
Omaehtoiset toimet tietoturvan parantamiseksi ja Lex Nokia

**Valtiontalouden tarkastusviraston ja
tietosuojavaltuutetun toimiston IT-foorumi
Pikkuparlamentti, 28.1.2010**

Jari Råman, OTT
Erityisasiantuntija
Tietosuojavaltuutetun toimisto

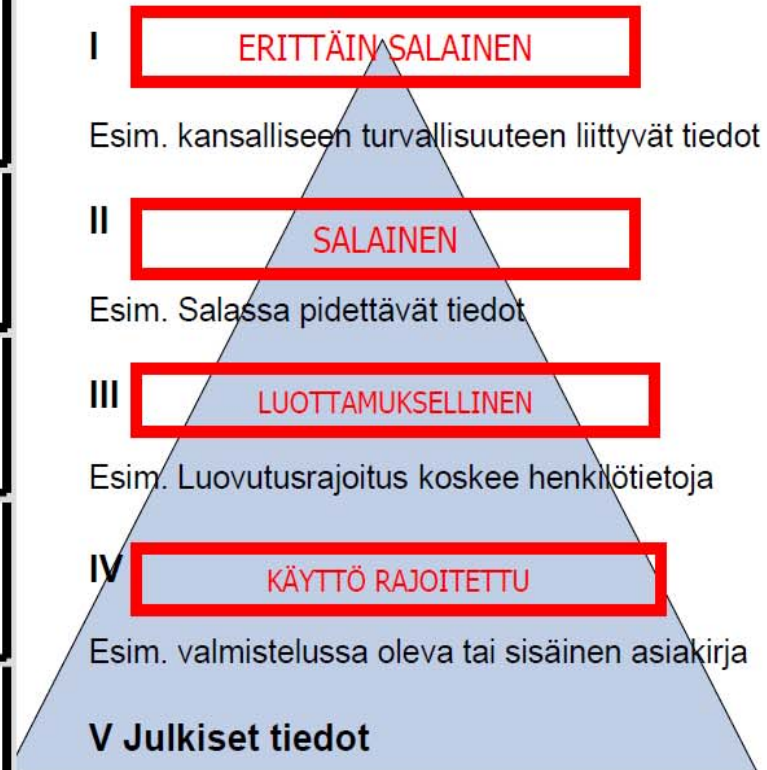


Tietoturvasat ja asetuksen luokittelut

Tietoturvasat



Turvallisuusluokitusmerkintä



Huom. LUONNOS

DATA TYPES TO PROTECT

PERSONAL DATA

REGULATORY COMPLIANCE

- ▶ Account Information
- ▶ Credit Card Numbers
- ▶ Contact Information
- ▶ Health Information

