



Digitalisoitu työelämä ja kyberturvallisuus

Raportin tekijät: ABB, Beweship, Cyberwatch, Danske Bank, DB Schencker, Ensto, Finnair, FISC, Fortum, F-Secure, Konecranes, Kreab, SOL, Staffpoint, Telia, Valmet, VTT & Elinkeinoelämän keskusliitto EK



Digitalisoitu työelämä ja kyberturvallisuus - koko tarina

Digitalisaatio muuttaa työnteon ja elämisen totuttuja tapoja. Digitaalisten työkalujen ja nopeiden internet-yhteyksien ansiosta paikkariippumaton etätö on jo arkipäivää, ja jopa monet etäältä tehdyt toimenpiteet onnistuvat vaikeuksitta. Koronapandemia on nopeuttanut perinteisen toimistotyön muutosta hybridityöskentelyksi, jossa työtä tehdään sekä etänä että paikan päällä. Tähän muutokseen sisältyy myös haasteita. Uudet työnteon tavat edellyttävät uudenlaisia johtamistaitoja – miten johdetaan ihmisiä, joita ei nähdä päivittäin? Miten viestintä ja tiedon jakaminen kannattaa järjestää? Onko meillä riittävät taidot ja kyvyt pärjätä digitalisaation mukanaan tuomissa nopeissa muutoksissa ja kilpailussa? Kuinka tietoturvallista toimintamme on ja miten kohtelemme

arkaluonteisia tietoja? Onko kyberturvallisuus olennainen osa digitaalista työntekoa ja jos ei, niin miten asia voidaan korjata? Yhä enemmän tärkeitä tietoja sijaitsee digitaalisena, mutta miten ne voidaan suojata? Tärkeintä on johtaa digitalisaatiota ja siirtymää hybridityöhön sujuvimalla ja tietoturvallisimmalla tavalla.

Kehityksen kärjessä pysyminen edellyttää, että uusia liiketoimintamalleja ja tehokkaita työtapoja kehitetään nopeasti. Se taas edellyttää muutosta perinteisissä johtamismalleissa ja -järjestelmissä. Digitaalinen ympäristö ei voi korvata ihmisten keskinäistä vuorovaikutusta, joten digitaalisessa työelämässä on äärimmäisen tärkeää vaalia ihmis-kohtaamisia ja hyvinvointia.





Vaasan yliopistossa on tutkittu etätyötä ja etätyöläisten hyvinvoinnin tukemisen tapoja. Tutkimuksessa tunnistettiin kolme osa-aluetta, joilla hyvinvointia on kehitettävä: henkinen, ruumiillinen ja sosiaalinen taso. Digital Game Changers -projektiin osallistuvissa suomalaisissa edelläkävijäryityksissä ollaan samaa mieltä.

On myös pidettävä mielessä, että digitalisaatio ei ole kestävä kehityspolku ilman kyberturvallisuutta. Kyberturvallisuus on digitalisaation erottamaton ja olennainen osa. Turvallisuutta ei voi lykätä toteutettavaksi ”sitten joskus”. Turvallisuuden on oltava sisäänrakennettuna kaikessa kehitystyössä, olipa kyse digitaalisista innovaatioista tai hybridityöskentelystä.

Digital Game Changers -ryhmä on tunnistanut viisi pääteemaa, joista digitaalinen työskentelytapa koostuu. Teemat esitellään tarkemmin jäljempänä tässä raportissa.

” Avainsanomamme on, että digitaalinen työelämä ja kyberturvallisuus ovat ratkaisevan tärkeitä liiketoiminnan mahdollistajia, ja siksi niiden oltava korkealla sijalla yritysten johdon strategiakeskusteluissa ja toiminnassa.

Teemat ovat:

1. johtajuudella aikaansaatu kulttuurinen muutos
2. uudet disruptiiviset ja ketterät liiketoimintamallit
3. henkilöstön jatkuva täydennys- ja uudelleenkorutus
4. innovaatiot ja yhteistyö ekosysteemeissä
5. teknologia ja infrastruktuuri

Tämä raportti perustuu Digital Game Changers -projektiin osallistuneiden edelläkävijäryitysten tekemään työhön. Ryhmä työsti Digitalisoitu työelämä ja kyberturvallisuus -aihekokonaisuutta puoli vuotta. Työn tulos perustuu ryhmätyöistuntoihin ja osallistujien parhaiden käytäntöjen jakamiseen. Digital Game Changers -projektin tavoite on pitää suomalaiset yrityksen digitalisaation tuomien muutosten terävimmässä kärjessä, ja siksi osallistujayritykset haluavat kertoa löydöksistään, jotta muutkin yritykset voivat liittyä eturivin yritysten joukkoon. Suomalaisen yritysten menestys on kaikkien etu.



