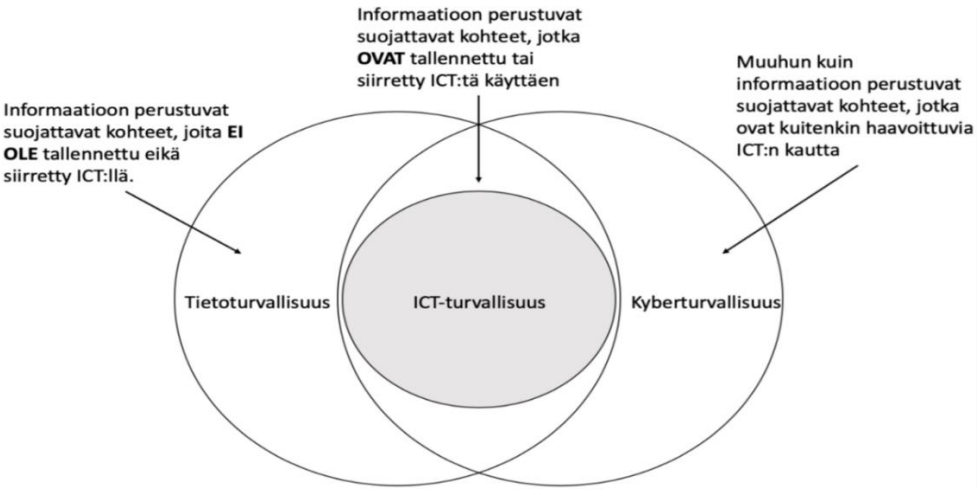
				harjoituksien perusteella.
7. Hyvin koulutettu ja harjoitettu kriisijohtamisorganisaatio, sekä kriisiviestintäsuunnitelma	Turvallisuushenkilöstön tieto- ja taitovaatimukset on määritelty johdonmukaisesti koko organisaatiolle. Digi- ja kyberturvallisuustiedon kerääminen ja jakaminen on suunniteltu koko organisaatiolle ja sidosryhmille.	Turvallisuushenkilöstöä, arviointeja ja koulutusohjelmia kehitetään säännöllisesti. Digi- ja kyberturvallisuustietoa kerätään, analysoidaan ja jaetaan johdonmukaisesti koko organisaatiossa ja sidosryhmille.	Turvallisuushenkilöstöä, arviointeja ja koulutusohjelmia kehitetään säännöllisesti. Digi- ja kyberturvallisuustietoa kerätään, analysoidaan ja jaetaan johdonmukaisesti koko organisaatiossa 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 ne ylläpidetään liiketoiminnan tai toimintaympäristön muuttuessa.			
9. Koko henkilöstön asianmukainen 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 digi- ja kyberkulttuuri	Yrityksen johtaminen tulee kulttuurin kehittymistä täysimääräisesti.			

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.



Kuva: Tietoturvallisuuden, ict-turvallisuuden ja kyberturvallisuuden määrittely

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 sen ymmärtäminen ovat edellytys 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 kaikille kokoluokan yrityksille sopivaa kybertilannekuvaa.

Kybertilannekuva ei muodostu ainoastaan teknisestä tilannekuvasta. Parhaimmillaan kybertilannekuvassa on kyetty yhdistämään onnistuneesti 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

Kybertoimintaympäristö

Yrityksen kybertoimintaympäristö on alati muuttuva. Toimintaympäristö voidaan esittää kolmella erilaisella tyypityksellä:

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

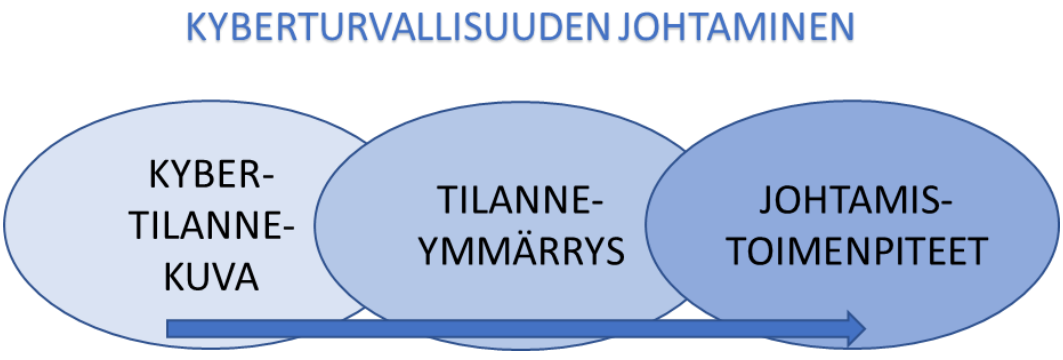
- dynaaminen ympäristö, jossa esiintyy lukumääräisesti useita muutoksia, mutta muutokset ovat enemmän tai vähemmän ennustettavissa aikaisemmista tapahtumista ja kokemuksista

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

2. 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 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- ja kyberriskien ja -sietokyvyn valvonnasta. Hallitus voi siirtää ensisijaista valvontatoimintaa olemassa olevalle valiokunnalle (esim. tarkastus- tai riskivaliokunnalle). 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 määräysten 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 sisältäen samat arvot, kohderyhmät ja tavoitteet, kuten myös ottaen huomioon organisaation haasteet ja toimintaympäristön. Näiden perusteella tehdään valintoja; mitä asioita tai tuotteita haluamme saattaa kohderyhmiemme tietoon, minkälaista viestiä, kieltä ja kanavia käytämme sekä kenen suulla viestintää tehdään käytännössä. Viestintästrategia sisältää kriisiviestinnän perusteet ja toimintatavat.

3. Strategia

Strategia on pitkän ajan toimintaan liitetty suunnitelma, jota organisaatio kehittää ja noudattaa parantaakseen tuotteiden ja palveluiden tuotantoa toimintaympäristön uhkat ja mahdollisuudet huomioiden. Strategian päämääränä kilpailumarkkinoilla 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 ja millainen sietokyky organisaatiolla on kestää toiminnasta ja teknologiasta johtuvia menetyksiä. Tämä on keino sitouttaa yritysjohtoa digi- ja kyberturvallisuuden huomioimiseen strategiassa[9].

Riskienhallinta

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

4. Tavoitteet

Resilienssi, sietokyky

Yrityksen organisaation, henkilöstön, järjestelmän, tietoverkon, toimenpiteiden ja prosessin kyky sietää liiketoimintakatkon tai häiriön aiheuttamat seuraukset ja jatkaa toimintaa hyväksyttävällä minimitasolla. (ISO 2007)

Jatkuvuuden hallinta

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. (ISO 22301)

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. mobiili- ja sosiaalinen teknologia, analytiikka). Digitaalisuutta strategisesti hyödyntävät yritykset menestyvät taloudellisesti yleensä hyvin ja tuottavat arvoa yritykselle.

Digitaalisen ja kyberturvallisuuden kustannus-vaikuttavuuden arviointi

Digitaalisen ja kyberturvallisuuden kustannus-vaikuttavuuden 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 torjumiseksi. Toiminnallisten indikaattoreiden avulla mitattaisiin tavoitteita, joiden synnyttämiä hyötyjä ei voida arvioida euromääräisesti.[10] Esimerkiksi voidaan arvioida asiakkaiden luottamuksen menetystä, jonka seurauksena asiakkaiden siirtymistä kilpailijalle. Poikkeamatilanteista aiheutuvat menetykset voidaan jaotella seuraavasti: taloudelliset menetykset, operationaaliset vaikutukset, vaikutukset asiakkaisiin ja vaikutukset henkilöstöön.