IPR

COMPETITIVE

- ▶ Source Code
- ▶ Engineering Specs
- ▶ Pricing

COMPANY CONFIDENT

CONTRACTS

REPUTATION

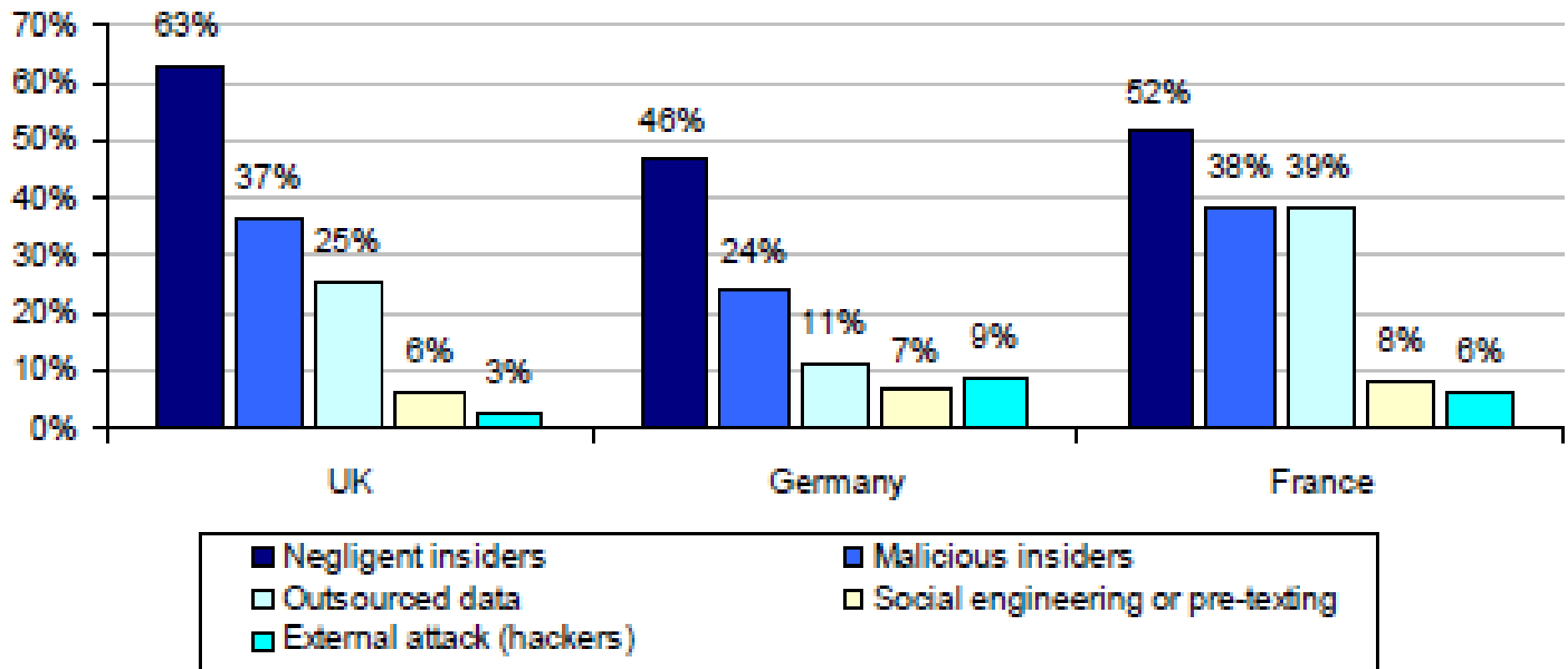
- ▶ Quarterly results
- ▶ M&A Strategy
- ▶ Strategy Documents

Ponemon Institute

Study on the Uncertainty of (Personal) Data Breach Detection 2008

Bar Chart 5

What are the most likely causes of data breach?