Menestyksen osatekijät

Kyberturvallinen digitaalinen työelämä

Johtajuudella aikaansaatu kulttuurinen muutos

- Muutos johtajuudessa sekä johtamis- ja ajattelutavoissa
- Jatkuva tavoitteiden asetanta ja seuranta
- Ketterä tulosjohtaminen
- Kyberturvallisuus strategisena tekijänä ylimmän johdon ja hallituksen asialistalla
- Strateginen tilannekuva kyberturvallisuudesta
- Hybridityöskentely

Uudet disruptiiviset ja ketterät liiketoimintamallit

- Joustavat ja sopeutuvat mallit
- Muutosvoimana kestävä kehitys
- Organisaation prosessit sovitettu digitaaliseen maailmaan
- Turvallisuus sisäänrakennettu kaikkiin prosesseihin ja järjestelmiin
- Digitaaliset ratkaisut mahdollistajina

Henkilöstön jatkuva täydennys- ja uudelleen koulutus

- Elinikäinen täydennys- ja uudelleen koulutus
- Itsensä johtamiseen tarvittavat taidot ja asenne
- Kyky omaksua uusia asioita ja työkaluja
- Digitaalinen ja kyberturvallisuusosaaminen kaikilla tasoilla
- Globaalit osaajavarrannot ja paikkariippumaton työ

Innovaatiot ja yhteistyö ekosysteemeissä

- Uusi ketterä organisaatiokulttuuri, epäonnistu nopeasti
- Ekosysteemien kasvava tärkeys
- Uudet innovointia edistävät käsitteet ja työkalut
- Selkeät säännöt ja rutiinit: oikea-aikaiset kokoukset ja tehokkaat kokousmenettelyt
- Uusi kyberturvallisuuden kasvu- ja investointiohjelma

Teknologia ja infrastruktuuri

- Digitaalinen muutos alkaa työnkuluista, jotka yhdistävät ihmiset ja teknologian
- Kyberturvallisuus kriittisenä teknologisenä mahdollistajana
- Digitaaliset alustat, jotka mahdollistavat uudet liiketoimintamallit ja innovaatiot
- Kyberturvalliset yhteydet etätyössä
- Tekoäly ja automaatio

Edelläkävijäyritysten tunnistamat teemat digitaalisessa työelämässä ja kyberturvallisuudessa



1. Johtajuudella aikaansaatu kulttuurinen muutos

Ylimmän johdon on toimittava tiennäyttäjänä

Koronaviruspandemiasta seurannut nopea digitalisoituminen haastaa johtajuuden. Etä- ja hybridityö haastavat perinteiset johtajuusmallit ja edellyttävät muutosta ajattelutavoissa. Etätyössä on tuettava ihmisten välisiä kohtaamisia ja yhteyksiä. Työntekijät eivät saa kokea olevansa eristyksissä ja heidän on koettava, että organisaatio tukee heitä ja tarvittaessa tarjoaa apua. Tulosjohtamisen on oltava entistä ketterämpää ja kyettävä jatkuvaan tavoitteiden asetantaan ja seurantaan.

Hybridityöskentely edellyttää selkeitä periaatteita organisaatiossa. Nämä periaatteet on viestittävä huolellisesti koko organisaatiolle. Se edellyttää kaikkien osallistumista. Ketterien työtapojen ja kehityssprinttien omaksuminen auttaa organisaatiota pysymään kehityksen tasalla. Kokousten on oltava oikea-aikaisia ja tehokkaita, varsinkin esimiehen ja työntekijän välillä. Pulssikokoukset ja usein toistuvat kahdenkeskiset tapaamiset auttavat työntekijöitä pitämään työn tavoitteet mielessä samalla kun ne antavat esimiehelle tietoa työntekijän suoriutumisesta.

Työntekijän hyvinvointi on taattava myös hybridityöskentelyssä. Kasvokkain tapahtuvien kohtaamisten puuttuessa se voi olla haasteellista, sillä etätyöskentelyssä monet vaikeudet voivat jäädä huomaamatta. Työnantajien on varmistettava, että työntekijöillä on helppo pääsy terveydenhuoltopalveluihin, mielenterveyspalvelut mukaan lukien. Myös tehtyjen työtuntien määrää on seurattava, jotta se säilyisi kohtuullisena. Työnantajien on muistettava päivittää työuupumuksen, stressioireiden ja muiden terveysongelmien käsittelymallinsa hybridityöelämään sopivaksi.

Työnantajien on myös edistettävä organisaatiossaan luottamuksen kulttuuria ja henkistä turvallisuutta. Kun työntekijä kokee olevansa luotettu ja turvassa, hän suoriutuu paremmin. Se näkyy myös hybridityössä. Luottamus myös auttaa kertomaan ongelmista esimiehille jo aikaisessa vaiheessa ennen kuin niistä ehtii kasvaa suurempia ongelmia. Luottamusta tarvitaan myös yhteistyöyritysten kanssa työskennellessä. Tässäkin auttaa, jos organisaatiossa on luottamuksen kulttuuri.