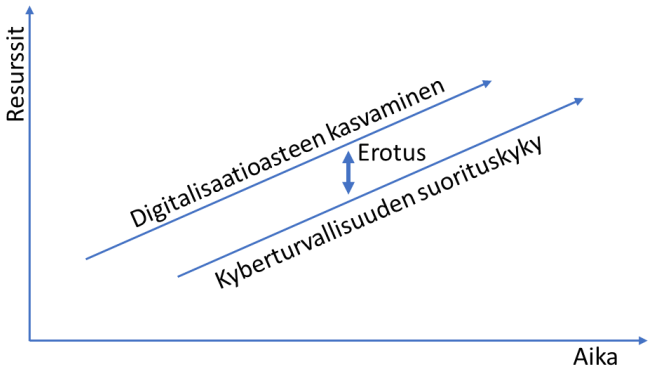
5. Tehokkuus

Digitalisaatioaste

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

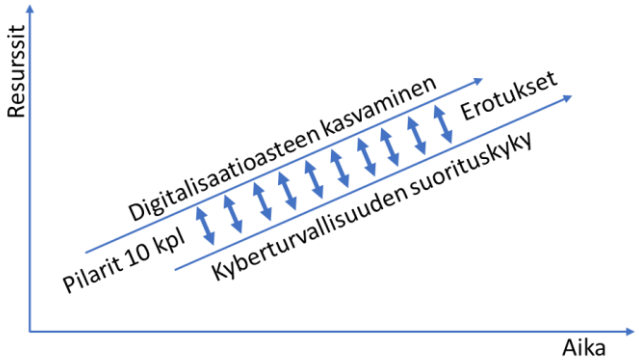
Kehitysvelka

Yrityksen digitalisaation kehitysvelka muodostuu digitalisaation 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 pilarimallilla. Jokainen pilari arvioidaan asteikolla 0–5 (0=paras tulos) ja pisteen 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 turvallisuuden edistämisessä. Digitalisaation hyödyt jäävät saavuttamatta, jos kehitysvelka on liian suuri.



6. 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 oltava yhdenmukaistettu koskien yrityksen kaikkia liiketoiminta-alueita. Tämä edellyttää, että toimitusjohtaja (tai nimetty vastuujohtaja) seuraa suorituskykyä ja raportoi siitä säännöllisesti hallitukselle.

Harjoittelu

Hallitus varmistaa ja johtoryhmä osallistuu itse rooliensa mukaisesti yrityksen digi- ja kyberturvallisuuteen liittyviin harjoituksiin. Johtoryhmä raportoi havainnoista ja muutosesityksistä hallitukselle.

YRITYSJOHTAJAN TOIMENPIDEKORTIT

Kortti koostuu kahdesta osiosta, joista ensimmäisessä on aihealueeseen johdattelevia kysymyksiä, ja sen jälkeen toinen osio, jossa on listaus niistä 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 digitaalisen turvallisuudesta päätöksenteon tueksi?

Onko hallitus vastuuttanut yrityksen oikeat henkilöt, jotta digi- ja kyberturvallisuutta ja sen edistymistä voidaan hallita digitalisaatiotavoitteiden mukaisesti?

Miten digitalisaation turvallisuuden kehitystä seurataan ja ylläpidetään?

Tehtävälista, varmistettavat asiat

Yrityksellä on selkeä toimintamalli, miten tilannekuvan kolme eri tasoa saadaan tehokkaasti käyttöön (tasot: strateginen, riskien hallinta ja operatiivinen).

Hallitukselle annetaan tarvittavat osakkeenomistajien, sääntely-, asiakas- ja muut yhteiskunnalliset ulkoiset näkökulmat, jotta he voivat asettaa digi- ja kyberriskit oikeaan suhteeseen.

Liiketoiminnot on priorisoitu huomioiden tuki kriittiselle kansalliselle infrastruktuurille, tai muille kansallisille eduille, joilla vastataan yhteiskunnan asettamiin vaatimuksiin.

Yritys ymmärtää, miten tekniset järjestelmät, prosessit, tai resurssit edistävät tavoitteiden saavuttamista, sekä luovat kilpailuetua.

Nimetyllä vastuujohtajalla on pääsy hallitukseen ja johtoryhmään, riittävä toimivalta, aiheen hallinta, kokemus ja resurssit tehtävien hoitamiseksi.

