CDSYS
COMPLIANCE DATA SYSTEMS Kft.

Adatbiztonság aktuális kérdései:

Az adatszivárgás

Tóth Péter Barnabás, CIA, CISA, CISM
IT biztonsági tanácsadó

Adatlopás, szivárgás: valóság

CDSYS
COMPLIANCE DATA SYSTEMS Kft.

index 2009. június 10., szerda - Margit, Gréta.

Címlap | Belföld | Külföld | Bulvár | Gazdaság | Tech | Tudomány | Kult | Sport | Vélemény

Hírblog | Anyádat | Webisztán | Hoaxkábel | Mobil | Kmk | 3G vs. Wifi | Embervadászat 2.0

Net

Személyes adatok egy dobozos kóla áráért

MTI

2009. április 16., csütörtök 11:30 | Frissítve: 2009. április 16.

Fillérekért cserélnek gazdát az internetes feketegazdaságban a személyes adatok, a csapolható bankszámla-hozzáféréshez meg már 200 ezer forintért hozzá lehet jutni.

A Symantec informatikai biztonsági cég csütörtökön Budapesten sajtótájékoztatón nyilvánosságra hozott éves internetbiztonsági jelentése szerint a felhasználók bizalmas adatait célba vevő, kártékony programkódok aktivitása 2008-ban is nagy iramban nőtt.

Tavaly a cégnek az új kártékony kódok ellen több mint 1,6 millió új azonosítót kellett létrehoznia, amelyekkel havi átlagban több mint 245

Hasonló cikkek

- Vérdíj a vírusírók fejére
- Vasárnap a zombik sem dolgoznak

Címkefelhő

adatvédelem, bing, cenzúra, európai bizottság, facebook, gmail, google, internet, internet explorer, kereső, közösségi oldalak, microsoft, pirate bay, street view, torrent, twitter, upc ügyfélkapu, wikipedia, youtube

A tech rovat cikkei

- Nem volt elfogult a bíró a Pirate Bay perében

Computer disks with bank account info on 25 million people were lost

Jaikumar Vijayan Today's Top Stories ▸ or Other Security Stories ▸

Comments (3) Recommendations: 103 — Recommend this article

Magyarország sem kivétel!

CDSys
COMPLIANCE DATA SYSTEMS Kft.

ITcafé

CÍMLAP HÍREK CIKKEK FÓRUM KARR

gazdaság társadalom technológia net szoftver

A veszprémi egyetem mindenképp felelős az adatvesztésért - I

A veszprémi egyetem adatvesztésért

Szerző: Dajkó Pál | Dátum: 2008-12-11 20:28 | Rovat: Biztons

Az adatvédelmi szakértő szerint az egyeten rejtőzhet el, felelősség terheli a történteké

A héten egy olyan súlyos adatvédelmi ügyről különlegessége miatt vált fontossá, hanem a veszprémi Pannon Egyetem tökéletesen felkés kapcsán nyilatkozó mértékadó biztonságtechn hogy a digitalizáció miatt az adatkezelési inci gyakoriak, mint az ilyen ügyek sorozatait produkáló nyugati társadalmakban, ám hazánkban még ott sem tartunk, ahol ezek az országok, pedig még náluk is komoly problémákat okoz az adatvédelem mind technikai, mind jogi szempontból.

MINISZTERELNÖKI HIVATAL

INFORMATIKAI BIZTONSÁGI FELÜGYELŐ

Részletes jelentés
a Központi Elektronikus Szolgáltató Rendszer
egyes szolgáltatásainak üzemzavarairól

2009. január 19. és február 7. között három olyan üzemzavar következett be a Központi Elektronikus Szolgáltató Rendszer szolgáltatásaiban, amelyek nagy nyilvánosságot kaptak. Az eseményekkel kapcsolatban parlamenti kérdés került benyújtásra és interpelláció hangzott el, illetve az eseményekkel kapcsolatban tájékoztatást kért az Országgyűlés Gazdasági és Informatikai Bizottságának Informatikai Albizottsága.

Az események az érintett szervezetek, valamint az informatikai biztonsági felügyelő által kivizsgálásra kerültek. Mindhárom esetben megállapítást nyertek az eseményeket kiváltó okok, és azok felelősei, és a további, hasonló eseményeket előidéző okok megelőzése érdekében az érintett szervezetek intézkedési terveket készítettek.

