Tietokannan tietoturva

Heli Helskyaho

20.3.2014

Tietoturva-aamupäivä, Oracle House

MIRACLE
Miracle Finland Oy

Lähde: IOUG:n käyttäjätutkimus

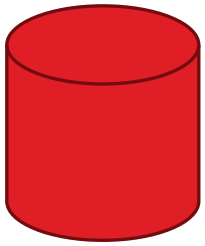
* IOUG tehnyt 2013 kyselytutkimuksen tietokannan tietoturvasta. Tässä esityksessä olevat tilastot (kuvat) pohjautuvat tähän (ladattavissa Oraclen sivuilta):

DATA SECURITY: LEADERS VS. LAGGARDS 2013 IOUG ENTERPRISE DATA SECURITY SURVEY (By Joseph McKendrick, Research Analyst Produced by Unisphere Research, a Division of Information Today, Inc. December 2013)

MIRACLE
Miracle Finland Oy

Mikä on tietokanta?

* Se paikka, jossa kaikki yrityksen tärkeä ja kriittinen tieto on tallessa. On tietysti olemassa myös julkista tietoa, mutta tärkeintä on se salainen tieto...



MIRACLE
Miracle Finland Oy

Mitä on tietoturva?

* Tieto on turvassa sellaiselta taholta, jolle se ei kuulu.
* Tietoon pääsevät käsiksi vain ne, joille se kuuluu.

MIRACLE
Miracle Finland Oy

Miksi tietokannan tietoturva?

* Tietokannassa oleva **tieto** on yleensä yrityksen kallein omaisuus.
* Jos tieto pääsee vääriin käsiin:
  * Kilpailijat saavat aiheetonta etua
  * Asiakkaat suuttuvat
  * Maine menee
  * ...
  * Business saattaa loppua...

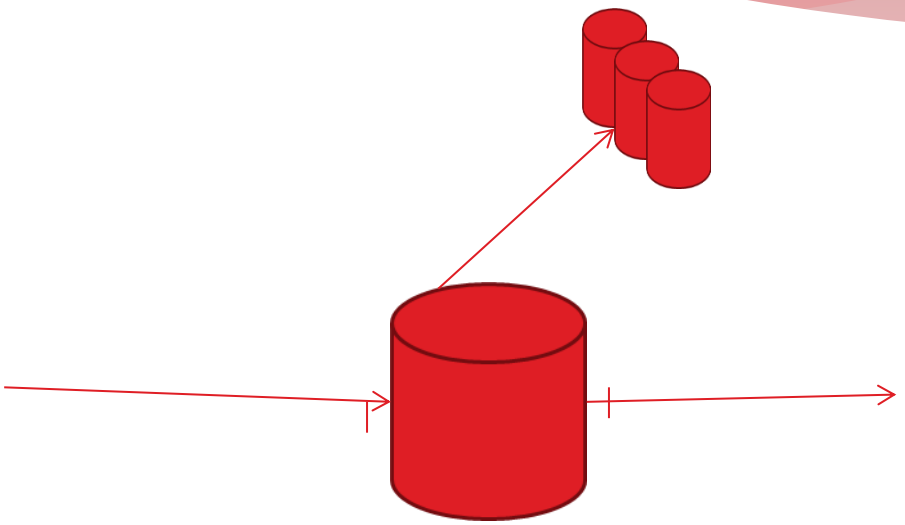
MIRACLE
Miracle Finland Oy

Mikä on tietovuoto?

* Tietoa on vuotanut sellaiselle taholle, jolla ei siihen ole oikeutta
  * Vahingossa (esim. bensa-asema, suklaapatukka)
  * Tarkoituksella (esim. erotettu työntekijä, rikollinen)

MIRACLE
Miracle Finland Oy

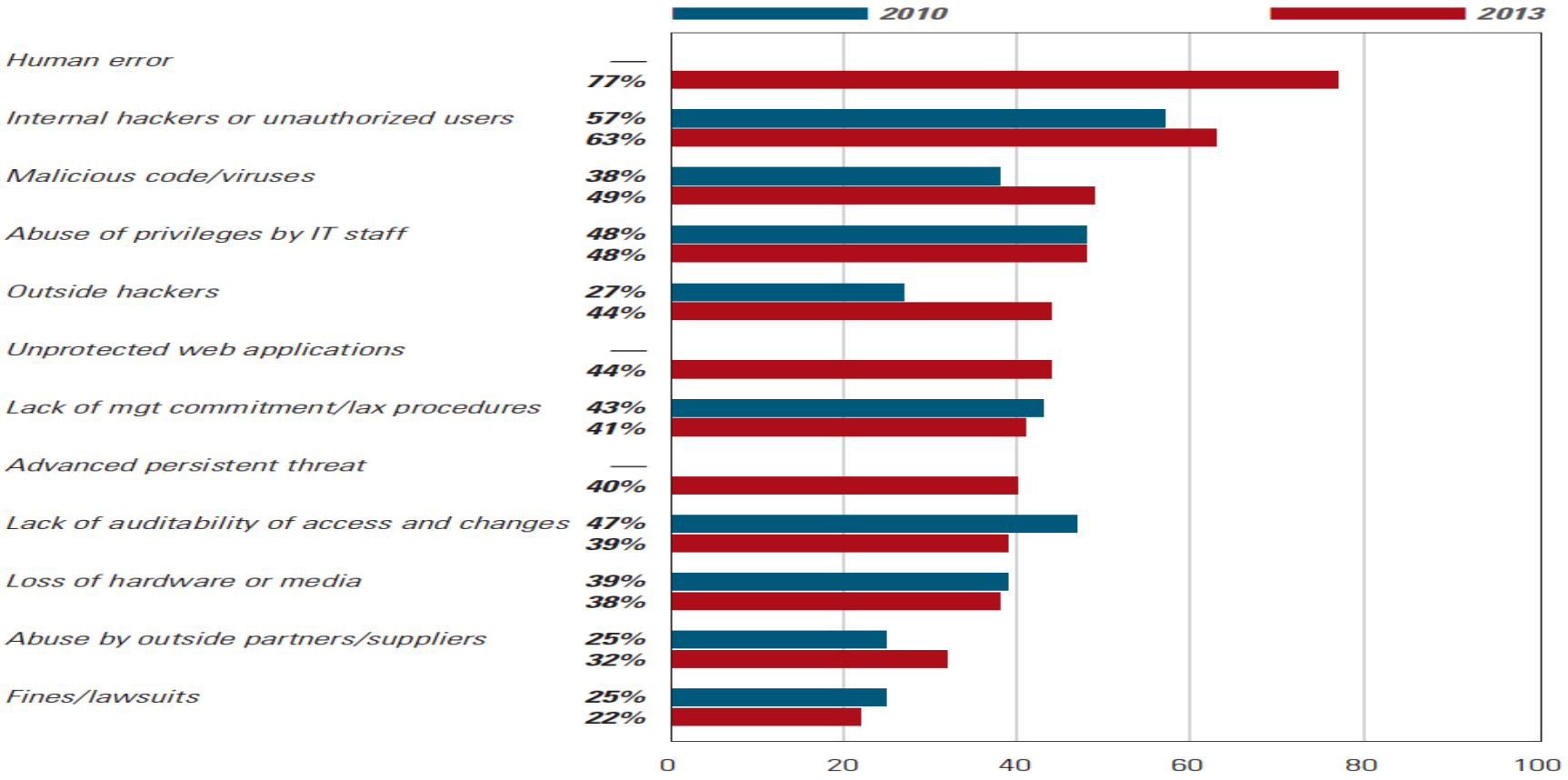
Mistä vuotaa?