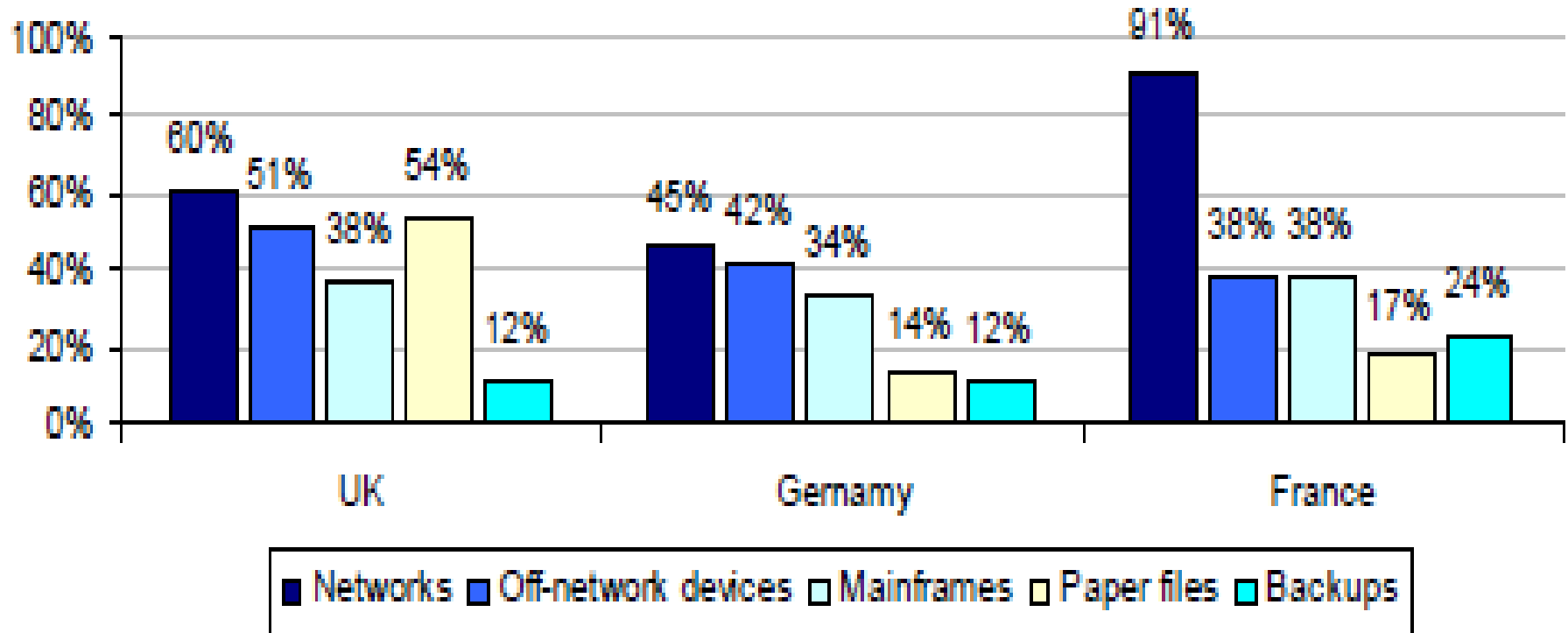


Ponemon Institute

Study on the Uncertainty of (Personal) Data Breach Detection 2008

Bar Chart 4

IT environment where data breached occur



Seuraukset henkilötietojen loukkauksista

Organisaatio

- Selvittely-, korjaus- ja tiedottamiskustannukset
- Negatiivinen julkisuus
 - Luottamuksen väheneminen, asiakkaiden menetys, vaikutus osakkeen arvoon (Cambell et al. 2003)...
- Oikeudelliset seuraukset
 - Sakko (ja vankeus), mutta myös sopimusrikkomukset, vahingonkorvaus, toiminnan kieltäminen ja keskeyttäminen, teettämis- tai sakon uhka
 - Esim. FSA sakotti Norwich Union Life vakuutusyhtiötä 1,26 miljoonaa puntaa; U.S. Veterans Affairs sopi ryhmäkanteen 26 miljoonalla dollarilla.
 - Täytöntöönpano vaihtelee maittain: meillä ensisijaisesti ohjein ja neuvoin

Tiedon kohteet

- Identiteetti varkaudet ja petokset, kunnianloukkaukset, yksityiselämää koskevan tiedon levittäminen
 - Henkilötiedot haluttua tavaraa: valmiit markkinat ja jakelukanavat (spam, asiakirjaväärennökset, vakuutuspetokset, maksuvälinepetokset jne.)
- Vaiva tietojen korjaamisesta ja selvittelystä, sekä mahdollisesti myös palvelujen käyttöoikeuksien ja luottotietojen väliaikainen menetys



Kustannukset / Ponemon Institute

Cost factors under study: detection, notification and response along with legal, investigative and administrative expenses, customer defections, opportunity loss, reputation management, and costs associated with customer support such as information hotlines and credit monitoring subscriptions.

