Pk-yrityksen riskienhallinta

- Tietoriskien hallinta

VTT Automaatio • Turun kauppakorkeakoulu
Työterveyslaitos • Tampereen teknillinen korkeakoulu

Kalvoluettelo

Mitä ovat tietoriskit

- Tietoriskit ovat riskejä, jotka liittyvät yrityksen kaikkeen toimintaan, jossa käsitellään tietoja
- Sähköisten tietojärjestelmien riskit ovat näistä vain pieni osa
- Peruskysymykset:
  - Mitä varjeltavaa yrityksessä on?
  - Mitkä seikat voivat uhata niitä?
  - Miten uhilta voidaan suojautua
- Tietoriskien hallinta tapahtuu samoilla periaatteilla kuin muidenkin riskien. Ja hallitsemalla tietoriskejä, tuetaan muidenkin riskien hallintaa

Tieto tärkeä tuotantotekijä

- Jokaisessa yrityksessä on sen toiminnalle kriittisiä tietoja, esimerkiksi asiakastiedot, tuotannonohjauksen tiedot, tuoteideat, markkinointisuunnitelmat.
- Tietoa on **paljon monessa eri muodossa**: henkilökohtainen osaaminen ja kokemustieto; asiakirjat, sopimukset, ohjeet, suunnitelmat ja muut paperidokumentit sekä asiakas-, tilaus- ja palkkatiedot yms. tietojärjestelmien sisältämä tieto.

Tiedot hallittava

- Monessa pk-yrityksessä **tieto on suurin pääoma**.
- Silti tietojen hallintaan ja suojaamiseen ei aina kiinnitetä riittävästi huomiota. Yrityksen toiminnan kannalta on tärkeätä, että
  - Tiedot oikein, luotettavia ja ajantasalla
  - Tiedot ovat aina oikeiden henkilöiden saatavilla
  - Tiedot eivät joudu vääriin käsiin.

Tietoriskien maailma muuttuu

- Yritysten elämä on jatkuvaa, monimutkaista tietojen käsittelyä
- Yritysverkostoissa tieto liikkuu uudella tavalla
- Työsuhteen lyhenevät — väheneekö henkilöstön sitoutuminen?
- Makrovirukset ovat uusi tekstidokumenttien uhka
- Maahanmuuttajien tai uuden vientimaan tavat voivat poiketa siitä, mihin yrityksessä on totuttu
- Tiedonsiirtotavat monipuolistuvat ja nopeutuvat
- Missä puhut matkapuhelimeesi?
- Internetissä koko maailma on naapurinasi
- Elektroninen kauppa uudistaa kauppaa ja maksuliikennettä.

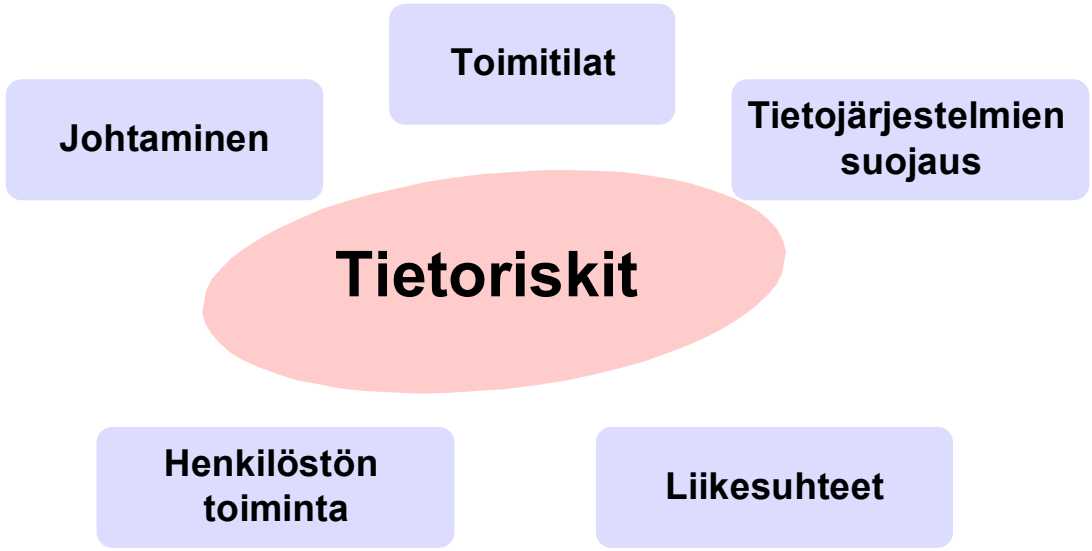
Ihmisten toiminta riski-enhallinnan lähtökohtana