Hallitus varmistaa, että organisaatiosta tehdään vuosittain virallinen riippumaton digi- ja kyberturvallisuusturvallisuuskatselmus.

Kortti 2: Luotettava ja uskottava digi- ja kyberriskianalyysi ja riskienhallintajärjestelmä

Ohjaavat kysymykset

Saavatko hallituksen ja johtoryhmän jäsenet säännöllisen päivityksen yrityksen digi- ja kyberkypsyydestä, riskialttiudesta ja riskitilanteesta, sekä toimeenpanotilanteesta?

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 määrittelee yrityksen selviytymiskykyä koskevan strategian ja siihen liittyvien riskien / riskitason?

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 liiketoiminnan kannalta, kuten liiketoiminnan häiriöt, tai vaikutuksen tuotteen/palvelun laatuun, tai maineeseen.

Yritys kykenee hallitsemaan digi- ja kyberturvallisuuden, suunniteltuun liiketoimintaan, tai teknologiaan tehtyjen muutoksiin liittyen.

Yrityksen toimintaa arvioidaan, tai auditoidaan sisäisesti ja ulkoisesti.

Yritys on sertifioitu, edistämään kilpailuetua ja osoittamaan vastuullisuutta.

Yritys viestii riskeistä ja niiden seurauksista omalle henkilöstölle ja sopimuskumppaneille.

Kortti 3: Strateginen kyberjohtamisen konsepti osana liiketoimintastrategiaa

Ohjaavat kysymykset

Tekevätkö yrityksen eri osat sisäistä yhteistyötä (esim. muiden liiketoimintayksiköiden 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 syntyä sen liiketoiminnan, tai teknologian suunniteltujen muutosten seurauksena?

Tehtävälista, varmistettavat asiat

Tunnistetaan ja huomioidaan toimintaympäristön muutoksesta johtuvat tekijät omalle liiketoiminnalle ja turvallisuudelle.

Käytetään hyväksi havaittuja ja liiketoiminnan turvallisuutta edistäviä vakioituja ja standardoituja toimintatapoja.

Valitaan ja hallitaan liiketoimintakehittämistä hyödyntäviä teknologioita perustellusti.

Otetaan huomioon kyberturvallisuuden kattava rakentaminen edellyttäen toimenpiteitä yrityksen strategisella, operatiivisella ja teknillisellä/taktillisella tasolla.

Kortti 4: Oikeasuhtainen digi- ja kyberturvallisuuden resursointi

Ohjaavat kysymykset

Kuinka suuri osuus vuotuisista toimintamenoista käytetään yrityksen jatkuvuuden hallintaan, ja miten tämä vertautuu itseasetettuihin 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 digitalisaation turvallisuuden vaikutukset huomioiva prosessi kokonaisbudjetin muodostamiseen.

Hallituksella on kyky ymmärtää digi- ja kyberturvallisuusriskien vaikutuksia ja sitä, miten ne voivat olla erilaisia suhteessa yrityksen eri tavoitteisiin riskien ja kyberturvallisuustoimenpiteiden operatiivisten kustannusten/vaikutusten tasapainottamisessa.

Käytettäessä kybervakuutusta on sen kustannukset huomioitava.

Digitalisaation ja sen turvallisuuden investointien hyödyt on mitoitettu.

Kortti 5: Oikeat ja innovatiiviset teknologiavalinnat ja niiden toimintakyvyn seuraaminen

Ohjaavat kysymykset

Onko yrityksen strategiassa määritetty tavoitteet digi- ja kyberteknologian hyödyntämisestä liiketoiminnan ja yrityksen hallinnon osalta?

Onko yrityksellä käytössä prosessi digisietokyvyn arvioimiseksi sellaisten kolmansien osapuolten kanssa, jotka voivat hallita tieto- tai teknologiaresursseja?

Tehtävälista, varmistettavat asiat

Digitalisaation tavoitteet on määritetty (esim. yrityksen digitalisaatioaste). Ennen tavoitteiden asettamista tulee käydä läpi erilaiset teknologiat, niiden mahdollisuudet ja käyttöön liittyvät kyberuhat ja muut riskit (esim. alustapalvelut, pilvipalvelut, tekoälymahdollisuudet, 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 liiketoimintatavoitteiden saavuttamiseksi.