Kyberturvallisuus on digitaalisen työelämän kulmakivi, eikä siihen saa suhtautua pelkkänä jälkikäteenä lisukkeena. Kyberturvallisuuden johtamisessa on olennaista tilannekuva, jonka on oltava ajan tasalla sekä julkisella että yksityisellä sektorilla, niin valtionhallinnossa kuin yrityksissä. Meillä on suhteellisen vankka kyky operatiivisen tilannekuvan luomiseen akuutin kyberturvallisuushkan ja haavoittuvaisuuksien ilmetessä, mutta Suomessa ei vielä analysoida kyberturvallisuusriskejä kansallisella tasolla. Yhdessä nämä kaksi kykyä tuottaisivat strategisen tason tilannekuvan, joka tukisi päätöksentekijäitä ja mahdollistaisi entistä luotettavammat, riskeistä tietoiset päätökset. Tämän aikaansaamiseksi tarvitaan yhteinen alusta, jonne kerättäisiin tietoja kyberturvallisuusmaailman ilmiöistä. Tietoja jaettaisiin sekä julkiselle että yksityiselle sektorille, mukaan lukien kolmannen sektorin toimijat. Uuden digitaalisen työelämän ja kyberturvallisuuden on oltava ylimmän johdon asialistalla päivittäin, eikä niitä saa jättää vain teknisten asiantuntijoiden huoleksi.



Suositukset yritysjohtajille: Määritä hybridityölle selkeät periaatteet ja säännöt yhteistyössä esimiesten ja työntekijöiden kanssa. Periaatteiden ja sääntöjen on katettava seuraavat osa-alueet:

1. Kuinka etä- ja hybridityöskentely muuttavat johtamista ja johtamisjärjestelmiä (kuten tulosjohtaminen, johtamisen foorumit, pulssikokousten tarve)?
2. Mitä periaatteita, sääntöjä ja sopimuksia tarvitaan etä- ja hybridityöskentelyyn (esim. kotona työskentelyn vakuutukset, ajanhallinta, yhteiset etätöön säännöt, mukaan lukien kyberturvallisuus)?
3. Mitä tietoja ja taitoja tarvitaan?
4. Millainen vaikutus etä- ja hybridityöskentelyllä on tarvittavaan toimistotilaan ja työpisteisiin ja miten monipaikkatyötä voidaan tehdä tehokkaasti?

Aseta hybridityöskentelylle selkeät ja mitattavissa olevat tavoitteet. Seuraa keskeisiä suorituskypsyindikaattoreita ja keskity pitämään tehokkaita pulssikokouksia, jotta olet jatkuvasti selvillä siitä, ollaanko tavoitteita saavuttamassa.

Varmista, että kyberturvallisuus on säännöllisesti hallituksen ja johtoryhmien asialistalla organisaation kaikilla tasoilla.

Hybridityöskentelyn mallit auttavat tasapainottamaan työajan ja vapaa-ajan, mikä auttaa perheitä tekemään arkielämästään sujuvaa. Hybridityöskentelyn mahdollisuuden tarjoaminen työntekijöille voi olla kilpailukykytekijä parhaiden osaajien houkuttelussa.



Suositukset päättäjille: Hybridi- ja etätöy vaikuttaa työlaainsäädäntöön ja työtä koskeviin sopimuksiin, koska paikallista joustavuutta tarvitaan enemmän. On tärkeää kehittää hybridityön käytäntöjä Suomessa.

Varmista, että sekä julkisella että yksityisellä sektorilla on yhteinen operatiivinen tilannekuva akuutin kyberturvallisuusuhan ja haavoittuvaisuuksien ilmetessä, ja että Suomessa analysoidaan kyberturvallisuusriskejä kansallisella tasolla. Kehitä yhteinen alusta, jonne kerätään tietoja kyberturvallisuusmaailman ilmiöistä. Tietoja jaetaan sekä julkiselle että yksityiselle sektorille, mukaan lukien kolmannen sektorin toimijat.



Suositukset työntekijöille: Tee oma osuutesi oman hyvinvointisi eteen. Keskity itsesi johtamiseen. Hae apua ja tukea. Tee oma osuutesi kyberturvallisuusasioissa. Käytä riittävästi aikaa (varo lankeamasta kiireellisyysansaan). Jos olet epävarma jostakin, kysy neuvoa.



Suositukset koulutuslalle: Digitaalisen työelämän ja kyberturvallisuuden on oltava osa tai moduuli kaikessa kaupallisen alan koulutuksessa ja johtamiskoulutuksessa.



2. Uudet disruptiiviset ja ketterät liiketoimintamallit

Suomi hyöttyy uusien mallien kehittämisestä

Digitalisaation myötä voidaan kehittää uusia liiketoimintamalleja. Tulevaisuudessa tarvitaan joustavia ja dynaamisia liiketoimintamalleja, jotka kykenevät sopeutumaan nopeasti asiakkaiden muuttuviin vaatimuksiin. Uudet liiketoimintamallit myös varmistavat, että organisaation kaikki prosessit ovat sopeutuneet digitaaliseen maailmaan. Uudet digitaaliset liiketoimintamallit ovat tulevan menestyksen perusta.