Pahimmat tieto-vuotojen lähteet

1. Keskustelut
2. Paperidokumentit
3. Tietojärjestelmät

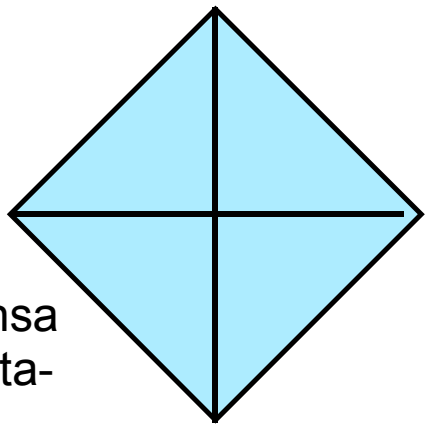
Hallinta vaatii monipuolisia keinoja

- Tietojärjestelmien tekninen suojaus vain pieni osa riskienhallintaa



Tietoriskien hallinta on kaikkien tehtävä

Johto luo puitteet,
tavoitteet ja resurssit



Esimiehet vastaavat paikallisen toiminnan turvallisuusta, alaistensa osaamisesta ja toiminta-tavoista

Tekninen henkilöstö suunnittelee ratkaisut uhkia vastaan

Työntekijät vastaavat työssään tietoriskien käytännön hallinnasta

- Kaikilla oma roolinsa, oma vastuunsa ja suojaustahtonsa

Yhteistyöllä tietoriskit hallintaan

- Kaikilla yhteinen käsitys keskeisistä suojattavista tiedoista ja niiden uhista, ja suojaamisen pelisäännöistä!
- Kaikilla silmät ja korvat auki
- Yhteistyö tärkeää – tietojen käsittelyn pelisäännöt ja järjestelmät suunnitel-tava yhdessä realistisesti
- Riskien tunnistaminen edellyttää yh-teistyötä – eri näkökulmat täydentävät toisiaan
- Kaikilla tavoitteena liiketoiminnan jat-kuvuus

Johtaminen

- Johdon tietoisuus tietoriskien hallinnan merkityksestä on kaiken a ja o
- Tietojen käsittelyä on johdettava ja luotava siihen systemaattiset menettelytavat – muistaen kuitenkin, että varsinkin pk-yrityksissä toiminnan on oltava kevyttä ja joustavaa

Henkilöstön toiminta

- Henkilöstön arkiset toimet altistavat yrityksen tietoriskeille
- Samoin henkilöstö arkisissa toimissaan hallitsee tietoriskejä
- Toimintatapoja on arvioitava riskien näkökulmasta
  - Milloin tietoa voi joutua vääriin käsiin?
  - Voiko tietoa kadota tai vääristyä?
  - Onko tieto aina saatavilla (sairaustapaukset yms.)?
- Henkilöstön osaaminen ja asenteet ovat a ja o. Tarvitaan koko porukan valmentamista näihin asioihin.
- Lisäksi henkilöstö tarvitsee hyvät tekniset puitteet – esimerkiksi automaattiset tekniset suojausjärjestelyt

Toimitilat

- Yrityksen toimitilat ovat suuri riskien aiheuttaja
- Avoimet konttorit, pöydillä oleva asiakkaiden tiedot, käytävillä olevat faksit houkuttelevat väärinkäyttöön
- Tulipalon jäljiltä voidaan uusi talo rakentaa helposti, mutta mitä tehdään, kun kaikki tuotetiedot ja asiakasrekisterit katoavat?

Tietojärjestelmien suojaus

- Kaikki tietojen liikkuminen paperilla, suullisesti, tallennusvälineissä, tietokoneissa ja tietoverkoissa on suojattava
- Heikkoja lenkkejä ei saa jäädä
- Oikea suojaustaso kohteen mukaan: isoin panostus keskeisiin riskeihin
- Suojaukset toimittava toimintaa häiritsemättä, automaattisesti taustalla
  - Esimerkiksi automaattisesti toimiva ja päivittyvä virustentorjuntaohjelmisto
- Toimintaa on jatkuvasti kehitettävä uusien teknisten uhkien varalta