Az ellenőrzés során megállapítást nyert, hogy **mindhárom esemény ugyanazon okra vezethető vissza**: a nem kellő gondossággal leteszteltt programmódosítások éles üzembe állítására, **a változáskezeléssel kapcsolatos – informatikai biztonság körébe tartozó – szabályok és eljárásrendek személyi mulasztás miatt bekövetkezett figyelmen kívül hagyására**.

Mi lehet veszélyben?

CDSYS
COMPLIANCE DATA SYSTEMS Kft.

- Hitelkártya és bankkártya adatok
  - Kártyaszám, PIN, CVC2, CVV2 kódok, lejárat
  - Mágnescsík adatok
  - Kártyabirtokos adatai
- Pénzforgalmi és értékpapír számlák
  - Tulajdonosok adatai
  - Egyenleg
  - Forgalom
- Belső működéssel kapcsolatos adatok
  - Munkavállalói személyes adatok, bérek
  - Pénzügyi eredmény
  - Büdzsék, beruházási tervek
  - Biztonsággal, védelemmel kapcsolatos információk
- Versenypiaci előnyt biztosító információk
  - Kiemelt ügyfélkör adatai
  - Új termék kialakításával kapcsolatos információk
  - Marketingstratégia és tervek
- Termékfejlesztési tervek
  - K+F eredmények
- Vállalati stratégia
  - Terjeszkedés
  - Felvásárlás
  - Eladás

Az adatvesztés, adatszivárgás növekvő aggodalmat szül.

CDSYS
COMPLIANCE DATA SYSTEMS Kft.

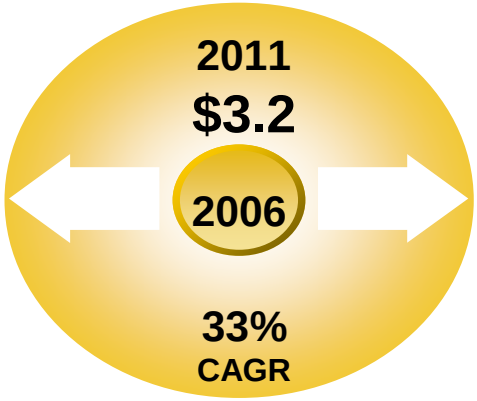
A biztonsági vezetők legfőbb gondjai

- **A biztonsági vezetők 85%-a** jelentett legalább egy olyan biztonsági eseményt, incidenst, amely adatszivárgással összefüggő volt – tavaly[2]

  - 63% esetében észleltek 6-20 biztonsági eseményt, ami személyes információkat is érintett.

- **52%** gondolja, hogy a DLP meghatározó, markáns eleme lesz a biztonsági büdzsének[1]
- **216 millió** személyes adatot ért támadás 2005 óta
- 2007-ben az incidenesek következtében **6.3 mrd dollár** költség keletkezett – 2006-ban ez 4.8 mrd volt .
- Az esetek **40%-ában a betörés „kiváltója” 3. fél,** - vállalat, szervezet, outsource vagy szerződött partner.[3]

Előrejelzés:
2011-re 2-3 milliárd dollárt fordítanak megelőzésre



IDC May 2007, “Information Protection and Control”

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Nov 12, 2008 08:00 ET

eDiscovery and Data Loss Prevention (DLP) Market Poised to Grow to Over $2 Billion by 2012