U.S.: \$204 per compromised customer record
 \$6.75 million per incident (least expensive \$750.000) } (2009)
 Largest increase due to legal defense costs (loss of customers in 2008)

\$202 / \$6.65 million (2008)
\$197 / \$6.3 million (2007)

U.K.: £60 per compromised customer record / £1.7 million per incident (2008)
 £47 / £1.4 million (2007)
 Largest increase due to loss of trust

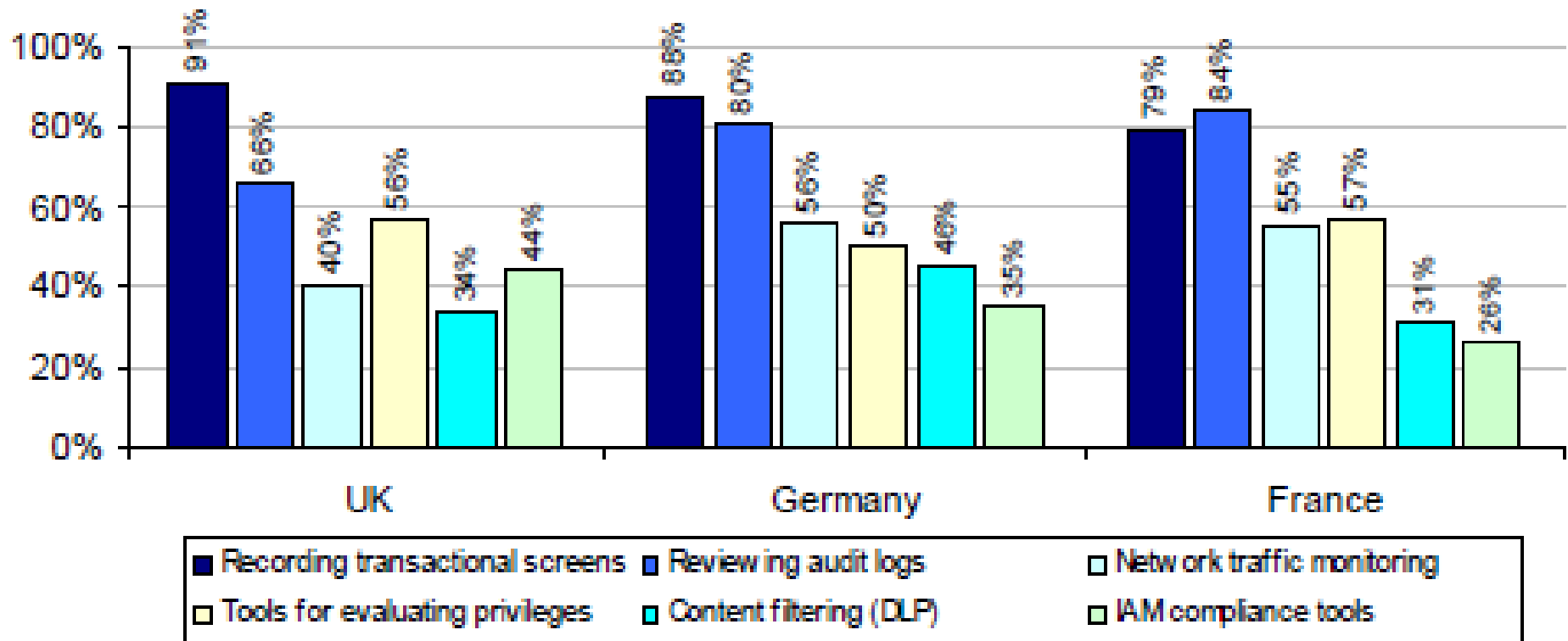
Germany: €112 per compromised customer record / €2.4 million per incident (2008)

Ponemon Institute

Study on the Uncertainty of (Personal) Data Breach Detection 2008

Bar Chart 10b

Should be performed to determine root cause
More than one response is permitted



LVM:n selvitys B 2/2001 (kyselykartoitus)

- Internetin ja sähköpostin valvonta yleistä
 - Lokitietoja kerätään vaihtelevasti
- Lokitietoja käytetään esim.
 - Työajankäytön seurantaan
 - Yrityssalaisuuksien vuotojen selvittämiseen
 - Siveettömän materiaalin käytön valvontaan
 - Ohjeiden vastaisen toiminnan valvontaan (esim. kielletyn ohjelman asentaminen)
- Valvonnasta ei raportoida
- Lainsäädäntö koettiin olevan jäljessä käytännöistä

Onko käytäntö nyt merkittävästi muuttunut?