Kestävä kehitys ja vihreä siirtymä ovat muutostekijöitä, jotka lisäävät digitaalisten liiketoimintamallien tärkeyttä. Kestävät liiketoimintamallit tuovat etua markkinoilla. Organisaatioiden on kehitettävä kestävän kehityksen strategioita ja varmistettava, että niiden toiminnot yhtäältä täyttävät sääntelyn vaatimukset ja toisaalta lisäävät brändin ja työntekijäbrändin arvoa.

Kyberturvallisuus (kuten kaikki muutkin turvallisuuden ja riskienhallinnan osat) varmistaa osaltaan liiketoiminnan sujuvuuden ja sen tarvitseman luottamuksen. Digitalisaatio ei menesty eikä kehity kestävällä tavalla, jos turvallisuusvaatimuksia ei oteta huomioon. Turvallisuutta on pidettävä luonnollisena ja pakollisena osana kehitettyä prosessia, järjestelmää, tuotetta tai palvelua. Tämä toteutuu, kun turvallisuus on näiden sisäänrakennettu ominaisuus. Kyberturvallisuuden on oltava integroitu osa liiketoimintamalleja, ei pelkkä erillinen saareke. Innovaatioita on tuettava, jotta asiakkaiden jatkuvasti muuttuviin tarpeisiin voidaan vastata.



Suosituksat yritysjohtajille: On tärkeää sekä seurata liiketoimintamallien kehittymistä maailmanlaajuisesti yrityksen toimialalla että varmistaa, että yrityksen oma liiketoimintamalli on ajan tasalla. Työntekijöiden lisä- ja uudelleen koulutus ovat työkaluja, joilla voidaan luoda uusien mallien luontiin tarvittavaa pätevyyttä. Varmista, että kyberturvallisuus toteutuu kaikissa digitaalisissa prosesseissa ja järjestelmissä.



Suosituksat päättäjille: Varmista riittävä rahoitus tutkimus- ja kehitystyölle ja liiketoimintaohjauksille ekosysteemeille. Yhdessä olemme vahvempia, ja se koskee myös liike-elämää. Luo pysyvät rakenteet julkisen ja yksityisen sektorin yhteistyölle kyberturvallisuuspolitiikkojen ja -säädösten suunnittelussa ja laadinnassa.

Tietotaloutta ja omien tietojen käyttöä voi edistää omadatan avulla. Tämä kattaa henkilöt sekä julkisella että yksityisellä sektorilla.



Suosituksat työntekijöille: Huomioi kyberturvallisuus myös uusien innovaatioiden, työtapojen ja liiketoimintatapojen luonnissa.



Suosituksat koulutus alalle: Tue yrittäjyyttä ja tee yhteistyötä innovatiivisten start-up-yritysten kanssa.





3. Henkilöstön jatkuva täydennys- ja uudelleenkoulutus

Työelämän osaamisvaatimukset ovat suuremmassa muutoksessa kuin koskaan ennen

Digitalisoituneessa maailmassa tarvitaan erilaisia tietoja ja taitoja kuin ennen koronapandemiaa. Entistä tärkeämmäksi on noussut kyky oppia nopeasti ja sopeutua uusiin olosuhteisiin. Etä- ja hybridityön yleistyessä korostuvat myös itseohjautuvuustaidot: tehokas työnteko edellyttää omien työtehtävien johtamista. Hyvät itsensä johtamisen taidot myös auttavat priorisoimaan työtehtävät järkevällä tavalla. Muita tarvittavia taitoja ovat psyykkinen palautumis- ja sopeutumiskyky. Elinikäinen oppiminen, jatkuva täydennyskoulutus ja uudelleenkoulutus muodostuvat organisaatioissa yhä yleisemmiksi. Ajan tasalla olevat tiedot ja taidot lisäävät myös työntekijän markkina-arvoa.

Työpaikalla oppimisesta tulee jatkossa yhä tärkeämpää. Työssä oppiminen on suunnitelmallinen ja tavoitteellinen prosessi, jossa tietoja ja taitoja seurataan ja arvioidaan. Täydennyskoulutus ja uudelleenkoulutus ovat tärkeitä digitalisoituvassa maailmassa. Meidän on sopeuduttava jatkuvaan oppimiseen, ja tässä apuna ovat lisä- ja uudelleenkoulutus. Digitalisaation myötä myös osaajavarannoista tulee maailmanlaajuisia, jolloin myös rekrytointia voidaan tehdä maailmanlaajuisesti, sillä monissa työtehtävissä ja asiantuntijajäsenöissä sijainnilla ei ole merkitystä. Yrityksissä osaamisen hallinta ja oppiminen integroituvat.

Työntekijöiden tietämystä arkipäivän kyberturvallisuusperiaatteista, menettelytavoista ja

työtavoista on parannettava. Hybridityöskentelyssä työntekijöiden turvallisuustietämys ja turvalliset työtavat korostuvat entisestään, koska työntekijät eivät aina voi valita työskentely-ympäristöään ja sitä, kuka voi kuulla työhön liittyviä keskusteluja. Siksi työntekijöitä on koulutettava turvallisuusasioissa jatkuvasti. Se luo vankan pohjan kestäväälle turvallisuuskulttuurille.