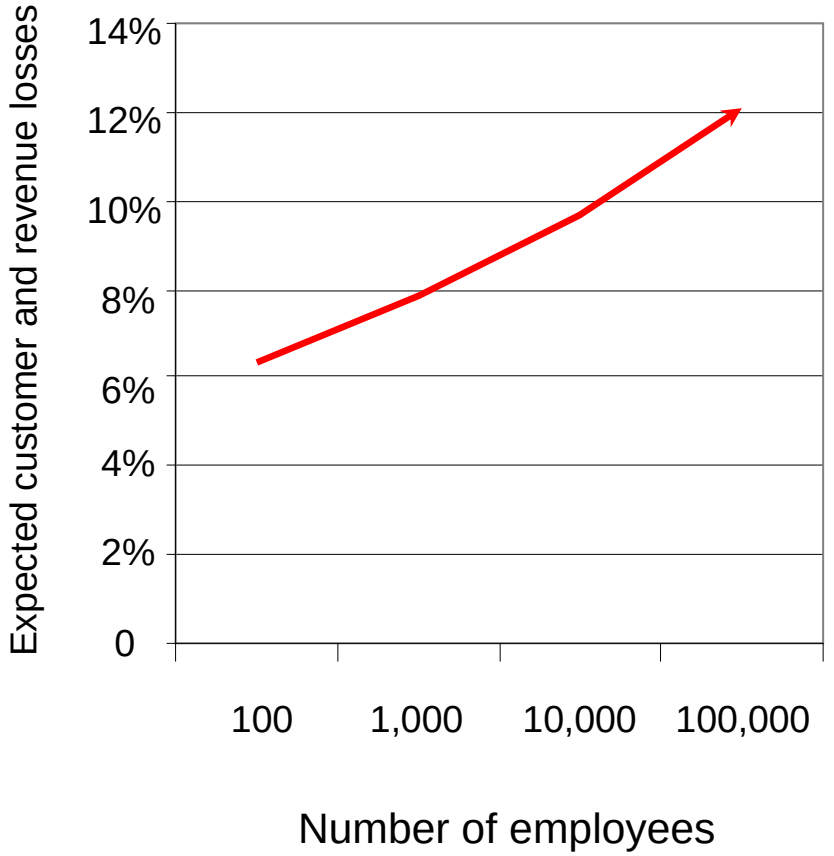
A New Study by The Radicati Group, Inc. Shows an Increasing Demand for eDiscovery and DLP Solutions Coming From Organizations in Non-Regulated Industries

PALO ALTO, CA--(Marketwire - November 12, 2008) - The latest study by The Radicati Group, Inc. "eDiscovery and Data Loss Prevention Market 2008 - 2012" provides market size, four-year forecasts, and discusses legislative and technology issues of the eDiscovery and DLP market. The study also provides an analysis of the leading market players.

… és a betörések költségesek

Közvetett és közvetlen költségek a nyilvánosan jelentett adatlopások kapcsán

- Kárelhárítási folyamat költsége $100 - 300 elveszített személyes adatonként*
  - Felhasználó értesítése
  - Hitel monitorozás
  - Rendszer helyreállítás
  - Nyomozati költségek
  - Audit költségek
  - Hitelkártyák letiltása, újabbak készítése
- Jelentős közvetett költségek*
  - A márka értékének, piacnak illetve a felhasználók bizalmának vesztése
  - Jogi eljárások, bírság
  - Részvény vagy árbevétel csökkenése



*July 2007, IT Policy Compliance Group

Nemrég történt

CDSYS
COMPLIANCE DATA SYSTEMS Kft.

technet

CÍMLAP | TECHTUD | PDAMÁNIA | TELEFON | SZÁMÍTÓGÉP | GPS | FÓRUM

ITT VAGY MOST : TECHNET : TECHTUD

MÁJ 06 2009

Óriási adatvesztést hallgattak el

Mi a megoldás arra, ha több tízezer ember személyes adatai kompromittálódnak? Egyesek szerint nem szabad figyelmeztetni a nyilvánosságot.

Legalább harminckétezer ember személyes adatai k
ChoicePoint cégeknek. A szivárgás 2004. júniusától
mindenféle információt erről.

Az ok? Az Amerikai Postai Vizsgálati Szolgálat erre
se tudtak a rájuk leselkedő potenciális veszélyről. Te
felhasználva postafiókokat béreltek, majd hitelkártyá

A LexisNexis és a ChoicePoint a múltban sem védte
arra, hogy nagyjából 45-50 esetben nyertek ki jogosu
rendszeréből. A 2004 februári esetről, amiben 310 00
megkésve, 2005 áprilisában értesültek az érintettek.