American Management Association: 2007 Electronic Monitoring & Surveillance Survey

- Computer monitoring:
 - 45% track content, keystrokes, and time spent at the keyboard
 - 43% store and review computer files
- Network monitoring
 - 66% monitor Internet connections (web surfing)
 - 43% monitor e-mail
 - 12% monitor the blogosphere
 - 10% monitor social networking sites
- Telephone
 - 45% monitor time spent and numbers called
 - 16% record phone conversations
- Video surveillance
 - 48% monitor to counter theft, violence and sabotage
 - 7% track employees' on-the-job performance

About 1/3 have fired workers for email or Internet misuse

About 80 % inform employees about monitoring

HP Settles Spying Charges for \$14.5 Million

By Ryan Singel  December 8, 2006 | 8:28 am | Categories: Uncategorized

20.10.2009

Deutsche Bahn faces fine for e-mail spying

After a scandal revealed widespread e-mail spying at Germany's national rail company, Deutsche Bahn has been fined. The data protection scandal involved thousands of employees and raised concerns about workplace privacy.

Berlin's data protection agency has imposed a fine against Germany's national rail operator, Deutsche Bahn, for an e-mail privacy scandal that shook the company earlier this year.

A spokesman for Deutsche Bahn confirmed that the company had been fined, but refused to discuss the amount. According to the German daily newspaper Sueddeutsche Zeitung, the fine is 1.1 million euros (\$1.6 million). The company now has two weeks to file an appeal.

Hewlett-Packard agreed Thursday to pay \$14.5 million to California to settle charges it violated the law when it used private investigators to spy on and get the phone records of reporters, employees and directors in a botched leak investigation.

SPIEGEL ONLINE

05/26/2008 12:53 PM

The World from Berlin

Telekom Spying Accusations 'an Enormous Scandal'

www.helsinginsanomat.fi/english [print](#) | [close wi](#)