Jokaisen on ymmärrettävä kyberturvallisuudesta vähintään perusteet, eli mitä kyberturvallisuus edellyttää minulta ammatissa toimijana tai kansalaisena. Kyberturvallisuustaidot on sisällytettävä kaikkiin koulutuksen tasoihin päiväkodista korkeakoulutasolle asti, unohtamatta työpajoilla tapahtuvaa koulutusta. Kyberturvallisuustaitojen on oltava ajan tasalla varsinkin koodaajilla, ohjelmistoarkkitehteillä ja kaikilla palveluiden, tuotteiden tai prosessien kehittämiseen osallistuvilla tahoilla. Tyttöjä ja naisia on rohkaistava valitsemaan urapolkuja kyberturvallisuuden alalla, koska turvallisuusasiat koskettavat kaikkia yhteiskunnan alueita.

Tämä tunnistetaan ehdotetussa kansallinen kyberturvallisuuden kehitysohjelmassa, jossa ehdotetaan, että nämä asiat otetaan osaksi opetus-sisältöjä kaikilla tasoilla päiväkodista ammattikoulutukseen, ammattikorkeakoulutukseen ja korkeakoulutukseen.

Suomessa tarvitaan sekä lyhyen aikavälin koulutusohjelmia että pitkän aikavälin koulutusta.



Nopeatempoisessa maailmassa ei voida odottaa vähintään viittä vuotta, että yliopistoista ja ammattikorkeakouluista valmistuu oikealla tietämyksellä varustettuja osaajia. Tarvitsemme uusia tapoja löytää ja tuoda yhteen ihmisiä, joiden osaaminen vastaa työtehtävän vaatimuksia. Yksi tapa hankkia lisää tietämystä ovat avoimet oppimisympäristöt, kuten suomalaisten yliopistojen äskettäin kehittämä FITech.

On tärkeää, että tietojen ja taitojen kehittäminen tehdään kestäväällä tavalla. Pelkkä opiskelijamäärien lisääminen ei ole kestävä ratkaisu, sillä pitkällä aikavälillä suomalaisia hakijoita ei riitä kaikkiin avoimiin paikkoihin. Meidän on lisättävä ulkomaalaisille opiskelijoille tarkoitettuja tutkinto-opiskelijapaikkoja, jotta Suomi voi ajan mittaan

hyötyä heidän osaamisestaan osana pätevää henkilöstöä. Ratkaisevan tärkeää parhaiden osaajien saannin varmistamiseksi on huippuosaajien aktiivinen rekrytointi ja houkuttelu ulkomailta Suomeen. Se tarkoittaa, että Suomeen on voitava asettautua helposti ja suhteellisen nopeasti, jotta Suomi olisi kilpailukykyinen globaaleilla työmarkkinoilla. Suomessa on jo joitakin aloja, kuten kyberturvallisuus, joilla tarvitaan kipeästi ulkomaisia osaajia.

Siksi oppiminen siirtyy yhä suuremmassa määrin työpaikoille ja jatkuvasta oppisesta tulee uusi normaali. Koulutuksessa on panostettava modulaariseen oppimiseen ja henkilöstön nopeaan täydennys- ja uudelleen koulutukseen, joka vastaa työelämän uusiin tarpeisiin.



Suosituksukset yritysjohtajille: Edistä työssä oppimista, koska työpaikka on se paikka, jossa uusia taitoja sovelletaan. Työssä tapahtuvan täydennys- ja uudelleen koulutuksen on oltava suunnitelmallinen ja tavoitteellinen prosessi, jossa taitoja seurataan ja arvioidaan. Kun varmistat, että työntekijöilläsi on tarvittavat tiedot ja taidot, yrityksessäsi on helpompaa omaksua ketterät työskentelymenetelmät, joilla saadaan aikaan laadukkaita tuloksia. Kehitä modulaarista ja mikro-oppimissisältöä, jotka täydentävät olemassa olevia oppimishajelmia ja koulutusta. Varmista, että kaikilla työntekijöilläsi on työtehtävän edellyttämä kyberturvallisuuskoulutus ja -taidot.



Suosituksukset päättäjille: Lisää rahoitusta elinikäiselle modulaariselle oppimiselle ja lyhyemmille oppimis-sprinteille, esimerkiksi mikro-oppimiselle. Oppisisältöjen on oltava saatavana verkossa digitaalisessa muodossa kattaen digitalisaatioon ja kyberturvaan liittyvät aiheet. Koulutuksen on vastattava koronaviruspandemian jälkeisen työelämän nopeasti muuttuviin vaatimuksiin. Varsinkin modulaarista kyberturvallisuuskoulutusta tarvitaan lisää. Paranna päättäjien ja viranhaltijoiden kyberturvallisuusosaamista.



Suosituksukset työntekijöille: Elinikäinen oppiminen on avain digitalisoituvassa maailmassa toimimiseen. Päivittäisessä työssä oppiminen on tärkein täydennys- ja uudelleen koulutautumisen tapa. Tämä lisää markkina-arvoasi työntekijänä.