Az akkori esetekben azzal védekeztek, hogy „egy tö
ügyfeleinket ilyen esetben". Most részben azzal véde
amelyek egykoron a LexisNexis vagy a ChoicePoint

Forrás: The Register
Cimkék: Hacker Adatlopás Adatvédelem

The New York Times

Global Business

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Search Business: News, Stocks, Funds, Companies — Go
Financial Tools: Select a Financial Tool
More in Business »: Global Business | Markets | Economy

E.U. to Consider More Stringent Reporting of Data Breaches

By KEVIN J. O'BRIEN
Published: May 6, 2009

SIGN IN TO E-MAIL
PRINT
SHARE

BERLIN — The European Commission said Tuesday that it would pursue a new law that would require most businesses, agencies and organizations in Europe to notify consumers when they lose sensitive customer data.

Az USA-ban már ma is kötelező a nyilvánosságra hozatal!

Az EU is tervezi!

A PCI DSS szabvány

- **P**ayment **C**ard **I**ndustry
  Data **S**ecurity **S**tandard

- Az 5 nagy kártyakibocsátót egyesítő PCI Security Standards Council hozta létre, 2004-ben
- **Cél**: A kártyaadatokkal való visszaélések csökkentése
- **Eszköz**: Szigorú információbiztonsági követelmények
- **Hatókör**: Minden olyan szervezet, amely a fizetőkártyák adatainak kezelésével, továbbításával vagy tárolásával foglalkozik.

PCI DSS követelmények

CDSYS
COMPLIANCE DATA SYSTEMS Kft.

1. A kártyabirtokos adatainak védelmére tűzfalat kell telepíteni és üzemeltetni.
2. Nem szabad a gyártók által használt alapbeállítású rendszerjelszavakat és beállításokat használni.
3. Védeni kell a kártyabirtokosok tárolt adatait.
4. A nyílt hálózatokon történő adatátvitel során titkosítani kell a kártyabirtokos adatait.
5. Vírusvédelmi megoldásokat kell használni, és azokat rendszeresen frissíteni.
6. Biztonságos rendszereket és alkalmazásokat kell fejleszteni és üzemeltetni.
7. A kártyabirtokos adataihoz csak az férhessen hozzá, akire az tartozik.
8. Minden személy, aki hozzáférhet a rendszerhez, rendelkezzen egyedi azonosítóval.
9. A kártyabirtokos adataihoz való fizikai hozzáférést meg kell akadályozni.
10. A hálózati erőforrásokhoz és a kártyabirtokos adataihoz történő hozzáférést monitorozni kell.
11. A biztonsági rendszereket és folyamatokat rendszeresen tesztelni kell.
12. Információbiztonsági szabályzatot kell fenntartani.

PCI DSS határidők

Határidők a megfelelőség elérésére	
2009. szeptember 30.	**Az adattárolás megtiltása a Level 1 és Level 2 kereskedők részére** A Visa visszaigazolást kér arról, hogy kártyaadatokat a tranzakciók engedélyezése után nem tárolnak az kereskedők. (Pl. kártyaszámok, mágnescsík információk, biztonsági kódok, CVC, CVV, PIN, stb.)
2010. szeptember 30.	**PCI DSS megfelelőség validálási határideje a Level 1 kereskedők részére** A Visa hivatalosan validált igazolást kér arról, hogy a kereskedők teljes körűen megfelelnek a PCI DSS előírásainak, azaz a kereskedőknek auditáltatniuk kell magukat egy erre feljogosított auditorral.

Adatszivárgás válság idején?

- A pénzügyi szektor kiemelten érintett
- Leépítések, elbocsájtások
- Bizonytalanság

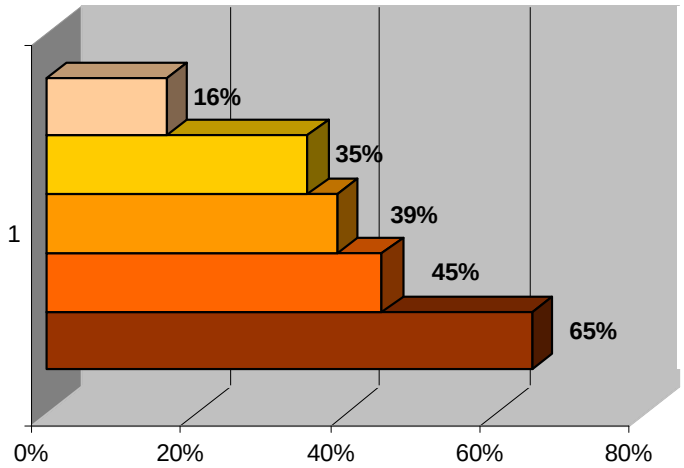
- Növekvő kísértés:
  - Visszaélés a jogosan kezelt adatokkal
  - Adatok jogtalan megszerzése
  - Jelentős a kereslet az adatokra