Mistä uhka tulee?

Figure 7: Greatest Threats to Data Security

(Respondents Indicating a high to medium risk.)



MIRACLE
Miracle Finland Oy

Omat työntekijät suurin uhka?

* Miksi? Ovatko siis epäluotettavia... Ei☺

* Näkyy olan takaa -> Data redaction
* Lipsauttaa vahingossa (ihmisluonto) -> koulutus
* On tietoa, joka on kaikille sallittua ja sitten tietoa, joka on vain perustellusti jollekulle sallittua. Mistä tietää, mikä on salaista tietoa? -> koulutus, tiedotus
* Käyttää konetta suojaamattomassa verkossa, eikä kryptattu salasana (eikä data) -> kryptaus, koulutus
* Hukkaa koneen (tai kännykän tai muistitikun) -> salasanat, kryptaus, koulutus
* ...

MIRACLE
Miracle Finland Oy

Tietokannan tietoturva, asennus

* Tietokannan tietoturva alkaa tietokannan asennuksesta
  * Oletussalasanat
  * Portti 1521
  * Oletusobjektit ja oikeudet
  * Oletusasetukset yleensä
  * ...

MIRACLE
Miracle Finland Oy

Salasana

* Suojaa yleensä tietoa
  * miten hyvin suojaa, kuinka hyvä salasana
  * keillä tiedossa
  * kuinka usein vaihdetaan (kovakoodaus tms., vanhat työntekijät yms)
  * onko esim. kryptattu...