Suosituksukset koulutuslalle: Koulutuksessa on panostettava lisää elinikäiseen modulaariseen oppimiseen sekä täydennys- ja uudelleen koulutautumiseen, joka vastaa työelämän tarpeisiin. Koulutuksen on vastattava työelämän tarpeisiin ketterästi ja elinikäistä oppimista tukevalla tavalla. Asiakastarpeisiin vastaavia opintokokonaisuuksia on kehitettävä tiiviimmässä yhteistyössä johtavien yritysten kanssa.





4. Innovaatiot ja yhteistyö ekosysteemeissä

Hybridityöskentely haastaa innovointia

Etätyö tekee innovoinnista haasteellista. Kun kasvokkaisia tapaamisia ei ole, tarvitaan uusia työkaluja. Uudet työkalut ja käsitteet mahdollistavat yhteistyössä tapahtuvan innovoinnin digitaalisessa ympäristössä. Myös organisaatiokulttuuria voidaan säätää tukemaan innovaatioprosesseja. Organisaation selkeät säännöt ja rutiinit tukevat innovaatiota. Oikea-aikaiset kokoukset ja tehokkaat kokouskäytännöt luovat ympäristön, jossa innovointi on mahdollista. On myös pidettävä mielessä, että kasvokkain tapaamiset ovat tärkeitä, eikä niitä voi kokonaan korvata digitaalisilla työkaluilla.

Meidän näkemyksemme mukaan kyberturvallisuus on yksi niistä aloista, joilla Suomi ja suomalaiset yritykset voivat olla globaaleja johtajia. Tämän aikaansaamiseksi meidän on kehitettävä kansallinen kyberturvallisuuden kasvu- ja investointiohjelma ja perustettava kansallinen kyberturvallisuuden kasvu- ja osaamiskeskus. Tästä hyötyisivät niin suomalaiset kyberturvallisuusyritykset kuin kaikki muutkin suomalaiset yritykset (PK-yritykset mukaan lukien), sillä teknologisten ja rahoitustarpeiden saattaminen yhteen kyvykkäiden yritysten kanssa tuottaisi tuotteita ja palveluita globaaleille markkinoille.

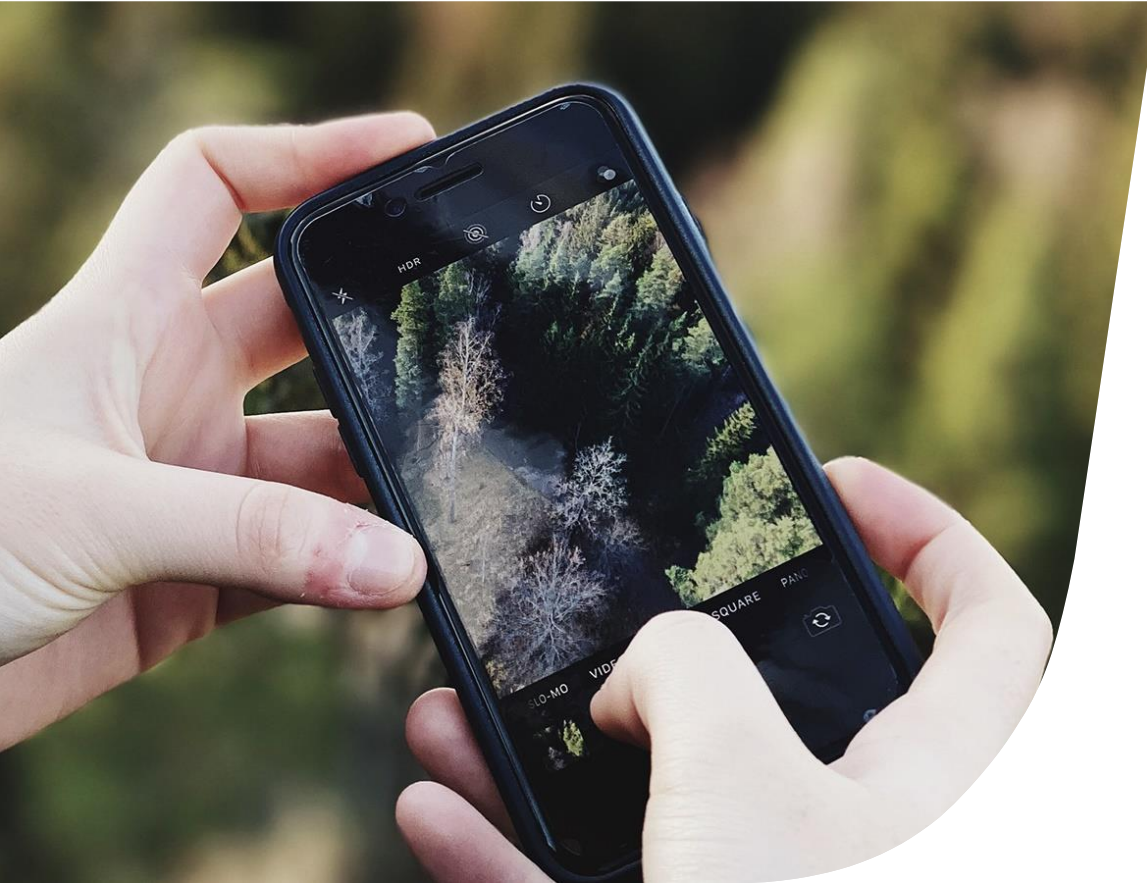
Kestävän kasvun ohjelmassa on keskityttävä erityisesti innovaatiotukemiseen, joissa yhdistyy kaksi vahvaa megatrendiä, ilmastonmuutos ja

digitalisaatio. Samassa yhteydessä on käytettävä nykyisiä rahoitusvälineitä ja kehitettävä niitä edelleen.