Tietoriskit liikesuhteissa

- Pk-yritysten erilaiset yhteistyömuodot altistavat tietoriskeille
- Verkostojen osapuolten ja alihankkijoiden luotettavuus varmistettava
- Yhteistoimintaa käynnistettäessä on luotava myös yhteiset pelisäännöt tietojen käsittelyyn ja suojaamiseen

Tietoriskien hallinnan välineet

- ”Pääkortti”, joka esittelee teeman
- Tietokortti, joka kokoaa keskeisiä kysymyksiä tiiviiksi paketiksi
- Tietokortti, jossa esitellään esimerkkejä elävän elämän tilanteista
- Kortit, joissa pääosin tarkistuslistoja
- Välinesarjan yleiset apuvälineet mm.
  - Yleiset riskianalyysimenetelmät (esimerkiksi Potentiaalisten ongelmien analyysi POA)
  - Tärkeä yleistekniikka on käydä läpi yrityksen toiminto vaihe vaiheelta – mikä voi mennä vikaan
  - Toimenpiteiden suunnittelun välineet

Tietoriskikartta karkean riskien kartoituksen väline

Johtaminen

- ☐ Johdon tietoisuus tietoriskien merkityksestä
- ☐ Tärkeimpien tietojen tunnistaminen
- ☐ Suurimpien riskien tunteminen
- ☐ Tietoturvapolitiikka ja -käytäntö
- ☐ Tietoturvallisuus osana laatujärjestelmää
- ☐ Hankittu käyttöön riittävä osaaminen
- ☐ Tietoturva-toiminnan kehittäminen

Toimitilat

- ☐ Alttius onnettomuuksille
- ☐ Yrityksen tilojen erottaminen kiinteistössä
- ☐ Kulunvalvonta
- ☐ Vartiointi ja murtoturvallisuus
- ☐ Tilojen erottaminen toisistaan ja kulkuoikeudet
- ☐ Arkistot ja dokumenttien käsittely
- ☐ Faksit, kirjoittimet, yms.
- ☐ Asiakastilat

Tietojärjestelmien suojaus

- ☐ Vastuut järjestelmistä
- ☐ Paperin käsittely
- ☐ Käyttöoikeudet
- ☐ Etätyö
- ☐ Toiminnan seuranta (häiriöt, käyttö, levytila)
- ☐ Arkistot ja dokumenttien käsittely
- ☐ Muutosten hallinta
- ☐ Käytöstä poisto
- ☐ Ohjelmistohankinnat
- ☐ Varmistukset
- ☐ Salasanat
- ☐ Extranet ja WWW

Tietoriskit

Henkilöstön toiminta

- ☐ Koulutus tietoriskien hallintaan
- ☐ Tietoturvaperiaatteet
- ☐ Selkeä toimintaohjeet
- ☐ Toimet työsuhteen päättyessä
- ☐ Käyttöoikeuksien hallinta
- ☐ Varautuminen häiriöihin ja onnettomuuksiin
- ☐ Suojaratkaisut henkilöstön välineissä (virustentorjuntaohjelmat yms.)

Liikesuhteet

- ☐ Yhteistyökumppanien luokittelu
- ☐ Yhteiset pelisäännöt
- ☐ Alihankkijoiden aiheuttamat riskit
- ☐ Eri osapuolten katselmointi
- ☐ Sopimukset
- ☐ Järjestelmien käyttöoikeudet
- ☐ Neuvottelutilojen yms. tietoturvallisuus
- ☐ Yhteistyön tietojen suojaus muilta asiakkailta

Kartan tarkastelun perusteella siirrytään korttien tarkistuslistoihin tai käyttämään muita menetelmiä

Täyttöesimerkki

☒ Sopimukset - *Merkittävä riski;* OK ☐ Asiakkaat - *Asia kunnossa;* ☐ ~~Laiterikot~~ - *Ei koske meitä*

Tieto- ja työkortit

- Tietoriskit -tietokortti
- Tietoriskien tärkeitä kysymyksiä -tietokortti
- Esimerkkejä lauenneista tietoriskeistä -tietokortti
- Tietoriskien hallinnan johtaminen ja organisointi -työkortti
- Henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa -työkortti
- Toimintaympäristön, työ- ja palveluti-lojen tietoturvallisuus -työkortti
- Tietojärjestelmien suojaus -työkortti
- Tietoriskit liikesuhteissa -työkortti

Harjoitustyö

- Kokeillaan tietoriskien tunnistamista esimerkkiyrityksen avulla (esimerkit ohessa)
- Tunnistetaan ensin riskikartan avulla keskeiset tietoriskien alueet
- Käydään sitten tärkeimmät alueet (tai kaikki, jos aikaa riittää) läpi tarkistus-listojen avulla
  - Tunnistakaa konkreettisia riskejä
  - Mitkä ovat suurimmat riskit
- Miettikää sitten toimenpiteitä riskien vähentämiseksi – mitä pitäisi tehdä ensimmäiseksi

Harjoitustyö – esimerkki 1

Oy Laakeri-Veikot Ab toimii Pohjanmaalla omassa toimitilassaan. Yrityksessä on 10 suunnittelijaa ja 100 henkeä tuotannossa.

