BOARDMAN

Digiturvallisuus

Omistajien, hallituksen ja johdon vastuut

DigiSignaali23

Ari Virtanen, Boardman

Esittäytyminen

Ari Virtanen

2022 –	Boardman, Partner
2021 –	Granarium Advisors, Founder & CEO
2019 – 2021	IMS Talent, Partner
2016 – 2019	Ensto, President and CEO
2011 – 2016	KONE, SVP People Flow Solutions
2008 – 2011	Elektrobit, EVP Wireless Solutions (currently Bittium)
2005 – 2008	Nokia Multimedia, VP Maemo/Meego (=Linux business)
1989 – 2005	Nokia Networks (Telenokia), from trainee to VP

- Board Member positions

- Chairman of Boardman's Renewal Forum

Boardman

Boardman on ajatuspaja ja osaamisverkosto, jolla on keskeinen rooli suomalaisen omistajuuden, hallitustyöskentelyn ja johtamisen (OHJ-ketjun) kehittämisessä.

Boardman-osaamisverkostoa hallinnoi voittoa jakamaton Boardman Oy, jonka omistaa 60 partneria.

Luomme ja jaamme uutta tietoa omistajien, hallituksen ja johdon päätöksenteon tueksi.

Toimintatapoina:

- Hallitusarvioinnit ja tilannekuva-analyysit
- Valmennukset
- Jäsen- ja kehittämisfoorumitoiminta
- Tapahtumat
- Julkaisut

BOARDMAN

Agenda

- Kyberturvallisuus
- Kyberturvallisuuteen liittyviä uhkia
- Lyhyesti lainsäädännöstä
- Omistajien, hallituksen ja johdon roolit & vastuut
    - Kirkkaan tilannekuvan merkitys
    - Kyberturvallisuusstrategian rakentaminen
    - Kyberturvallisuusriskien tunnistaminen ja tarvittavien toimintatapojen rakentaminen
- Yhteenveto

BOARDMAN

”Jos kyberrikollisuus olisi valtio, se olisi maailman kolmanneksi suurin talous USA:n ja Kiinan jälkeen”

(IBM)

BOARDMAN

”Suomalaiset menettivät nettirikollisille yli 32 miljoonaa euroa vuonna 2022.”

(Varo, varmista, varoita – kampanja)

BOARDMAN

Juonipaljastus

Kyberturvallisuudesta huolehtiminen on yhtä tärkeä osa hallituksen ja johdon työtä kuin esimerkiksi tuloskehityksen varmistaminen.

BOARDMAN

Kyberturvallisuus

- Nykyisin lähes jokaisen organisaation keskeiset toiminnot ovat digitaalisten ratkaisujen varassa.
- Digitaalinen turvallisuus eli kyberturvallisuus on yhä keskeisempi osa yrityksen kokonaisturvallisuutta, ja se on sulautettava koko yrityksen toimintaan.
- Kyberturvallisuus käsittää tietoturvallisuuden sekä jatkuvuuden hallinnan ja varautumisen. Kyse on järjestelmien, ohjelmistojen, laitteiden ja verkkojen suojaamisen lisäksi myös liiketoimintaprosesseista sekä ihmisten käyttäytymisestä ja asenteesta.
- Hyvin rakennettu kyberturvallisuus suojaa yrityksen toimintakykyä, varmistaa palvelun laadun ja turvaa liiketoiminnan jatkuvuuden.

Lähde Teknologiateollisuus

BOARDMAN

Kyberturvallisuuteen liittyviä uhkia

- Kyberrikollisuuden määrä ja maailmanlaajuiset kustannukset nousevat nopeasti, mikä johtuu hyökkäysten toteuttamiskustannusten laskusta.
- Kyberuhat ovat haitallisia tapahtumia tai kehityskulkuja, jotka voivat vaikuttaa organisaation toimintaan, talouteen, sen hallussa olevaan tietoon ja pahimmillaan jopa liiketoiminnan jatkuvuuteen.
- Tyypilliset haavoittuvuudet:
    - **Tietojenkalastelun** tavoitteena on saada rikollisten haltuun käyttäjätunnus- ja salasanapareja tai muita käyttäjälle tai organisaatiolle arvokkaita tietoja.
    - **Haittaohjelmat** ovat tietokoneohjelmia, jotka aiheuttavat ei-toivottuja tapahtumia tietojärjestelmässä tai sen osissa.
    - **Kiristyshaittaohjelmat** lukitsevat tiedostoja tai koko laitteen vaatien lunnaita näiden lukkojen avaamiseksi.
    - **Palveluestohyökkäyksessä** verkkoa kuormitetaan ylimääräisellä tietoliikenteellä. Tavoitteena on lamaannuttaa jokin palvelu- tai tietojärjestelmä.

BOARDMAN

Lyhyesti lainsäädännöstä

- **Osakeyhtiölaki** 2006/624 § 8: ”Yhtiön johdon on huolellisesti toimien edistettävä yhtiön etua.”

- Euroopan Unionin **yleinen tietosuoja-asetus** (GDPR) mahdollistaa sanktiot säännösten rikkomisesta ja korvaukset tietosuojavahingoista.

