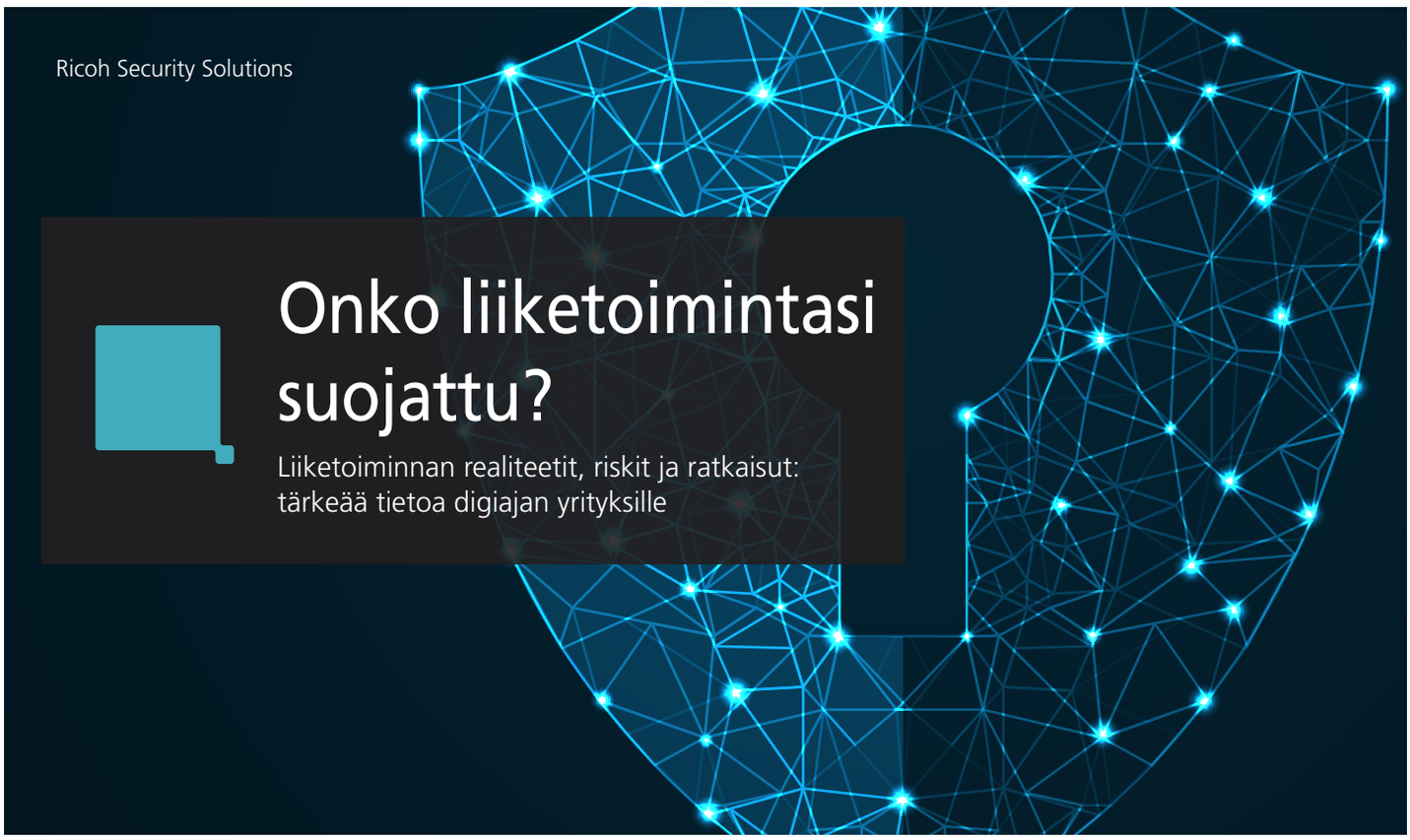
Ricoh Security Solutions



Onko liiketoimintasi suojattu?

Liiketoiminnan realiteetit, riskit ja ratkaisut: tärkeää tietoa digiajan yrityksille

Kyberturvallisuus on suurin haaste nyky-yritysten pärjäämiselle ja menestymiselle.