MIRACLE
Miracle Finland Oy

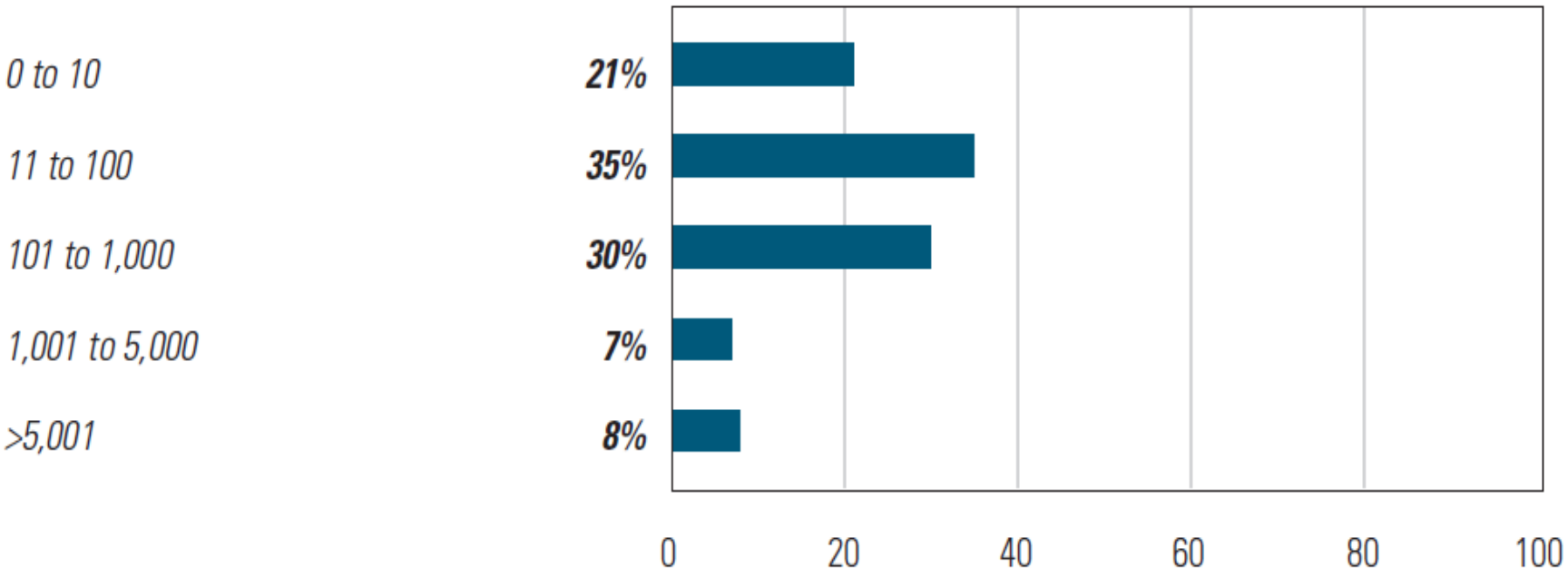
Käyttöoikeudet

* Mietittävä huolella
* Toteuttava suunnitellun mukaisesti
* Ylläpidettävä jatkuvasti (esim. lähtevät työntekijät, muuttuvat toimenkuvat)
* Onhan käyttöoikeudet toteutettu oikealle tasolle (jos esim. vain sovelluksessa, niin vaikkapa PL/SQL:llä ehkä kantaan pääseekin tekemään ihan muuta kuin pitäisi)

MIRACLE
Miracle Finland Oy

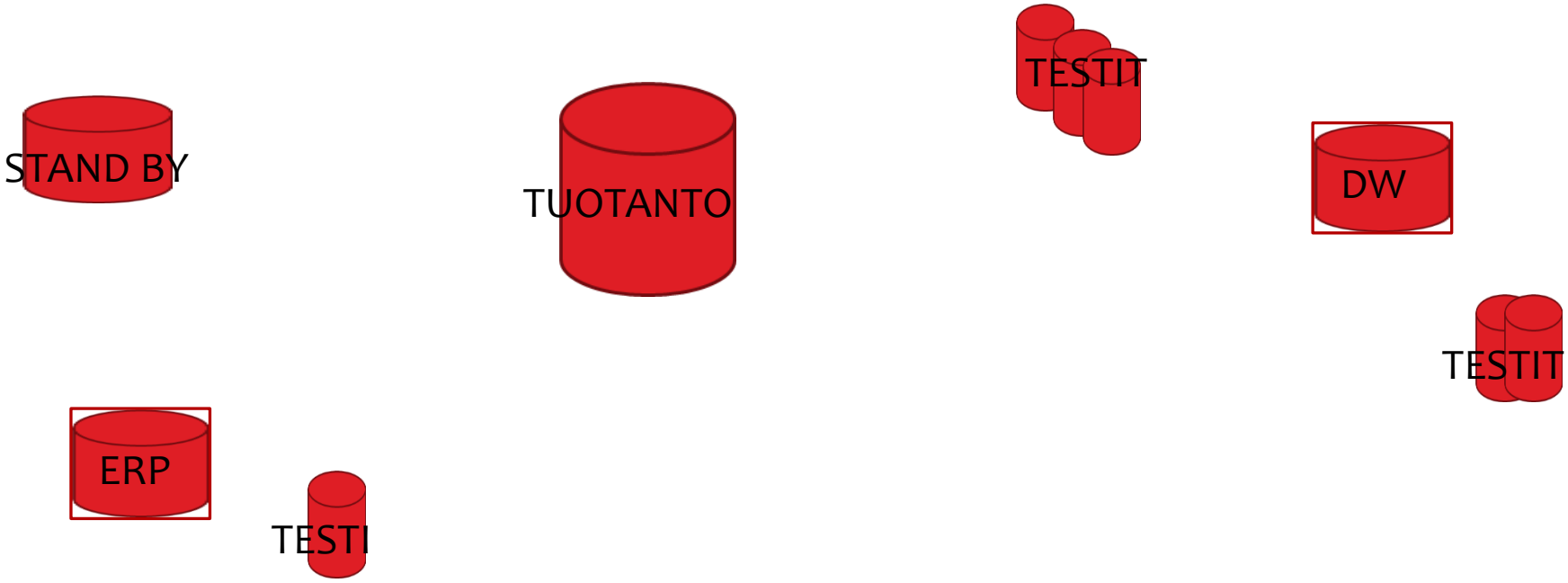
Tietokantojen määrä kasvaa

Figure 29: Number of Database Instances at Respondents' Sites



MIRACLE
Miracle Finland Oy

Tietokantojen määrä



Tietokannan tietoturva, monet kannat

* Helpompi murtaa, kun on monta kantaa, jossa samaa tietoa. Joku niistä on varmasti huonommin suojattu.

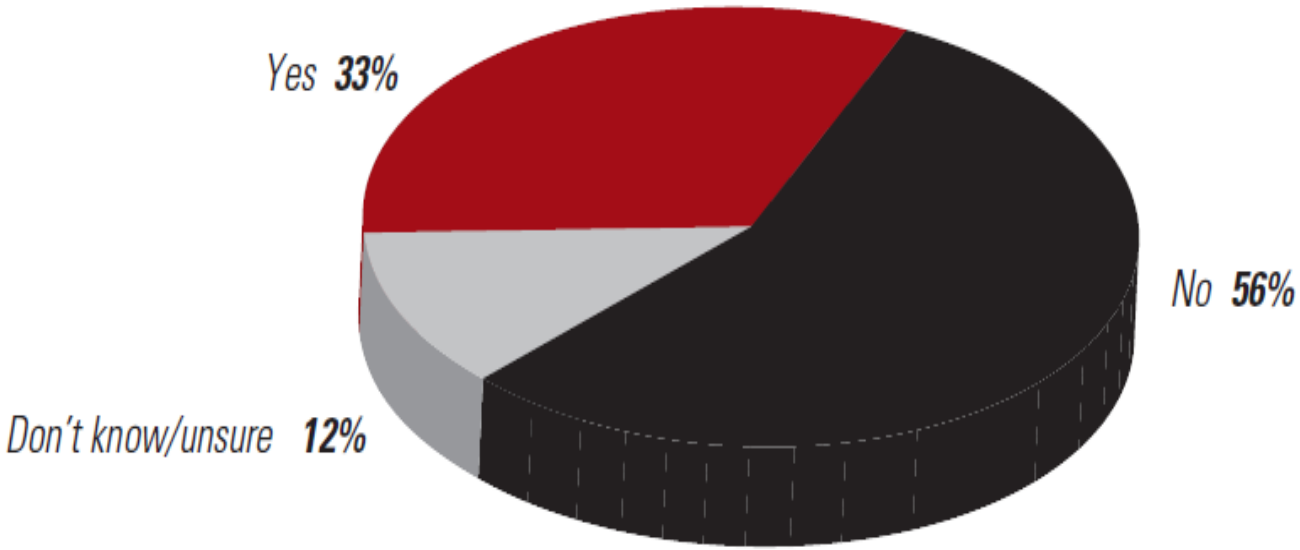
* Konsolidointi?