Nokia snooped on employee e-mail communications in 2005

Company suspected leak of company secrets to Chinese company

YKSITYISELÄMÄ

Perustuslaki 10 §

YKSITYISYYS

- 📖 RIKOSLAKI 24 LUKU
- 📖 E-SANANVAPAUSLAKI
- 📖 SALASSAPITO-SÄÄNNÖKSET

VIESTINTÄ

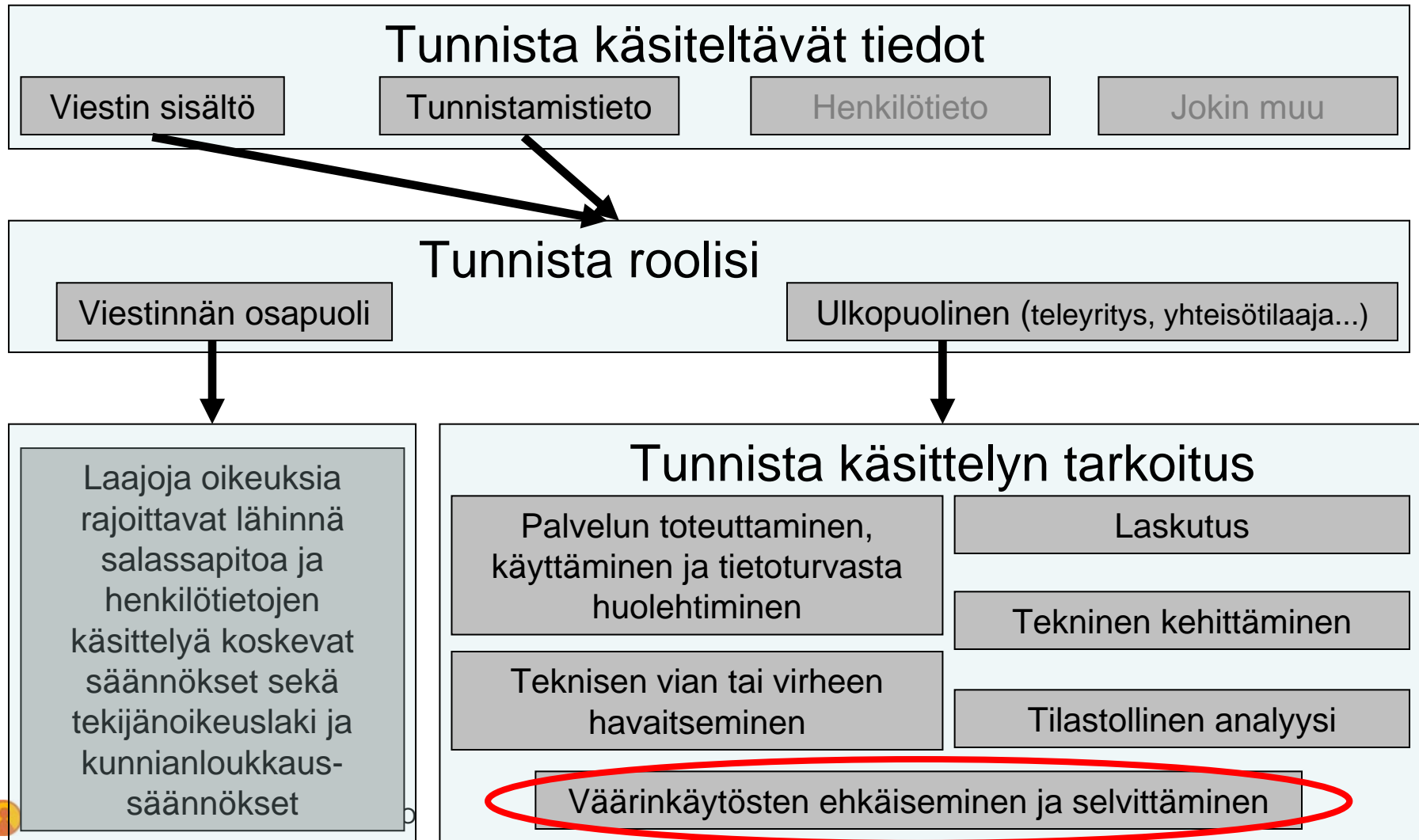
- 📖 SÄHKÖISEN VIESTINNÄN TSL
- 📖 TYÖ TSL
- 📖 Suojaa saavat
 - ▶ Viestin sisältö
 - ▶ Tunnistamistiedot

TIETOSUOJA

- 📖 HENKILÖTIETOLAKI
 - ▶ oikeus tietää, vaikuttaa
 - ▶ oikeus järjestää yksityiselämänsä...
 - ▶ henkilötietojen automaattinen käsittely ja rekisterinpito

📖 **JULKISUUSLAKI**
(Perustuslaki 12 §)

Sähköisen viestinnän tunnistamistietojen käsittelyn lähtökohdat



Väärinkäytöstapauksissa yhteisötilaajalla on: SVTSL 13 a – k § (entinen 13 §)

- Kaksi eri käsittelyoikeutta
 - Yrityssalaisuuksien vuotamisen selvittäminen
 - Maksullisen tietoyhteiskunnan palvelun sekä viestintäverkkojen tai –palvelujen luvattoman käytön selvittäminen
- Omissa järjestelmissään
- Ei oikeutta tarkastella viestin sisältöä
- Ei koske kiinteän tai matkapuhelinverkon puhelinpalveluja