Kaikenkokoiset yritykset ovat jatkuvassa vaarassa joutua vahingollisten hyökkäysten, kuten tietojen kalastelun, palvelunestohyökkäysten tai kiristysohjelmien kohteeksi, ja näiden aiheuttamat kustannukset voivat nousta miljooniin. Lait ja säännökset, kuten EU:n yleinen tietoturva-asetus GDPR, rankaisevat yhä useammin lamaannuttavilla sakoilla niitä yrityksiä, jotka eivät onnistu turvaamaan järjestelmiään ja tietojaan asianmukaisesti. Nykyisen työympäristön digitalisaatio lisää kyberturvallisuushaasteita entisestään. Työnkulut kattavat entistä enemmän laitteita, verkkoja ja alueita, ja tietojen on oltava suojattuja niiden liikkuessa ympäri yritystä.

Samaan aikaan toimistojen tulostimien ja monitoimilaitteiden toiminnot ovat kymmenkertaistuneet viime vuosien aikana. Ne hoitavat nykyisin todella suuren osan liiketoimintaan liittyvien tietojen syötöstä, tulostuksesta, siirrosta ja tallennuksesta. Tämä saattaa tehdä näistä laitteista työpaikan vaarallisimpia, vaikkakin usein aliarvioituja, uhkatekijöitä.

Näiden haasteiden edessä yritysten täytyy varmistaa entistä tarkemmin asiakirja- ja tiedonhallintajärjestelmiensä turvallisuus – ja pystyä myös todentamaan se.

60 %

Viime vuonna suojaamattoman tulostuksen aiheuttamasta tietoturvahyökkäyksestä ilmoittaneet yritykset Euroopassa ja Yhdysvalloissa*

*Quocirca Enterprise MPS Study, 2017. Tiedot: 240 yli 500 työntekijän organisaatiota eri toimialoilta Isosta-Britanniasta, Ranskasta, Saksasta ja Yhdysvalloista.

€20m

Mahdollinen enimmäissakko yritykselle, joka ei noudata GDPR-asetusta*

*EU:n GDPR-portaalin tulevaa GDPR-asetusta koskeva UKK-osio sivustolla www.eugdpr.org/gdpr-faqs.html.

RICOH
imagine. change.

Neljä yrityksen suojaamisessa muistettavaa seikkaa

Ovatko tietosi turvassa?

- Tietojen tallennus
- Tietojen katoamisen ja varkauksien vaara
- Kyberhyökkäyksen vaara
- Muuttumisen ja vahingoittumisen vaara
- Ennakoimattomat tapahtumat

Todellisuus

Tietosi ovat yrityksesi arvokkain omaisuus. Vaikka voisikin olla helppo työntää pää pensaaseen erilaisten uhkien kuten tietovarkauksien, kyberhyökkäysten tai luonnonkatastrofien suhteen, suojaamattomuuden seuraukset voivat olla tuhoisia.

Riskit

- Kyberhyökkäys – Ricoh torjuu kuukausittain noin 8 miljardia palomuurihyökkäystä
- Liiketoiminnan keskeytyminen luonnonkatastrofin vuoksi
- Organisaation sisä- tai ulkopuolelta tapahtuvat tietovarkaudet

Onko asiakirjahallintasi turvallinen?

- Asiakirjojen jakaminen
- Asiakirjojen hävittäminen
- Laitehallinta
- Turvallinen tulostus

Todellisuus

Jokapäiväinen asiakirjojen jakaminen, tallentaminen ja tulostaminen voi merkitä myös tietoturvan vaarantamista. Vaatimaton toimistotulostin on usein aliarvioitu haavoittuvuus turvallisessa asiakirjahallinnassa.

Riskit

- Arkaluonteisten tietojen päätyminen vääriin käsiin suojaamattoman tulostuksen seurauksena
- Luottamuksellisten tietojen tuleminen julki epätäydellisen asiakirjan tai laitevahingon vuoksi
- Laitehakkerointi

Onko digitaalinen työpaikkasi turvallinen?