Tietokannan tietoturva, monet kannat

* Hups. Olinkin tuotannossa...

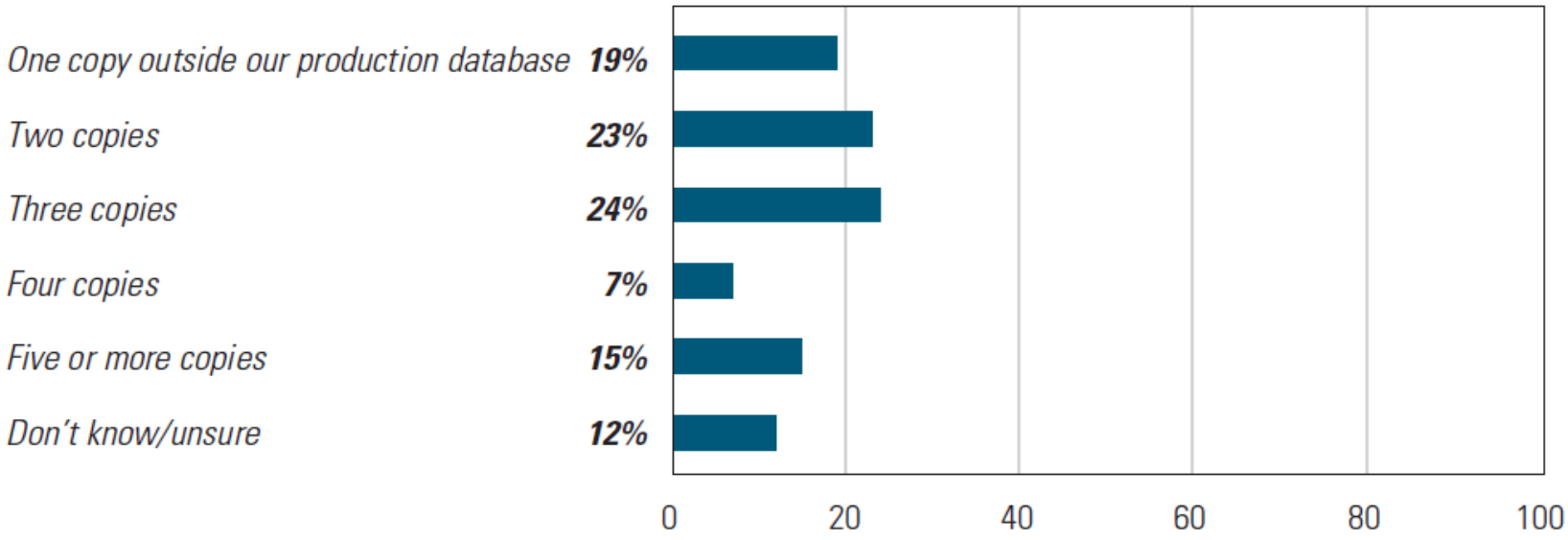
Miracle Finland Oy

Figure 16: Safeguards Against Administrator or Developer Data-Handling Errors



Testikantojen lukumäärä

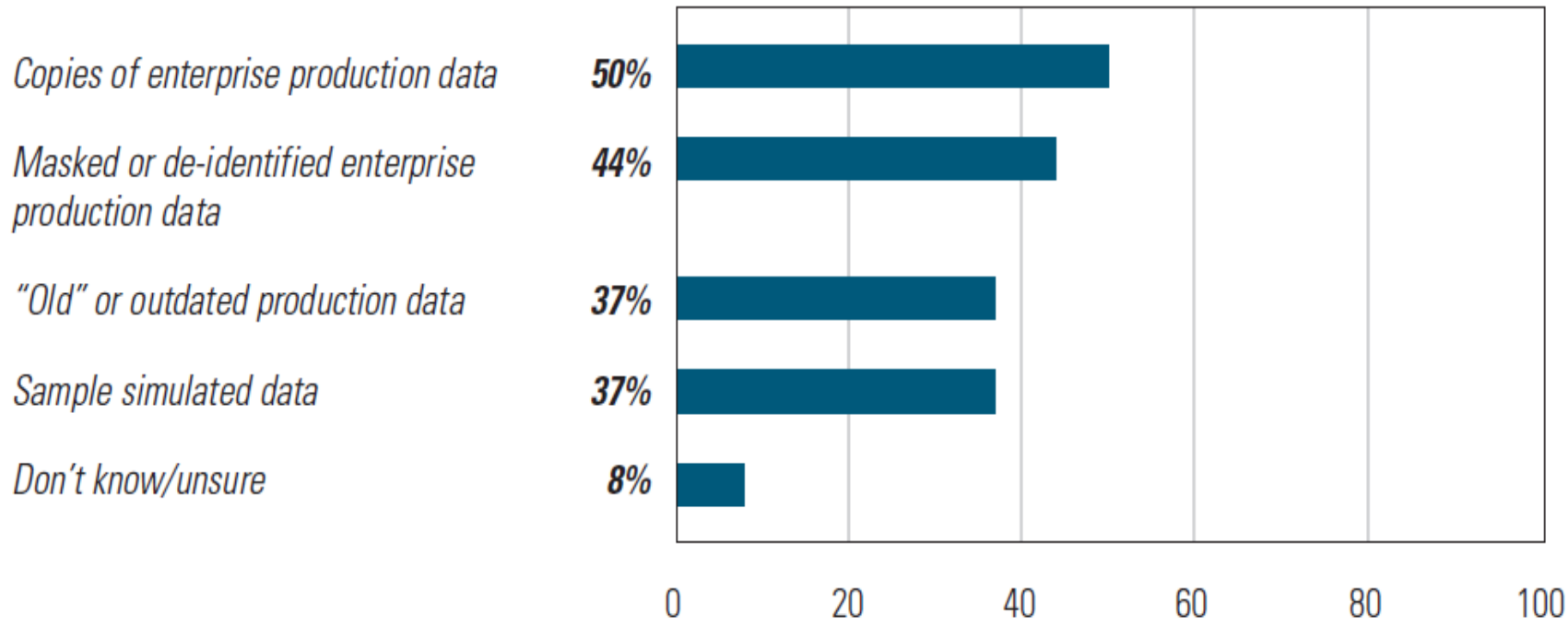
Figure 3: Number of Copies of Production Data



MIRACLE
Miracle Finland Oy

Testikantojen data