Yritys valmistaa paperikoneiden telojen laakereita ja markkinoi niitä ympäri maailmaa. Yhteistyön parantamiseksi on yritykseen rakennettu Extranet-palvelu osaksi nykyistä paikalliselta puhelinyhtiöltä ostettua WWW-palvelua. Järjestelmän rakensi kesäteekkari, ja nyt mietitään Java-ohjelmointikieltä osaavaa ylläpitäjää järjestelmälle. Tietoverkko-asiat ovat yrityksessä vielä vieraita. Vain suunnittelijoiden tietokoneet ovat lähiverkossa. Toimitusjohtaja osaa jo vastaanottaa sähköpostia! Extranetissa on useiden paperikonevalmistajien arkaluonteista tietoa, joten tiedot on suojattu salasanalla. Käytännön yhteistyö asiakkaisiin tapahtuu yleensä sähköpostilla tai faksilla. Käytävällä olevan faksin rätinä kertoo yleensä, että kohta taas juostaan!

Uusia tuoteideoita käydään kannettavan tietokoneen kanssa esittelemässä maailmalla sekä valmistajien luona että messuilla. Kannettavissa olevalla ohjelmalla saadaan tuotteet heti räätälöityä asiakkaan mukaisiksi. Tuotedokumenttien käännökset teetetään oman kielitaidon puuttuessa Teknillisen korkeakoulun opiskelijoilla. On saatu hyvää työtä halvalla. Riskienhallintaa suunnitellaan vakuutusasiamiehen kanssa. Paloriskit juuri kartoitettiin.

Harjoitustyö – esimerkki 2

Espoolaisessa Kopio-koneistajat -yrityksessä on töissä toimitusjohtaja, myyntipäällikkö, sihteeri ja viisi huoltomiestä.

Yritys huoltaa kopiokoneita. Huoltopalvelut myydään ylläpidon kokonaispaketteina. Kaikki merkit ja uusimmatkin mallit tuetaan.

Myyntiä ja asiakassuhteita pyörittää enimmäkseen myyntipäällikkö, jolla on kaikki asiakastiedot kalenterissaan. Kerran hänelle jouduttiin soittamaan sairaalaan (toipilaana sydänleikkauksessa), kun tarvittiin asiakkaan yhteyshenkilön tietoja. Tämä on hänelle jo ties miten mones työpaikka, joten ei häntä enää saa opetettua uusille tavoille.

Huollettavien koneiden huoltokirjat säilytetään helposti käden ulottuvilla palvelupisteessä, jossa sihteeri hoitaa myös kirjanpidon, kun on aikaa.

Harjoitustyö – esimerkki 3

Yrityspalvelu ETO Oy on aloittanut toimintansa vuonna 1960 nykyisen toimitusjohtaja Arttu Teemin isän johdolla. Vakinaisia työntekijöitä on 15. Päätoimipaikka on Tampereella, keskellä kaupunkia erään toimistotalon remontoimattomassa ja hyvin avoimessa 6. kerroksessa. Tilaa on 200 neliötä.

