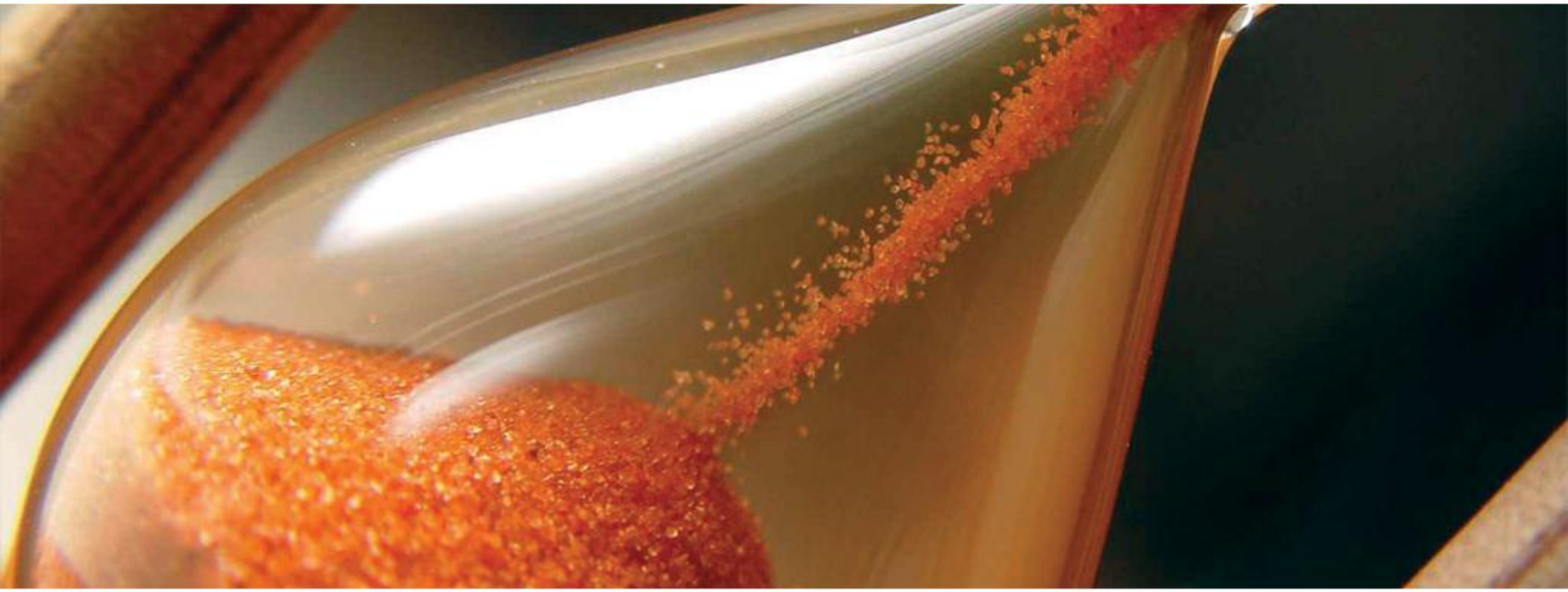


PCI DSS trendek külföldön és Magyarországon

Tátrai Péter
Gáspár Csaba

2011. december 7.