- Työnkulun hallinta
- Liikkuva työskentely
- Tietojen suojaaminen siirron aikana
- IT-infrastruktuuri

Todellisuus

Joustavuus ja liikkuva työ tuo monien etujensa ohella myös merkittäviä riskejä – miten vastaat BYOD-työympäristöjen (Bring Your Own Device) tuomiin haasteisiin? Onko julkinen langaton verkko epäluotettava? Päätyvätkö laitteet vääriin käsiin?

Riskit

- Yhtiön luottamuksellisten tietojen häviäminen joustavan työympäristön heikkojen lenkkien vuoksi
- Laitteiden käytön läpinäkyvyyden ja valvonnan puutteesta johtuvat tietoturvahyökkäykset

Täyttyvätkö kaikki säädökset?

- Säädösten noudattaminen
- EU:n tietosuoja-asetuksen (GDPR) noudattaminen

Todellisuus

Olemassa olevien lakisäädösten lisäksi EU:n tietoturva-asetus GDPR tulee voimaan toukokuussa 2018 – oletko valmis, ja miten voit varmistaa säädösten noudattamisen?

Riskit

- Merkittäviä sakkoja säädöksiä noudattamattomille yrityksille
- Maineen vahingoittuminen

Tietoturvauhkien ja uuden lainsäädännön vuoksi yrityksillä on entistä suurempi riski menettää sekä maineensa että suuri määrä rahaa. Nyt on oikea aika investoida digitaalisen työpaikan turvallisuuteen luotettavan kumppanin kanssa.

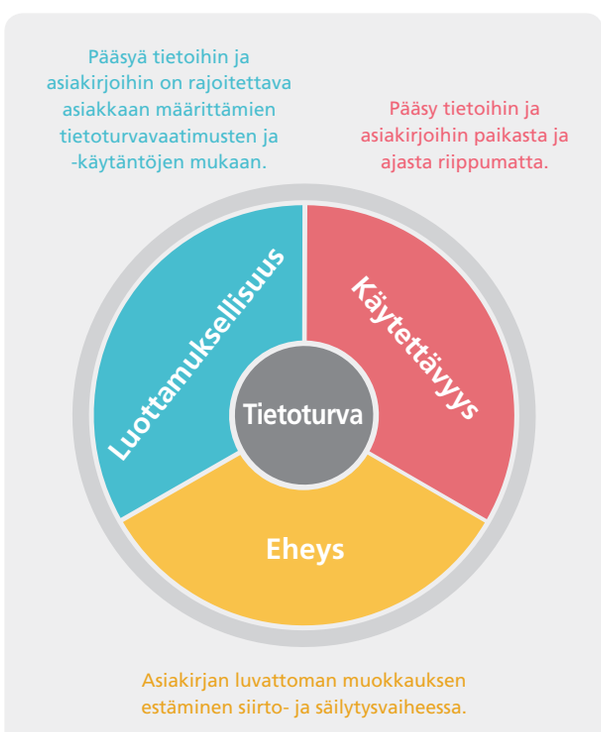
RICOH
imagine. change.

Hyvä uutinen on se, että Ricoh on miettinyt turvallisuusasiat valmiiksi puolestasi. Me olemme riskien ymmärtämisen asiantuntijoita, sillä olemme jo vuosikymmenten ajan kehittäneet keinoja niiden torjumiseen hyödyntäen vallitsevan teknologisen tason suojauskeinoja ja ratkaisuja koko valikoimassamme. Esimerkiksi tulostimissamme on ollut jo yli 20 vuotta käytössä turvallinen kiintolevyaseman päällekirjoitustoiminto. Turvallisuus on keskiössä koko digitaalisen työpaikan laitevalikoimassamme.

Ricoh tarjoaa asiakkailleen yhdenmukaisen maailmanlaajuisen palvelu- ja tukirakenteen, joka varmistaa uhkia koskevan ulkoisen tiedustelutiedon tehokkaan jakamisen ja käyttöönoton. IEEE 2600 -sertifiointi on vakiona käytössä kaikissa tulostuslaitteissamme, ja lisäksi Ricoh on johtava jäsen ja merkittävä tekijä IEEE-standardointiyhdistyksessä. ISO 27001 -sertifoituna yrityksenä Ricoh on sitoutunut noudattamaan tätä tietoturvajohtamisjärjestelmää.