- Toimialakohtaiset kyberturvallisuuden lakisääteiset vaatimukset koskevat yrityksiä kasvavassa määrin.
    - Näistä keskeinen on EU:n verkko- ja tietosuojadirektiivi NIS (Network and Information Security), joka otettiin käyttöön vuonna 2016.
    - **NIS2-direktiivi** tulee asettamaan yrityksille uusia vaatimuksia liittyen kyberriskien tunnistamiseen, raportointiin ja yhteistyöhön kansallisten viranomaisten ja muiden asianosaisten kanssa. Se tulee korvaamaan alkuperäisen NIS-direktiivin Suomessa 18.10.2024.

BOARDMAN

Omistajien, hallituksen ja johdon roolit & vastuut

BOARDMAN

Vastuunjako pätee myös kyberturvallisuuden johtamiseen

BOARDMAN

Kirkkaan tilannekuvan merkitys

- Digitalisaatio muuttaa liiketoimintaympäristöä kiihtyvällä vauhdilla.
- Yritysten lähes kaikki toiminta on digitaalisten ratkaisujen varassa.
- Toimintaympäristön trendien jatkuva seuranta ja yritykselle relevanttien tulevaisuuden skenaarioiden jatkuva ylläpitäminen on olennaisen tärkeätä.
- Hallitusten agendoilla toimintaympäristön seurannalle on syytä varata entistä enemmän aikaa.
- Operatiivinen johto tuntee liiketoiminnan kannalta keskeiset digitaaliset järjestelmät ja vastaa siitä, että kyberriskit ja niiden mahdolliset vaikutukset raportoidaan hallitukselle.

- Kaikkia liiketoimintaympäristön muutoksia ei kuitenkaan ole mahdollista ennakoida, minkä vuoksi OHJ-ketjun yhteisen tilannekuvan jatkuva ylläpitäminen on keskeisen tärkeätä, jotta nopeita toimenpiteitä voidaan tarvittaessa tehdä. Tässä työssä tilannekuva-analyysi on hyvä työkalu.

BOARDMAN

Kyberturvallisuusstrategian rakentaminen

- Kyberturvallisuus on nähtävä koko yritystä koskevana strategisena asiana, eikä pelkkänä teknologiahaasteena.
- Hallituksen ja johdon yhteistyönä tehdään kyberturvallisuusstrategia, joka on linjassa omistajan linjausten ja yrityksen liiketoimintastrategian kanssa.
- Hallituksen tehtävänä on varmistaa strategian toteuttamisen vaatimat resurssit, kuten budjetti ja osaamiset.
- Hallitus varmistaa, että kyberriskien sietokyky on yrityksen yleisen riskinottohalukkuuden mukainen.
- Hallituksen ja johdon osaamisia pitää arvioida jatkuvasti, pitäen mielessä kyberturvallisuus yhtenä keskeisenä osaamisalueena. Tässä työssä hallituksen ja johdon arviointi on hyvä työkalu.

BOARDMAN

Kyberturvallisuusriskien tunnistaminen ja tarvittavien toimintatapojen rakentaminen

- Strategisten ja operatiivisten riskien tunnistaminen on tyypillisesti osa hallituksen vuosikellon mukaista toimintaa.
- Riskikartoituksessa on huomioitava kyberturvallisuusriskien huolellinen tunnistaminen ja tarvittavien toimenpiteiden suunnittelu.
- Hallituksen on varmistettava, että johto valmistelee kyberturvallisuuteen liittyvät ohjeet ja prosessit, jotka myös pidetään ajan tasalla.
- Erityistä huomiota tulee kiinnittää kyberriskien nopeavaikutteisuuteen, minkä vuoksi myös ennakointi-, reagointi- ja korjausliikkeiden pitää olla totuttua nopeampia.
- Johdon on arvioitava tarve kansainvälisen tietoturvastandardin ISO 27001 mukaisen sertifioidun tietoturvallisuuden hallintajärjestelmän toteuttamiselle.
- Koko henkilöstön tietoisuutta digitaalisesta turvallisuudesta on lisättävä koulutuksen ja parhaiden käytäntöjen jakamisen avulla – luotava kyberturvallisuuskulttuuri.
- Kyberturvallisuuden seurantaan on rakennettava yritykselle relevantit mittarit ja niiden raportointi.

Yhteenveto

- **Kyberturvallisuudesta huolehtiminen on yhtä tärkeä osa hallituksen ja johdon työtä kuin esimerkiksi tuloskehityksen varmistaminen.**
- Hallituksen tulee varmistaa, että yrityksen strategia sisältää kyberturvallisuuden ja että riskikartoituksessa huomioidaan kyberriskit.
- Hallitus varmistaa, että kyberriskien sietokyky on yrityksen yleisen riskinottohalukkuuden mukainen.
- Operatiivinen johto tuntee liiketoiminnan kannalta keskeiset digitaaliset järjestelmät ja vastaa siitä, että kyberriskit ja niiden mahdolliset vaikutukset raportoidaan hallitukselle.
- Hallitus ja johto vastaavat yrityksen varautumis- ja kriisinhallintasuunnitelmista.
- Hallitus ja johto luovat edellytykset avoimelle kyberturvallisuuskulttuurille.
- Kirkkaan tilannekuvan ja ennakoinnin merkitys korostuu koko ajan.

”Peruutuspeilistä tuulilasinäkymään”

BOARDMAN