AperSky
Bankkártya és biztonság

Napirend

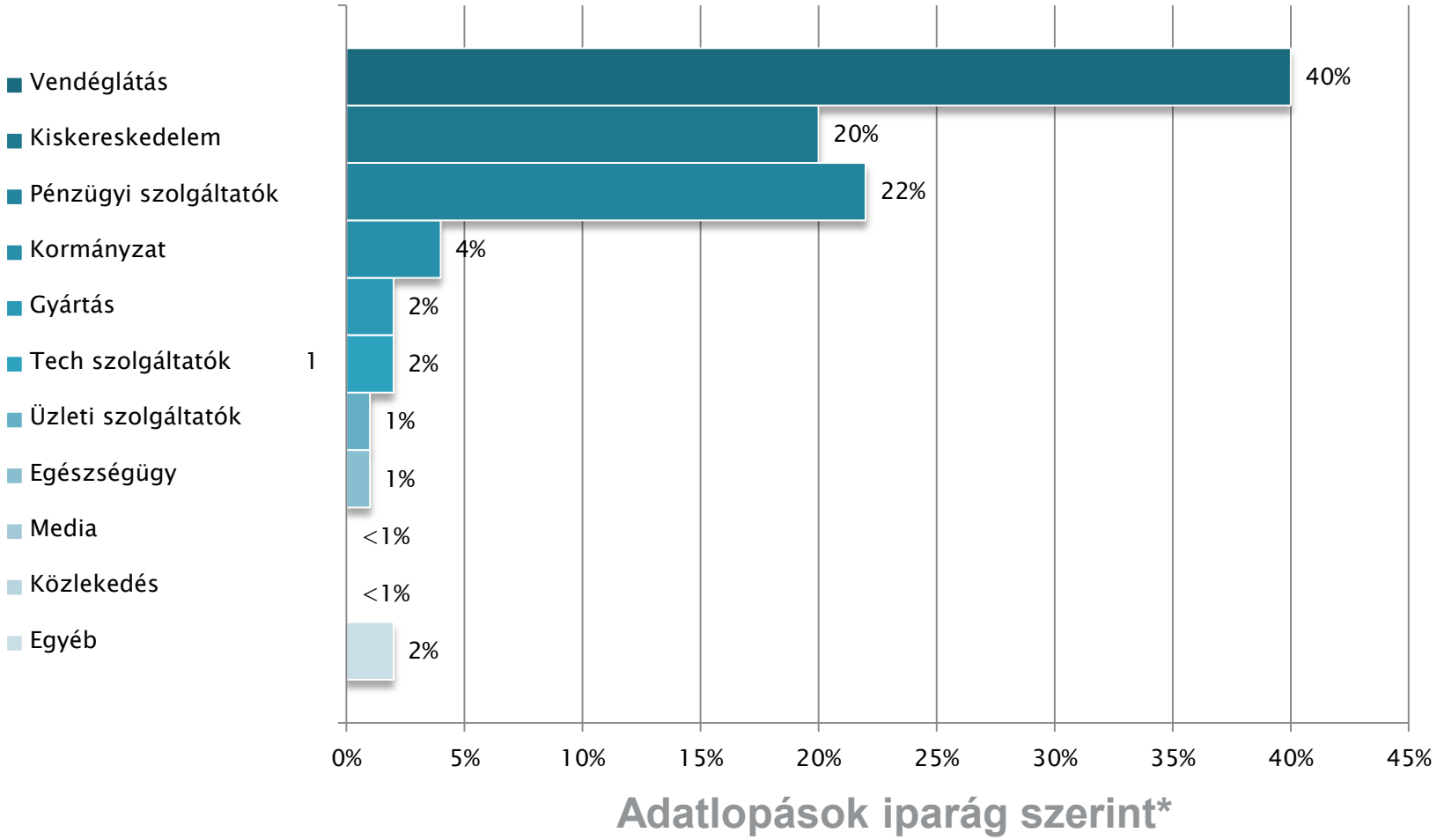
- A PCI DSS-ről röviden
- Nemzetközi trendek
- QSA cégek tapasztalatai - felmérés
- Magyarországi helyzet
- Hogy érint ez minket?

A PCI DSS-ről röviden

AperSky
Bankkártya és biztonság

- Egységes bankkártya-biztonsági szabvány
- Kiterjed minden intézményre, mely bankkártya adatot tárol, feldolgoz vagy továbbít
- Beszámolási kötelezettség a kártyatársaságok felé
- Beszámolás módja
  - Önértékelési folyamat (SAQ)
  - Helyszíni QSA Assessment (QSA audit)
- PCI DSS 2.0 verzió
  - 12 követelmény-csoport
  - 216 előírás
  - 418 tesztelendő eset