Jotta tehokkaan ja todistettavan kyberturvallisuuden käytäntöjä koskevat tiukat vaatimukset voidaan täyttää, Ricohin valikoiman jokaiseen tuotteeseen ja palveluun sisältyy tietoturvanäkökulma jo valmiina – ei koskaan jälkikäteen lisättynä. Uskomme, että haavoittuvuuksien kokonaisvaltainen tarkastelu on olennaista nykyaikaisessa liike-elämässä selviytymiselle.

Ricoh käyttää ns. CIA-periaatteita (Confidentiality, Availability, Integrity) työpaikan tietojen tehokkaaseen turvaamiseen niiden koko elinkaaren ajan: Luottamuksellisuus, eheys ja saatavuus.



RICOH
imagine. change.

Näin Ricoh suojaa digitaalisen työpaikan

Ymmärrämme, miten tärkeää digitaalisen työpaikan suojaaminen on liiketoimintaan liittyvien tietojen koko monimuotoisen eliniän ajan. Saavutamme tämän toteuttamalla suojaustoimenpiteitä neljällä olennaisella tasolla: hallinta, suojaus, poistaminen ja tuki.

NELJÄ OLENNAISTA TASOA

1 HALLINTA

Suojaa tietojen eheyttä ja varmistaa, ettei tietoja voida peukaloida siirron aikana tai muuten. Suojaa tietojen syötön ja tallennuslaitteet sekä tavat, joilla tietoja siirretään ja tallennetaan verkkojen välillä.

- Kopioinnin suojaus
- Käyttäjän todennus ja käyttöoikeudet
- Rajoitettu käyttö / lukittu tulostus
- Laitteen suojaaminen haittaohjelmilta

2 SUOJAUS

Mahdollistaa tietojen turvallisen käytön. Varmista, etteivät tietoturvaprotokollat estä liiketoiminnan innovaatioita, toimivuutta tai tuottavuutta.

- Tietojen salaus
- Käyttöoikeuksien hallinta
- TPM-salausmoduuli
- Nopea ja turvallinen käyttö käyttäjän sijainnista tai käytettävästä laitteesta riippumatta

3 POISTAMINEN

Minimoi tietohäviöiden tai varkauksien vaara, ja varmista säädösten noudattaminen tehokkaan tietojenpoiston avulla.

- Tietojen päällekirjoitusjärjestelmä (DOSS)
- Tietojen poistopalvelu laitteen käyttöiän päätyttyä
- Kiintolevyn hävittäminen
- Muistin tyhjennys

4 TUKI

Tarjoaa yrityksille kattavaa tietoturvatukea.

- Infrastruktuurin turvallisuuden arviointi
- Tulostusturvallisuuden optimointi
- Turvallisuustiimi (SIRT)
- Tukidokumentaatio ja säännösten noudattaminen

Nykyaikaisen digitaalisen työpaikan täytyy olla yhtä dynaaminen kuin kohtaamansa verkkouhat ja yhtä joustava kuin työtavat ja käytännöt vaativat. Tästä syystä uskomme, että kyberturvallisuuden täytyy toimia saumattomasti kaikessa asiakkaidemme työpaikoillaan käyttämässä teknologiassa. Olemme sitoutuneet noudattamaan koko organisaatiossamme ISO 27001 -standardia ja kaikissa tuotteissamme IEEE 2600 -sertifointia. Voit luottaa siihen, että kun valitset Ricohin, käytössäsi ovat tietoturvan parhaat hallintakeinot yrityksen rakenne- tai kasvumuutoksista riippumatta.

Haluatko tarkempia tietoja? Lisätietoja Ricohin tietoturvatoiminnoista saat lataamalla koko katsauksen: **Ricoh Security Solutions**

Tutustu sivustoomme **ricoh.fi** ja lue, miten Ricoh voi auttaa yrityksesi tietoturvaratkaisuissa ja kehittämisessä. Voit myös ottaa yhteyttä paikalliseen Ricoh-edustajaan.

Ricoh Finland Oy
Niittytaival 13
Espoo

0207 370 300

ricoh.fi

RICOH
imagine. change.