Figure 4: Data Used in Non-Production Environments



MIRACLE
Miracle Finland Oy

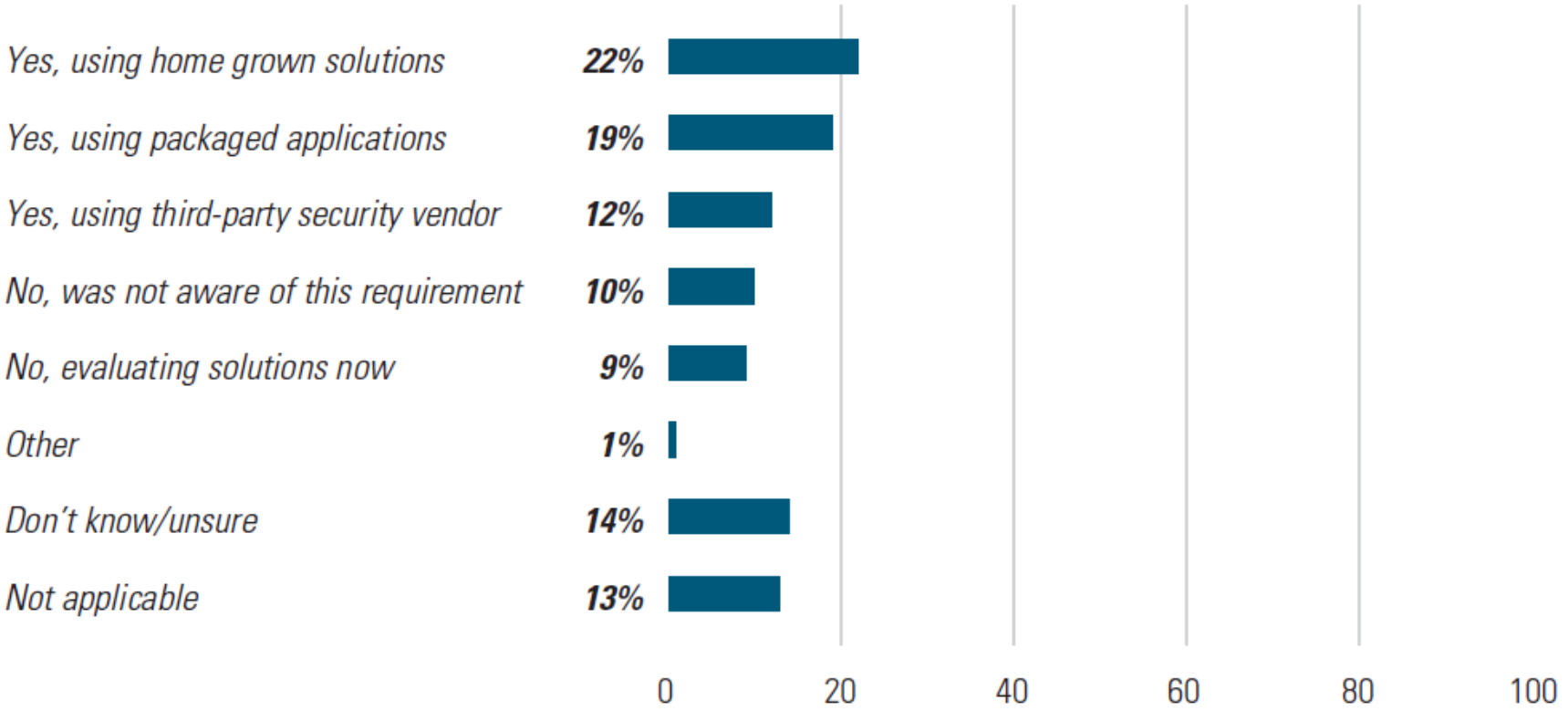
Tietokannan tietoturva, testikannat

* sama tieto kuin tuotannossa, onko muunnettu?
* Miksei?
  * Vie liikaa aikaa
  * On liian vaikeaa
  * Meillä kaikilla on nda
  * Meidän ihmiset ovat luotettavia
  * Samoilla ihmisillä on kuitenkin pääsy tuotantoon
  * jne jne jne ...