- **Megnövekedett az adatszivárgások kockázata!**

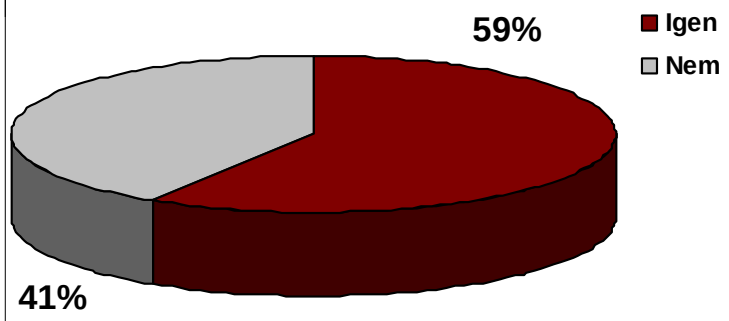
Ponemon study* –
Kérdőíves DLP felmérés a kilépőkről

CDSYS
COMPLIANCE DATA SYSTEMS Kft.

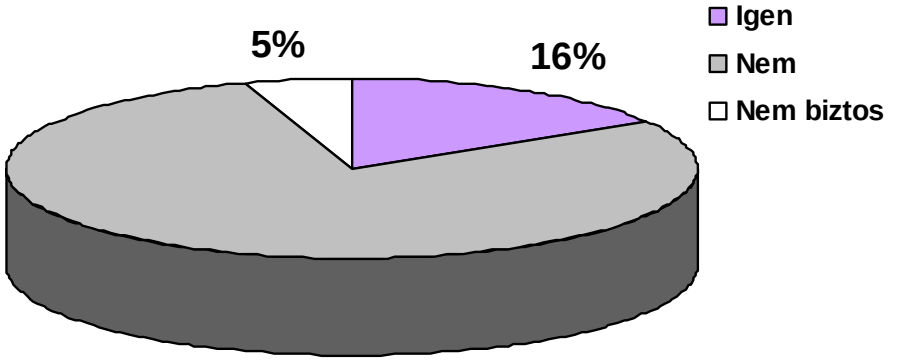
Milyen típusú bizalmas, fontos vállalati adatokat, információkat tartott meg miután elhagyta a vállalatot?



Tartott-e meg bizalmas adatokat miután elhagyta korábbi munkaadóját?