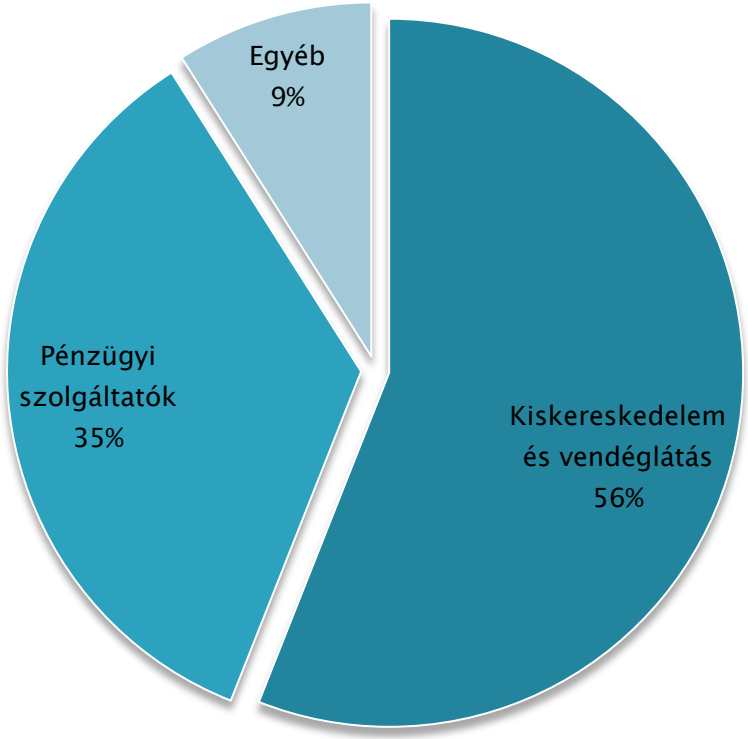
Nemzetközi trendek – adatlopás és iparág