MIRACLE
Miracle Finland Oy

Testikannat, miten maskattu?

Figure 19: Addressing Regulations Requiring Masking of Sensitive Data in Applications



MIRACLE
Miracle Finland Oy

Testikannat

* tuotannossa valvonta, mutta testissä ei?
* Erilaiset dumpit levyn kulmalla? Kenellä niihin on oikeus?
* Tietokantalinkit? Tiedon imeminen toiseen kantaan.....

MIRACLE
Miracle Finland Oy

Tuotantokannat

* tarvitseeko dba oikeudet dataan?
* miksi niillä ihmisillä, joilla on oikeudet dataan, on ne? Tarvitsevatko oikeasti vai olisiko joku muu tapa olemassa tarpeen ratkaisuksi?

MIRACLE
Miracle Finland Oy

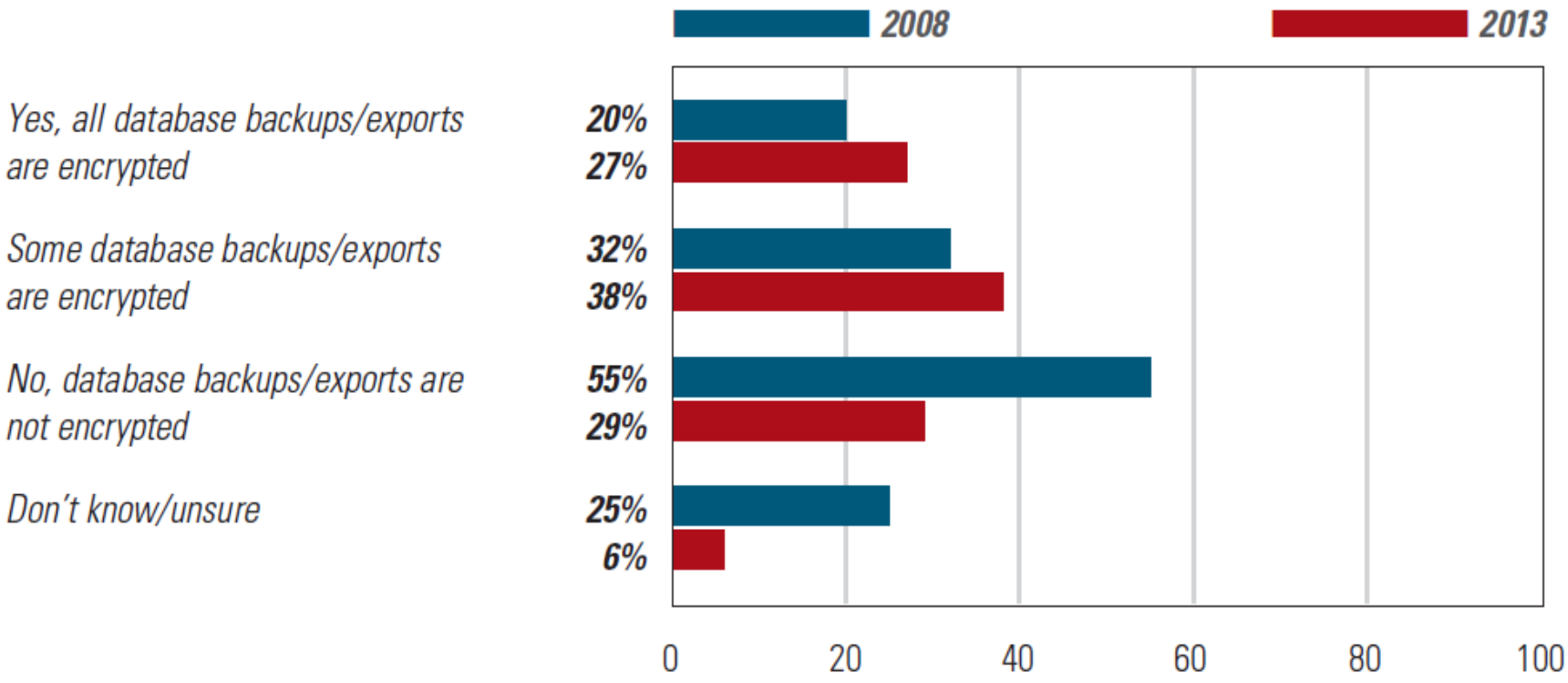
”Ulkopuolinen tiedon anastus”

* Luvaton sisäänkirjautuminen (monta rajapintaa...)
* Ulostulevan datan ”kaappaus” (ei kryptattua)
* SQL-injektio

Miracle Finland Oy

Tiedon liikuttelu, voiko silloin vuotaa?