Yrityssalaisuus

- RL 30:11: liike- tai ammattisalaisuus, taikka muu vastaava elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle
- Tulee olla *keskeinen* yhteisötilaajan elinkeinotoiminnan kannalta
 - määrittyy omasta toiminnasta, toimialasta ja siellä noudatettavista käytännöistä ja yhteistoimintamuodoista, sekä käyttäjälle annetusta ohjeistuksesta käsin
 - Esim. tiedot, jotka työnantaja erikseen ilmoittanut salassa pidettäväksi tai joiden käsittelystä ja suojaamisesta työnantaja laatinut erityisohjeet ja käytännöt



Luvaton käyttö

- Yhteisötilaajan viestintäverkkoon
 - oikeudetta asennettu laite, ohjelma tai palvelu,
 - oikeudeton pääsyn avaaminen sivulliselle
- Muu näihin rinnastuva viestintäverkon tai –palvelun käyttö, esimerkiksi
 - muuhun kuin yhteisötilaajan määrittämiin tarkoituksiin (elokuvien jakaminen tai oman palvelun ylläpitäminen toisen verkossa)
- Tulee olla käyttöohjeiden vastaista
- Tulee aiheuttaa merkittävää vahinkoa tai haittaa
 - Konkretisoitava käyttöohjeessa
 - Esim. lisääntyneet kustannukset sekä palvelun käytön vaikeuttaminen, vaarantaminen tai hidastaminen sille suunniteltuun tarkoitukseen



Yle: Yritykset välttelevät Lex Nokiana

Keskiviikko 14.10.2009 klo 08.09

Yksikään yritys ei ole ottanut käyttöön kohuttua ja kiisteltyä tietosuojalakea.

Yle uutisten mukaan yksikään yritys ei ole ottanut käyttöön Lex Nokiana, joka herätti paljon keskustelua viime talvena. Lakiuudistusta perusteltiin yritysten tarpeilla valvoa tietoliikennettä ja yrityssalaisuuksien vuotoa.

Lakia vastustettiin laajasti ja sitä vastaan järjestettiin mielenosoituksia. Muun muassa Elinkeinoelämän keskusliitto taisteli kuitenkin lain puolesta.

Lakia valmisteltaessa arveltiin, että kymmenet tai jopa sadat yritykset tarvitsevat lakia estämään tietovuotoja.

Laki runnottiin läpi vauhdilla ja lopputulos oli monimutkainen kompromissi.

Lakiin kirjattiin ehto, jonka mukaan lain käyttöön ottavan yrityksen tai yhteisön on tehtävä asiasta ilmoitus tietosuojavaltuutetulle. Yhtäkään ilmoitusta ei ole kuitenkaan tehty, vaikka laki on ollut voimassa lähes viisi kuukautta.

OTA KANTAA

Pitäisikö yritysten ottaa Lex Nokia käyttöön?



Kyllä

Ei

9%

91%

Ääniä 941

Potkut tuli – työntekijä kostaa

Sari Poijärvi / Lehtikuva



Yritysten omien työntekijöiden aiheuttamat tietovuodot ovat lisääntyneet räjähdysmäisesti tämän vuoden alkupuoliskolla viime vuoteen verrattuna. Irtisanomiset, lomautukset ja yleisesti huonontuneet työolot ovat saaneet työntekijät käyttämään väärin työssä saamiaan tietoja.

Economic uncertainty increases risk of data loss

Sharp increase in the number of respondents who say they would take proprietary / competitive / corporate security data in UK and US.

Cyber-Ark, Trust, Security & Passwords Survey, June 2009

59% admit taking company data after leaving former employer in US.

Ponemon Institute, Data Loss Risks During Downsizing, Feb 2009

Lisätietoja

- Lokiohje, VAHTI 3/2009, www.vm.fi/vahti
- Asiaa tietosuojasta 1/2009, Yhteisötilaajan oikeus käsitellä tunnistamistietoja väärinkäytöstapauksissa, www.tietosuoja.fi
– Mallilomakkeet

valvonta.tietosuoja@om.fi

+358 10 36 66700