*Verizon Data Breach Report 2011

Nemzetközi trendek – adatlopás és iparág

- Célkeresztben:
  - Pénzügyi szolgáltatók
  - Kereskedelmi cégek

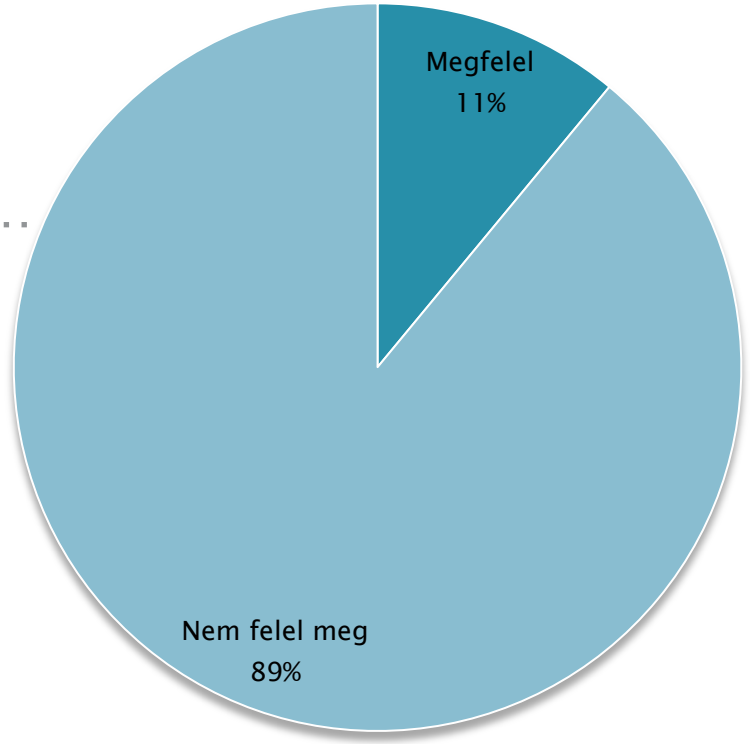


Kompromittált adatok mennyiségi megoszlása iparág szerint

*Verizon Data Breach Report 2011

Nemzetközi trendek – PCI DSS megfelelés

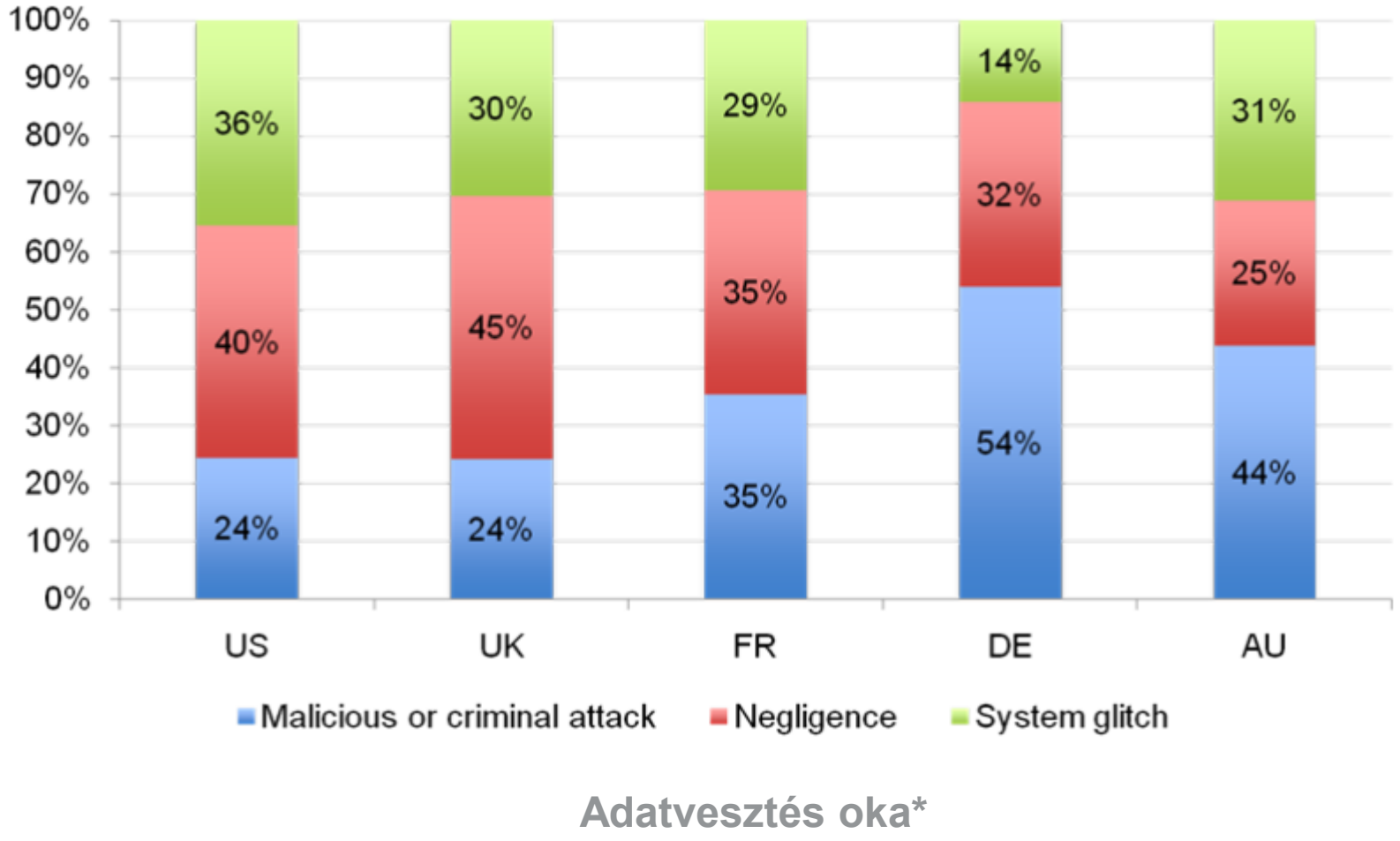
- A PCI DSS alkalmazása…
  - Radikális kockázatcsökkentést jelent…
  - de nem véd meg az adatlopástól!



PCI DSS megfelelés az adatlopást szenvedett cégeknél*

*Verizon Data Breach Report 2011

Nemzetközi trendek – adatvesztés oka



Adatvesztés oka*

*Ponemon Institute – Cost of a Data Breach 2010

QSA cégek tapasztalatai - felmérés

- Adatvédelem, adatkezelés fontossága QSA cégek szerint
  - 51% - nem megfelelő
  - 24% - megfelelő
- PCI DSS megfelelés költsége kereskedők szerint
  - 54% - túl drága
  - 20% - megfelelő
- QSA audit költségvetés biztosítása
  - PCI DSS megfelelés felelőssége – IT terület 30%
  - Szükséges költségvetés – üzleti terület 40%
- Éves QSA audit költség
  - Legnagyobb 1-es szintű kereskedők: ~225e USD/év
  - 10%-nál 500.000 USD vagy még több

*PCI DSS Trends 2010: QSA Insights Report - Ponemon Institute
(155 QSA cég bevonásával világszerte)