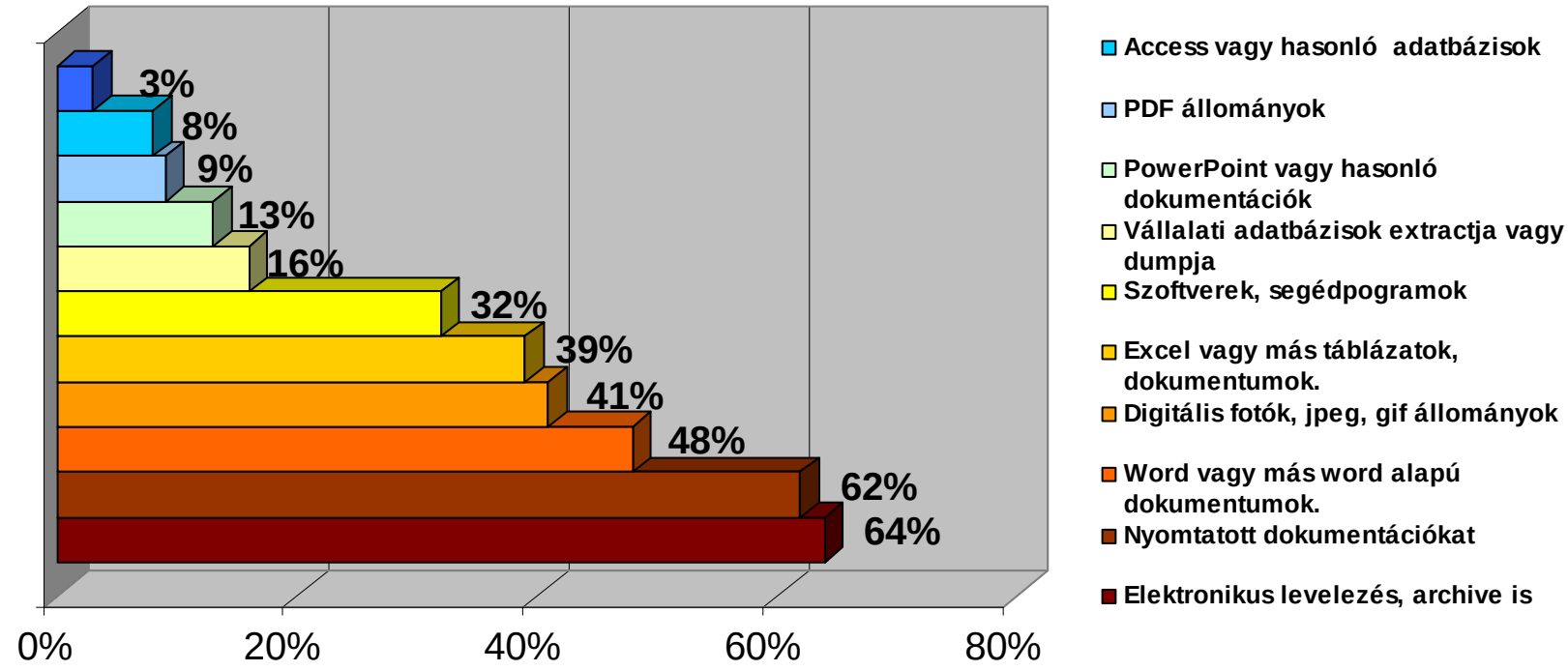
Engedélyezte a munkadója hogy ezeket a fontos, bizalmas adatokat megtartsa, birtokolja?



*Data Loss Risks During Downsizing, Ponemon Institute LLC, February 23, 2009

Ponemon study –
Kérdőíves DLP felmérés a kilépőkről

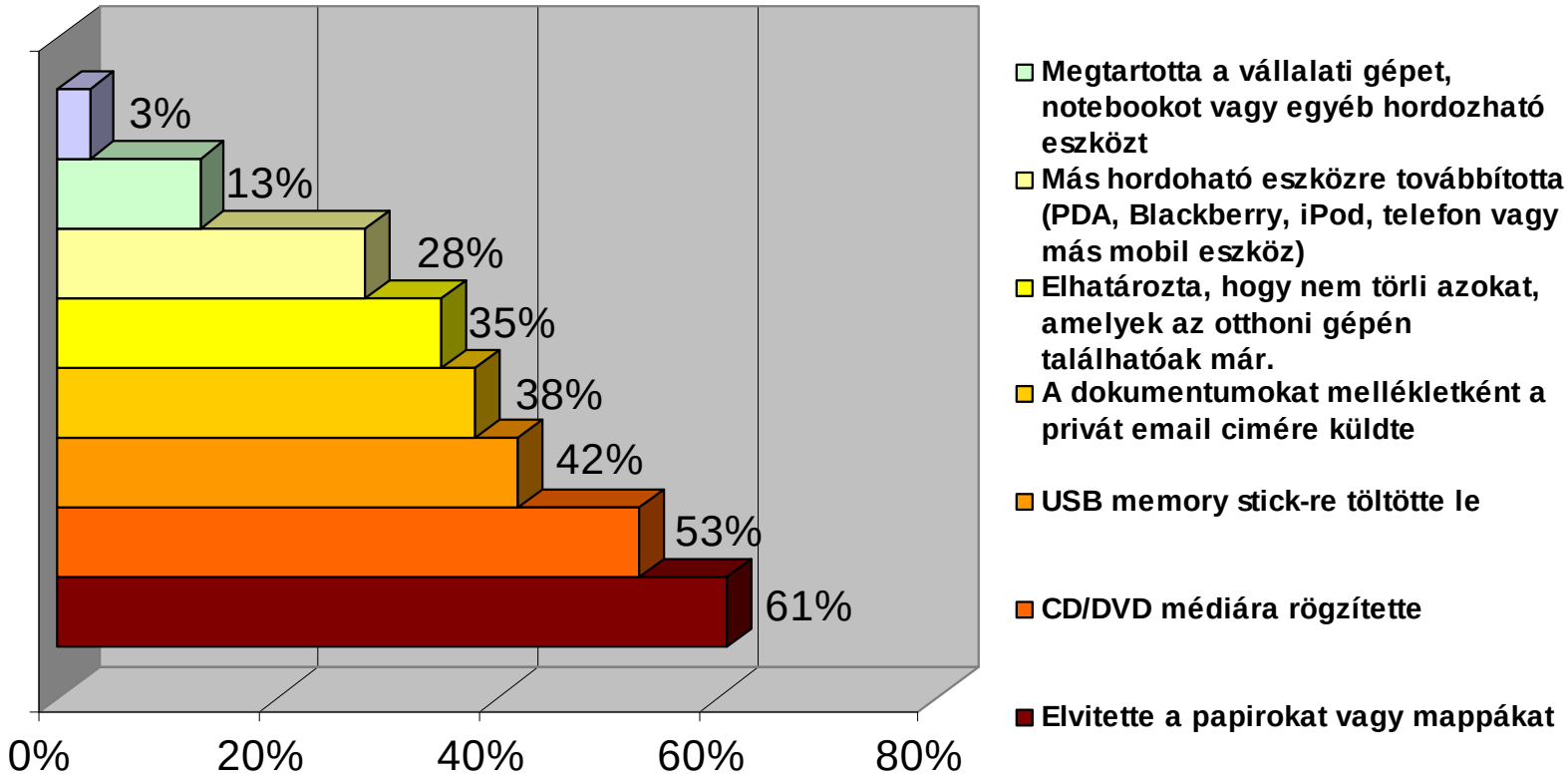
Milyen elektronikus vagy papir alapú információt tartott meg miután elhagyta a vállalatot?