Innovaatioprosesseja voi tehostaa myös muodostamalla kumppanuus ekosysteemejä. Uudet yritysten ekosysteemit ovat tulevaisuuden työn tapa. Ekosysteemimalli edellyttää luottamusta ja ymmärtämystä kumppaniyritysten välillä. Osapuolten on koettava antamansa panoksen ja saamansa hyödyn suhde tasapainoiseksi. Projektin puitteiden laatiminen yhteistyössä antaa projektille sen tarvitseman uskottavuuden. Lisäksi ekosysteemi tarvitsee menestyäkseen hyvän fasilitaattorin. Ekosysteemien kehittämisen edellyttää myös uusia ja nykyistä joustavampia rahoitusinstrumentteja ja tukea julkiselta sektorilta.

Hyvä tapa tukea innovaatioita on ottaa käyttöön ketteriä liiketoiminta- ja yhteistyömalleja. Yksi esimerkki on aivoriihi ja yhteistyö start-up-yritysten kanssa. Näin suuremmat ja vakiintuneemmat yritykset voivat sopeutua start-up-yritysten ketterään työskentelytapaan ja start-upit taas hyötyvät suurempien yritysten kokemuksesta. Tällaisessa mallissa kaikki osapuolet hyötyvät.

Ketterän kulttuurin luominen organisaatioon on siis avain innovaatioiden synnyn tukemiselle. Uusi organisaatiokulttuuri tukee innovaatioita.



Suosituksset yritysjohtajille: Luo kulttuuri, joka tukee innovaatiota ja mahdollistaa verkottumisen ja tiedon jakamisen. Luo työskentelytapoja, jotka tukevat innovointia hybridimallilla toimivassa organisaatiossa. Varmista, että kyberturvallisuus otetaan huomioon jo innovaatioprosessin alkuvaiheissa.



Suosituksset päättäjille: Varmista, että valtion ylläpitämät TKI-ekosysteemit ovat tuottavia myös digitalisoituneessa maailmassa. Luo joustavia rahoitusmalleja ekosysteemien kehittämiseksi.

Laadi Kyberturvallisuuden kasvu- ja sijoitusohjelma yhteistyössä yritys- ja korkeakoulumaailman kanssa ja perusta kansallinen Kyberturvallisuuden kasvu- ja osaamiskeskus, joka tukee ja kehittää vahvaa kansallista kyberturvallisuusekosysteemiä, joka kykenee toimimaan globaaleilla markkinoilla.



Suosituksset työntekijöille: Ylläpidä omilla toimillasi ketterää organisaatiokulttuuria. Ole luova ja kokeile uusia ideoiden innovointi- ja kehitystapoja tiimissäsi.



Suosituksset koulutuslalle: Yliopistojen on pohdittava koulutussisältöjä uudelleen ja muutettava niitä tukemaan työelämän tarpeita. Yliopistojen on tehtävä aktiivisesti tutkimusta aiheissa, ovat liike-elämän kannalta merkityksellisiä pitkällä aikavälillä. Yliopistojen on myös tultava mukaan kumppanuusmalleihin, jotta vuoropuhelu yritysten välillä onnistuisi.





5. Teknologia ja infrastruktuuri

Teknologia on kaiken perusta

Digitaalinen toiminta ei onnistu ilman oikeaa teknologiaa ja infrastruktuuria. Teknologia ja osaaminen muodostavat digitalisaation perustan. Yksi tämän perustan kulmakivistä on kyberturvallisuus, joka on integroitava yrityksen strategiaan ja jonka on läpäistävä yrityksen kaikki prosessit ja järjestelmät. Digitaaliset ympäristöt yleistyvät ja niistä tulee myös erottamaton osa yrityksen liiketoimintamallia. Prosessien digitalisointi alkaa työnkuluista, jotka yhdistävät ihmiset ja teknologian. Kyberturvallisuus ei ole pelkkää tekniikkaa, sillä turvallisuus on tehokasta vasta kun se takaa

tietojen salassapidon, saatavuuden ja eheyden sekä kriittisten järjestelmien ja infrastruktuurin toiminnan ja luotettavuuden. Esimerkiksi tietojen turvaaminen edellyttää myös fyysisen turvallisuuden huomioimista.