QUALIFIED SECURITY ASSESSOR

QSA cégek tapasztalatai - felmérés

- QSA audit sikere
  - Csak <2% bukik el
  - Jelentős a kompenzációs elemek használata (41%) – ideiglenes megoldás!
- Kártyaadat tárolás legjellemzőbb okai
  - Chargeback kezelés
  - Ügyfél szolgálat
  - Ismétlődő fizetések (recurring)
- Kártyaadathoz való korlátozott hozzáférés
  - Legfontosabb PCI DSS követelmény…
  - De a legnehezebb is megfelelni
- Kártyaadatok legnagyobb veszélyben
  - Továbbítás kereskedői hálózatokon
  - Tárolás adatbázisokban
  - Egyéb: POS terminálok és fizetési alkalmazások

*PCI DSS Trends 2010: QSA Insights Report - Ponemon Institute
(155 QSA cég bevonásával világszerte)

QUALIFIED SECURITY ASSESSOR

QSA cégek tapasztalatai - felmérés

Magyarországi PCI DSS helyzet

AperSky
Bankkártya és biztonság

Hogy érint ez minket?

- **1. PCI DSS hatálya**
  - Tárolunk, feldolgozunk vagy továbbítunk-e bankkártya adatot?
- **2. Piaci szerepkör meghatározása**
  - Szolgáltató
  - Kereskedő
  - Elfogadó és/vagy Kibocsátó bank
- **3. Besorolási szintek megismerése**
  - Letölthető a kártyatársaságok hivatalos oldalairól

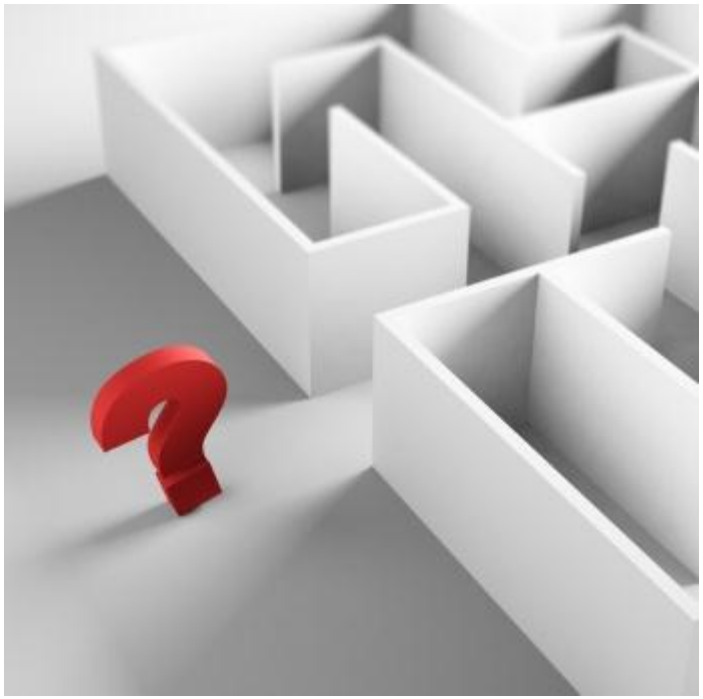
Hogy érint ez minket?

- **4. Besorolás éves tranzakció szám alapján**
  - Szolgáltató: Kártyatársaság, Kereskedő, Elfogadó Bank vagy másik Szolgáltató által
  - Kereskedő: Elfogadó bank által
  - Bankok: Kártyatársaság által
    - →Nem a QSA cég jogköre!

- **5. Jelentési kötelezettségek tisztázása**
  - Letölthető a kártyatársaságok hivatalos oldalairól
    - Elfogadó bankok 3 havonta kereskedői státuszt kártyatársaságok felé
    - PCI DSS megfelelési jelentések
      - Önértékelés során (SAQ)
      - Audit kötelezettként (QSA assessment)
      - → Kártyatársasági PCI compliance lista: csak auditált szolgáltatók!

Hogyan tovább?

- Szakértők bevonása…



AperSky

Bankkártya és biztonság

Köszönjük a figyelmet!

AperSky Tanácsadó Kft. | **Iroda:** 1053, Budapest, Veres Pálné u. 4-6. | **Telefon:** +36 1 781 2210 | **E-mail:** info@apersky.com | **Web:** www.apersky.hu