Összesen: 338%,
azaz egy átlagos kilépő a fentiek közül több mint 3 félét vitt el!

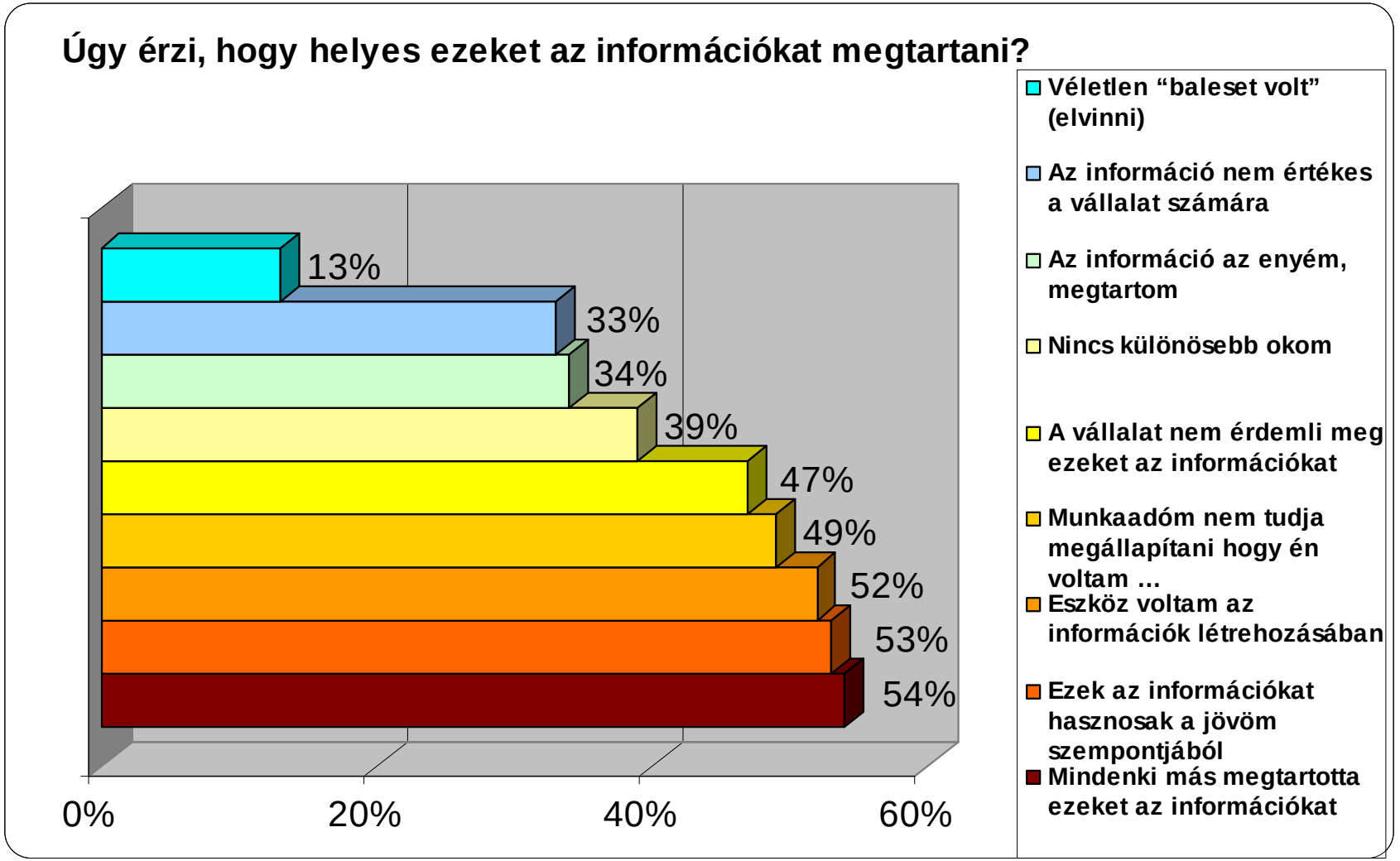
Ponemon study –
Kérdőíves DLP felmérés a kilépőkről