Yrityksessä on suunnitelma teknologioiden käyttämisestä toiminnan kehittämisessä ja niiden toimeenpanosta.

On varmistettu, että valittu teknologia tukee liiketoiminnan kehitystä digi- ja kyberturvallisesti.

On laadittu edellä mainittua analyysia vastaavat turvallisuus- ja kumppanuussopimukset.

Ohjaavat prosessit tuottavat yritykselle strategian, riskienhallinnan, toimintaympäristöanalyysin ja resurssit sekä toteuttavat muutosten hallintaa.

Hallinnolliset prosessit tukevat yrityksen päätöksentekoa ja viestintää muita prosesseja korkeammalla tasolla.

Kortti 6: Kokonaisvaltainen ja ajantasainen varautuminen ja jatkuvuuden hallinnan suunnittelu

Ohjaavat kysymykset

Onko yrityksellä käytössä liiketoiminnan jatkuvuussuunnitelmat, toipumissuunnitelmat, sisältäen viestintä, tietoturvaiskujen torjunta ja -häiriöiden torjunta?

Miten digitaaliset järjestelmät on suojattu? (esim. tekniset ratkaisut)

Miten turvallisuus on todennettu? (esim. auditoinnin, tunkeutumistestaus)

Tehtävälista, varmistettavat asiat

Vastuu näistä suunnitelmista on yrityksen johtoryhmällä.

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 määritetty henkilö, joka vastaa lakisääteisistä ja sääntelyvaatimuksista (ymmärtämisestä) eri lainkäyttöalueilla, joilla yritys toimii maailmanlaajuisesti, ja miten nämä vaatimukset sisällytetään suunnitelmiin.

Kortti 7: Hyvin koulutettu ja harjoitettu kriisijohtamisorganisaatio sekä kriisiviestintäsuunnitelma

Ohjaavat kysymykset

Saavatko hallituksen tai johtoryhmän jäsenet riittävän perehdytyskoulutuksen digitalisaatioon ja kyberturvallisuuteen ottaessaan vastaan uuden tehtävän?

Onko yrityksellä säännöllinen koulutus- ja harjoitusohjelma, jolla heidän tiedot ja taidot päivitetään viimeisimmistä turvallisuustapahtumista?

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 tarjoa uhkatekijöitä yritykseen päin?

Tehtävälista, varmistettavat asiat

Yrityksen toimintamalli ja tehtävät ovat hallituksen hyväksymät.

Kriisinjohtamisorganisaatio on koulutettu ja harjoitettu säännöllisesti, painopiste esimerkiksi riskianalyysin perusteella.

Organisaatiolla on jatkokoulutus- ja harjoitussuunnitelma.

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.

Viestinnän roolit on nimetty ja tehtävien hoitajat harjoitettu.

Yrityksen viestintä eri kanavissa on säännöllistä.

Maineenhallinta on huomioitu viestintäsuunnitelmassa.

Kortti 8: Koko henkilöstön asianmukaiset digi- ja kybertaidot, sekä osaaminen

Ohjaavat kysymykset

Saavatko yrityksen uudet työntekijät riittävän perehdytyskoulutuksen yrityksen digitalisaatioon ja sen turvallisuuteen?

Onko yrityksellä säännöllinen koulutus- ja harjoitusohjelma, jolla heidän tietojansa ja taitoja päivitetään viimeaikaisista uhkista ja suuntauksista (tilanneymmärryksen kehittyminen)?

Tehtävälista, varmistettavat asiat

Yrityksen tavoitteiden saavuttamiseen ja riskien hallitsemiseen tarvittavat taidot määritetty.

Työtehtävien vaatimat valmiudet ja osaamistasot on määritetty koulutussuunnittelun pohjaksi.

Työntekijöille on annettava osaaminen sietokyvystä oman työtehtävän mukaisesti.