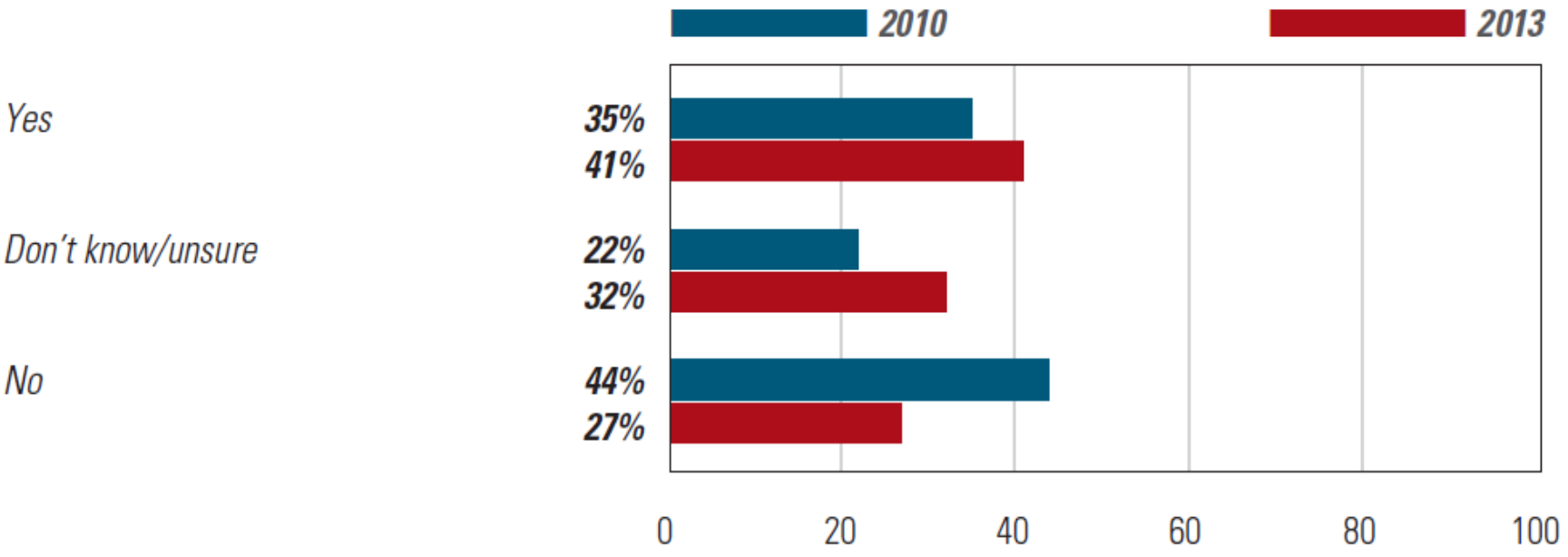
Figure 20: Data in Motion Encryption



MIRACLE
Miracle Finland Oy

SQL-injektio

Figure 24: Taken Steps to Prevent SQL Injection Attacks



MIRACLE
Miracle Finland Oy

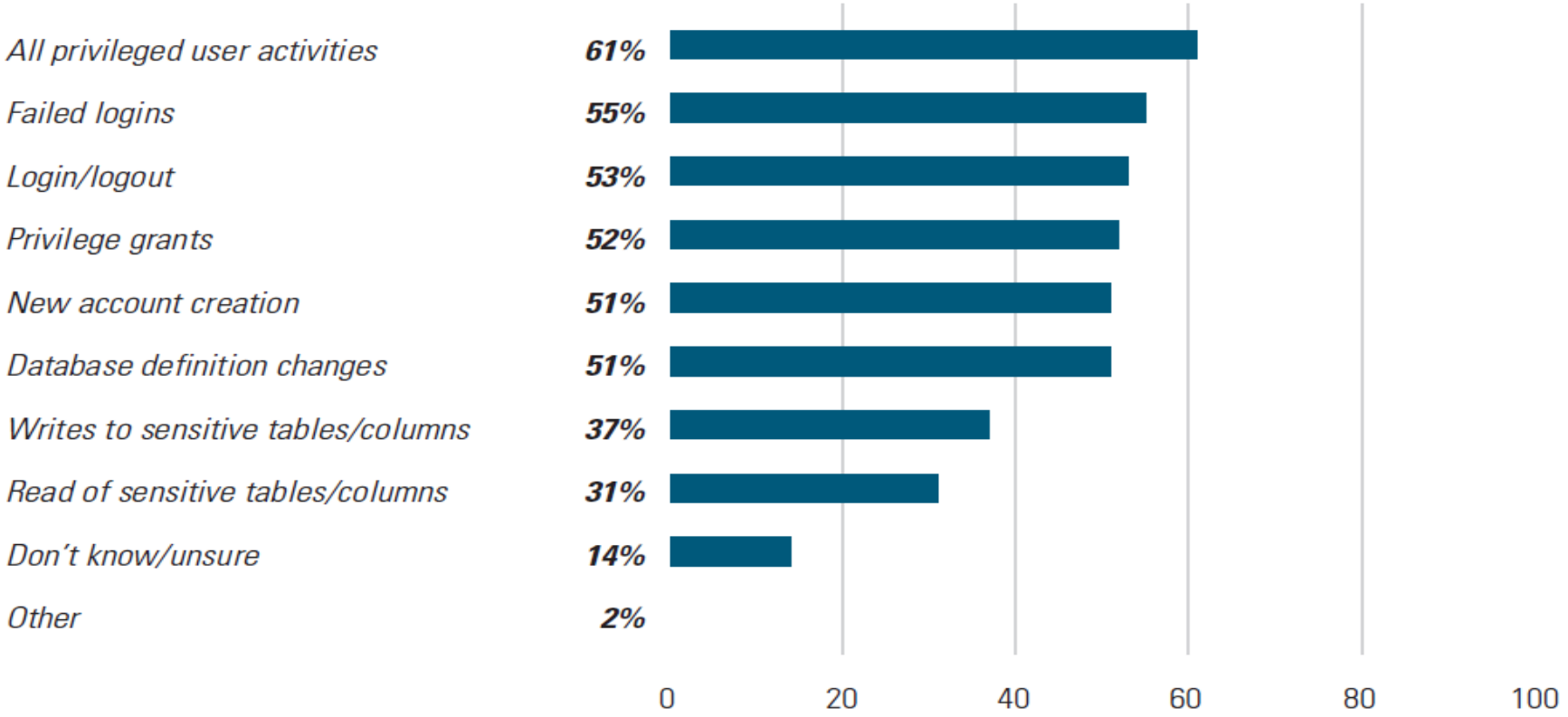
Tietovuoto tapahtunut? Onko?