Teknologia on liiketoimintamallien mahdollistaja, mutta mallien sisältö on peräisin itse liiketoiminnasta ja sen strategiasta. Vasta kun sisältö on kunnossa, voidaan kaikille prosesseille järjestelmille luoda vankka teknologinen perusta.



Suosituksset yritysjohtajille: Teknologia-arkkitehtuurin on tuettava liiketoimintaprosesseja ja niiden arkkitehtuuria. Liiketoiminnan tavoitteet on määritettävä ja ne on pidettävä mielessä koko teknologian kehitysprosessin ajan, jotta lopputulos olisi laadukas. Tarvittavien teknologisten palveluiden ja ratkaisujen riittävä rahoitus ja resurssit on varmistettava.



Suosituksset päättäjille: Hyvin toimiva ja turvallinen infrastruktuuri on kaikkien nykyaikaisten yhteiskuntien toiminnan edellytys. On tärkeää, että teknologiavalinnat tehdään poliittisten tavoitteiden ja valintojen perusteella ja että tarvittaville teknologisille palveluille ja ratkaisulle annetaan riittävät resurssit.



Suosituksset työntekijöille: Suhtaudu uuteen teknologiaan avoimesti ja osallistu organisaatiosi tarjoamiin koulutuksiin. Hyödyt paljon, jos omaksut uusia teknologioita aikaisin.



Suosituksset koulutuslalle: Panostakaa digitaalisiin oppimisympäristöihin ja -teknologioihin. Lisätty todellisuus voi auttaa oppimisessa ja tuoda yritysmaailmaan uusia taitoja.



Lisäksi: Digitalisaation tuomat muutokset haastavat työelämän käytännöt

Digitaalinen työelämä tuo monia haasteita, kuten uudenlaiset työkalut, työn tekemisen paikat ja työajat. Edellä mainitut viisi teemaa muuttavat totutut työnteon mallit ja tavat.

Kotona tai etänä työskenneltäessä työpäivä ei välttämättä ala yhdeksältä ja päätty viideltä. Työt saatetaan tehdä osittain päivällä ja osittain esimerkiksi iltaisin. Paikkariippumattomassa työssä ei useinkaan ole tärkeää, minä vuorokauden tunteina työt tehdään, kunhan tavoitteet saavutetaan määräajassa. Tulevaisuudessa monet työ-

hön liittyvät yksityiskohdat voidaan neuvotella paikallisesti.

Miltä työelämä näyttää koronapandemian jälkeen? Aika näyttää, mutta työaikalakia tulisi muuttaa vastaamaan nykypäivän työelämän vaatimuksia. Voi myös olla, että työehtosopimuksia muutetaan vastaavasti ja paikallinen sopiminen yleistyy. Näin myös työnteon malleja voidaan kehittää ketterästi vastaamaan digitaalista työelämää.



Suosituksset yritysjohtajille: Yrityksiä kehoitetaan lisäämään paikallista sopimista, koska se tuo lisää joustavuutta organisaatioon.



Suosituksset päättäjille: Asiantuntijatyössä koronapandemia teki hybridityöstä valtavirtaa. Työaikalakia on arvioitava uudelleen, jotta se vastaisi nykyaikaisen työelämän tarpeita.



Suosituksset työntekijöille: Ole aktiivinen organisaatiossasi ja anna palautetta siitä, mikä toimii ja mikä ei. Näin työelämästä tulee parempaa.



Tarkistuslista hybridityöskentelyä varten

Tarkistakaa organisaatiossanne seuraavat seikat, kun valmistaudutte hybridityöskentelyyn:

- ☒ Hybridityöskentelyn periaatteiden luominen
 - roolien ja vastuiden määrittäminen
 - etätöön ajankohtien ja paikkojen määrittäminen
 - kokouskäytännöt ja tavoitettavuus
 - turvallisuus, mukaan lukien kyberturvallisuus
 - hyvinvointi
- ☒ Ottakaa tiimit ja työntekijät mukaan kehitystyöhön.
- ☒ Laatikaa konkreettisia tarkistuslistoja.
- ☒ Kouluttakaa johtajat johtamaan hybridityöskentelyä.
- ☒ Valmistautukaa oppimaan kokemuksista ja sopeutumaan muuttuviin tilanteisiin.
- ☒ Muistakaa jakaa tietoa ja ylläpitää vuoropuhelua!

Tarkistuslista kyberturvallisuuden johtamista varten

- ☒ Luokaa organisaatioonne kattava ja vankka ymmärrys kyberturvallisuudesta.
- ☒ Varmistakaa riittävä kapasiteetti kyberriskien arviointiin ja hallintaan.
- ☒ Luokaa ketterä kybervalmius- ja jatkuvuussuunnitelma.
- ☒ Luokaa hyvin toimiva kyberkriisien hallinnan kyky.
- ☒ Saattakaa henkilöstön kyberosaaminen erinomaiselle tasolle.
- ☒ Hankkikaa huipputasoista kybertekniikkaa ja tehkää älykkäitä valintoja
- ☒ Varatkaa riittävä kyberbudjetti.
- ☒ Luokaa ketterä ja kattava kyberturvallisuuden kulttuuri.