Koulutusohjelma varmistaa säännöllisen tietojen ja taitojen ylläpidon ottaen huomioon muuttuvan toimintaympäristön asettava vaatimukset.

Koulutusohjelma sisältää yrityksen jatkuvuuden toimintamallit, sekä teknologioiden käytön ja poikkeustilanteiden toimintamallit.

Koulutuksen taso arvioidaan säännöllisillä harjoituksilla.

Kortti 9: Vaatimukset täyttävät ydinprosessit ja toimintatavat liiketoiminnan kehittämiseen

Ohjaavat kysymykset

Onko yrityksellä käytössä prosessi ja toimintatavat liiketoiminnan kehittämiseen, jolla voidaan tunnistaa myös tieto- tai teknologiaresursseja?

Onko yrityksen ydinprosessit määritetty liiketoiminnan ja yrityksen hallinnon osalta?

Onko keskeiset yhteistyötahot/ulkoistukset/alihankkijat/sopimustahot tunnistettu?

Mitä ulkoistussopimuksissa on sovittu tietoturvasta, jatkuvuudenhallinnasta, turvallisuussopimuksista?

Miten asiakastietoja hallitaan oman maineen ja asiakkaan/sidosryhmän kannalta?

Tehtävälista, varmistettavat asiat

Yrityksen liiketoiminnalliset tavoitteet ohjaavat liiketoimintaprosessin toimintoja.

Operationaaliset prosessit ovat kehittyneet turvallisiksi asiakkaille tehtävien tuotteiden ja palveluiden toteuttamiseksi.

Tukiprosessit mahdollistavat operationaaliset prosessit, esimerkiksi henkilöstöresurssien, järjestelmien, tai kirjanpidon avulla.

Hallitaan yritysostot ja niihin liittyvät kyberriskit. (Cyber Due Diligence merkittävissä tapauksissa, jos dataa ja/tai järjestelmiä siirtyy oston mukana)

Kortti 10: Joustava ja kehittyvä digi- ja kyberkulttuuri

Ohjaavat kysymykset

Onko varmistettu, että työntekijät kokevat voivansa vaikuttaa yrityksen digitalisaatioon, kyberturvallisuuteen ja että heillä on mahdollisuus tuoda esiin näihin liittyviä epäkohtia?

Ovatko hallituksen ja johtoryhmän jäsenet sitoutuneet digi- ja kyberturvallisuutta koskeviin päätöksiin, noudattavatko ne 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

Yrityksen hyvä turvallisuuskulttuuri koostuu digitalisaatioon liitetyistä toimintatavoista, työmoraalista, yhteisistä säännöistä ja ehdoista sekä työntekijöiden välisistä vuorovaikutustavoista.

Digitalisaation ja kyberturvallisuuden tuomat muutokset on käsitelty hyvässä hengessä, käsittäen yhteiset tavoitteet, työtehtävät ja vastuualueet, sekä pelisäännöt ja toimintatavat.

Yrityksen henkilöstö tietää, miten ja kenelle epäkohdista tai poikkeamista voi raportoida. He myös kokevat olevansa kannustettuja raportointiin.

Henkilöstö ei pelkää negatiivisia seurauksia raportoidessaan epäkohdista tai poikkeamista.

Henkilöstö kokee voivansa kyseenalaistaa toimintamalleja rakentavalla tavalla, hyödynnetään henkilöstön kyvyt, taidot ja luovuus.

Henkilöstön näkemyksiä hyödynnetään aidosti digi- ja kyberturvallisuuskäytäntöjen suunnittelussa ja muutoksessa.

Henkilöstö ymmärtää digi- ja kyberturvallisuuden tärkeyden ja merkityksen organisaatiolle. 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.

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

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.

Deloitte, Yritysvastuu alihankintaketjun vastuullisuus, https://www2.deloitte.com/fi/fi/pages/risk/articles/yritysvastuu-alihankintaketjun-vastuullisuus.html

Fujitsu, Customer-first security: What it is and best practices for success, Fu-jistu_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, Tietoturvastrategia ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa, Jyväskylän yliopisto, 2021, pro gradu.

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

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