Yritys tarjoaa pääasiassa tilintarkastuspalveluita ja siinä sivussa konsultointia alueen keskisuurille ja kasvussa oleville yrityksille. Kehitteillä on uusi tilintarkastuspalvelukonsepti keskisuurille yrityksille. Vakinaisia asiakkaita nykyisellään on 460 kpl. Konsultointi kohdistuu asiakkaiden uusien ideoiden ja toiminnan kehittämisen tukemiseen ja muuhun luottamuksellisiin asioihin. Palvelukonseptin myyjillä on käytössään kannettavat tietokoneet, joilla he voivat olla suoraan yhteydessä kumman toimiston toimistojärjestelmään tahansa, josta he voivat tarkastaa asiakkailta tulleet sähköpostit, valvontatietoja jne. Myyntiin pitäisi saada ulkopuolista apua. Asiakkailla on pääteyhteys yrityksen AS/400 -laitteistolle, jossa toimii mm. taloushallintojärjestelmä. Tältä laitteistolta tarjotaan asiakkaille talous- ja palkkahallinnon palveluita. Omia WWW-sivuja ollaan suunnittelemassa. Henkilöstöllä on käytössä MS Office -toimistojärjestelmä eli tekstinkäsittely, taulukkolaskenta ja sähköposti ja NT-lähiverkossa. Tietoliikenneyhteydet toimitilojen välillä kulkevat salaamattomina Internet verkon kautta, jossa myös tiuha sähköpostiliikenne liikkuu. Sähköpostijärjestelmällä vastaanotetaan asiakkaiden tilauksia ja ne vahvistetaan myös järjestelmällä. Joskus viestejä on myös hävinnyt, jolloin niitä on täytynyt jopa asiakkailta täsmentää. Jokaisella työntekijällä on modeemiyhteydet myös kotoa.

Yrityksessä on tekeillä oma laatujärjestelmä Suomen Laatupalkinto -kriteerien mukaisesti. Laatuasioista vastannut henkilö siirtyi kuitenkin isoon yritykseen sisäiseksi laatuasiantuntijaksi. Jotta tulevaisuudessakin voidaan tarjota kilpailukykyisiä palveluita, täytyy kehittää toimintaa ja palveluita turvalliseen suuntaan. Huonona puolena on se, että henkilöt jo muutenkin tekevät pitkiä päiviä ja antavat kaikkensa. Jokunen kaveri on jo siirtynyt muualle töihin – eikä aina täysin tyytyväisenä.

Tietoturvallisuutta ei ole ETO Oy:ssa aikaisemmin oikeasti pohdittu. Muutkin turvallisuuteen liittyvät asiat on lyöty laimin.

Harjoitustyö – esimerkki 4

Keksi esimerkki itse! Ota esimerkki julkisuudesta tai pohdi vaikka kilpailijasi ja tärkeän asiakkaasi tilannetta – tietenkin anonyymisti.

Voit myös tarkastella omaa yritystäsi. Silloinkin pitää harjoitustyötä purettaessa kertoa jotain tuloksia, mutta sellaisia asioita ei tietenkään saa kertoa, jotka vaarantavat yrityksesi tietoturvallisuuden.

Tietoriskien koulutus yrityksessä

Koulutus tärkeä lähtökohta

- Tietoriskien hallitsemiseksi tarvitaan yrityksissä osaamista sekä riskienhallinnan että erilaisten tietoriskien osalta
- On luotava omaa kyvykkyyttä tunnistaa riskejä – uusissa tilanteissa ei tätä taitoa voi korvata ulkopuolisella avulla

Perusteet kuntoon

- Yrityksen riskienhallinnan lähtötilanne-selvitys (kortti Yrityksen riskienhallinta-toiminnan arviointi)
- Mukana olevan ryhmän kokoaminen
- Luento riskienhallinnan perusteista – valmennus riskienhallinnan ajattelu-malleihin

Tietoriskien orientaatio

- Luento tuoteriskeistä ja niiden hallin-nan perusteista

Riskien tunnistaminen

- Yrityksen tietotoiminnan kuvaus
  - Toiminta, liikeidea, perusprosessit
  - Tärkeimmät tiedot ja niiden käsittelytavat
- Riskien kartoitus riskikartan avulla
- Löydettyjen riskialueiden läpikäynti tarkistuslistojen avulla (ja muilla menetelmillä)

Toimenpiteisiin

- Toimenpiteiden suunnittelu, kokoaminen ja käynnistäminen

Yhteenveto- ja palautetilaisuus

- Miten tästä eteenpäin?

VTT Automaatio
Tampereen teknillinen korkeakoulu
Turun kauppakorkeakoulu
Työterveyslaitos
Euroopan sosiaalirahasto
Työsuojelurahasto
Pohjola-Yhtymä
Tapiola-yhtiöt
Yrittäjäin Fennia
Yritys-Sampo
Suomen Vakuutusyhtiöiden Keskusliitto
Tapaturmavakuuutuslaitosten liitto
Suomen Yrittäjät
Kirjanpitotoimistojen Liitto
Sosiaali- ja terveysministeriö
Kauppa- ja teollisuusministeriö
SAK, STTK, Akava, TT
PORISHA-hanke