* Mistä tiedetään, että tietovuoto tai yritys on tapahtunut?
  * Onko säännöllistä valvontaa (esim. lokien läpikäynti)?

MIRACLE
Miracle Finland Oy

Valvonta

Figure 25: Database Activities Monitored



MIRACLE
Miracle Finland Oy

Tietovuoto tapahtunut? Kuka?

* Mistä tiedetään, ketkä ovat mahdollisia vuotajia?
  * Miten voidaan todistaa, että oma dba ei ole vuotaja?: dba:lla ei ole tietoon oikeutta tai voidaan osoittaa, ettei ole siihen koskenut (nähnyt)

Tietovuoto tapahtunut? Kuka?

Figure 22: Can Prove Privileged Users Were Not Tampering

	2010	2012	2013
Yes	32%	26%	39%
No	39%	48%	43%
Don't know/unsure	28%	25%	19%

MIRACLE
Miracle Finland Oy

Tietovuoto tapahtunut? Kuka?

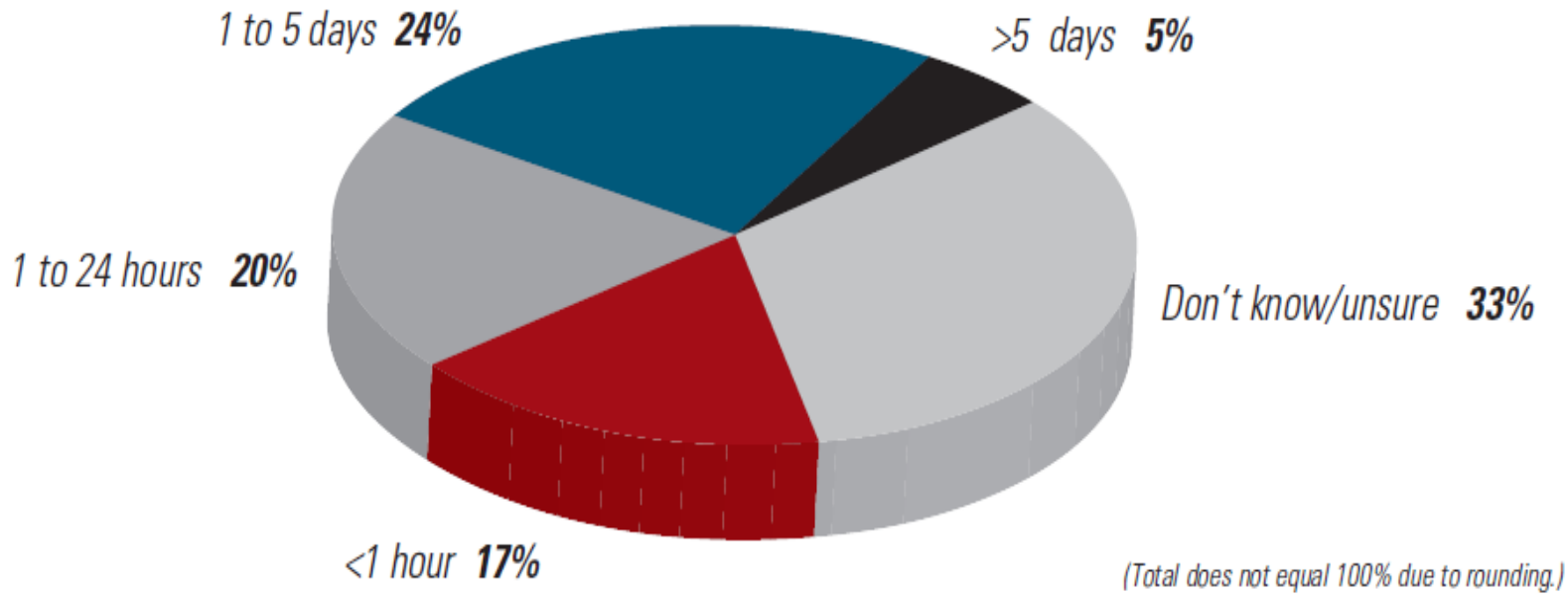
Figure 17: Prevent Privileged Users From Tampering With Sensitive Information

	2010	2012	2013
Yes	24%	32%	34%
No	44%	37%	42%
Don't know/unsure	32%	31%	24%

MIRACLE
Miracle Finland Oy

Miten vuodosta toivutaan?

Figure 23: Length of Time to Detect and Correct Unauthorized Database Access or Change



MIRACLE
Miracle Finland Oy

Onko tähän oikeasti varaa?

* Maailma pahempi joka päivä ja murtajat aina vaan näppärämpiä
* Estäminen välttämätöntä
* Havainnointi ja toipumisaika mahdollisimman pieneksi

MIRACLE
Miracle Finland Oy

”Oma ratkaisu on aina paras ja halvin”

* Onko?
* Oletko osannut varautua oikeisiin asioihin? Pystytkö muuttamaan tehtyä ratkaisua maailman muuttuessa? Onko ratkaisusi riittävästi testattu? Oletko huippuasiantuntija myös tietokannan tietoturvassa?
* Mitä itse tehty ratkaisu ja sen ylläpito maksaa? Mitä se maksaa, jos ratkaisu pettää?

MIRACLE
Miracle Finland Oy

Onko Oraclella valmiita ratkaisuja?

* Mitä noista asioista voidaan hoitaa Oraclen tuotteilla?
* Ovatko tuotteet niin kalliita, että meillä ei ole niihin varaa?

* Jukka?

MIRACLE
Miracle Finland Oy