Hogyan juttatta ki a fontos, bizalmas vállalati adatokat a volt vállalatának rendszereiből vagy hálózatából?

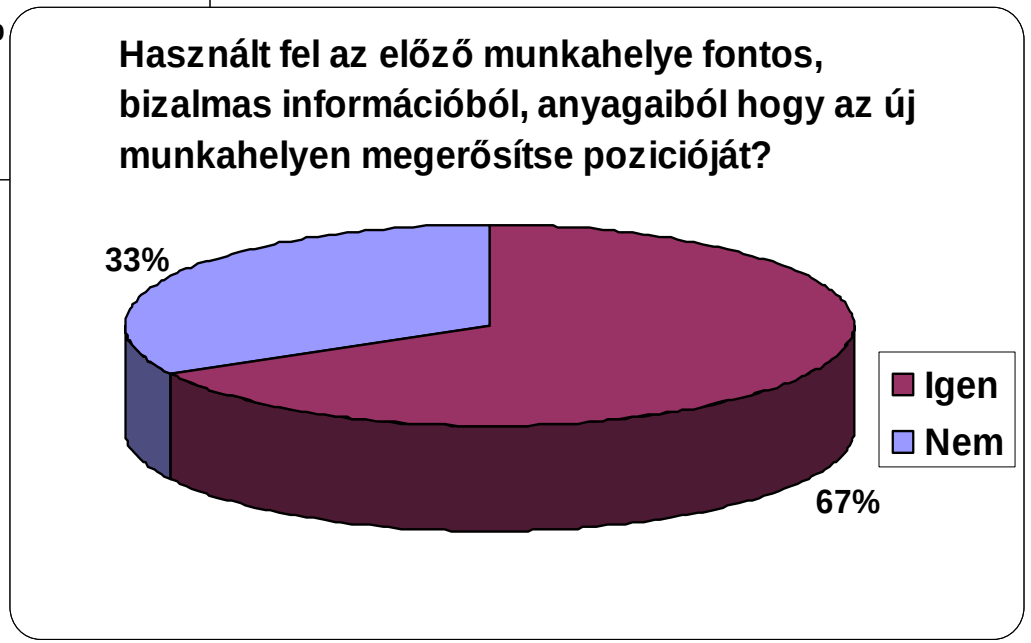


Összesen: 273%,
azaz egy átlagos kilépő a fentiek közül kb. 3 csatornát használt!

Ponemon study –
Kérdőíves DLP felmérés a kilépőkről



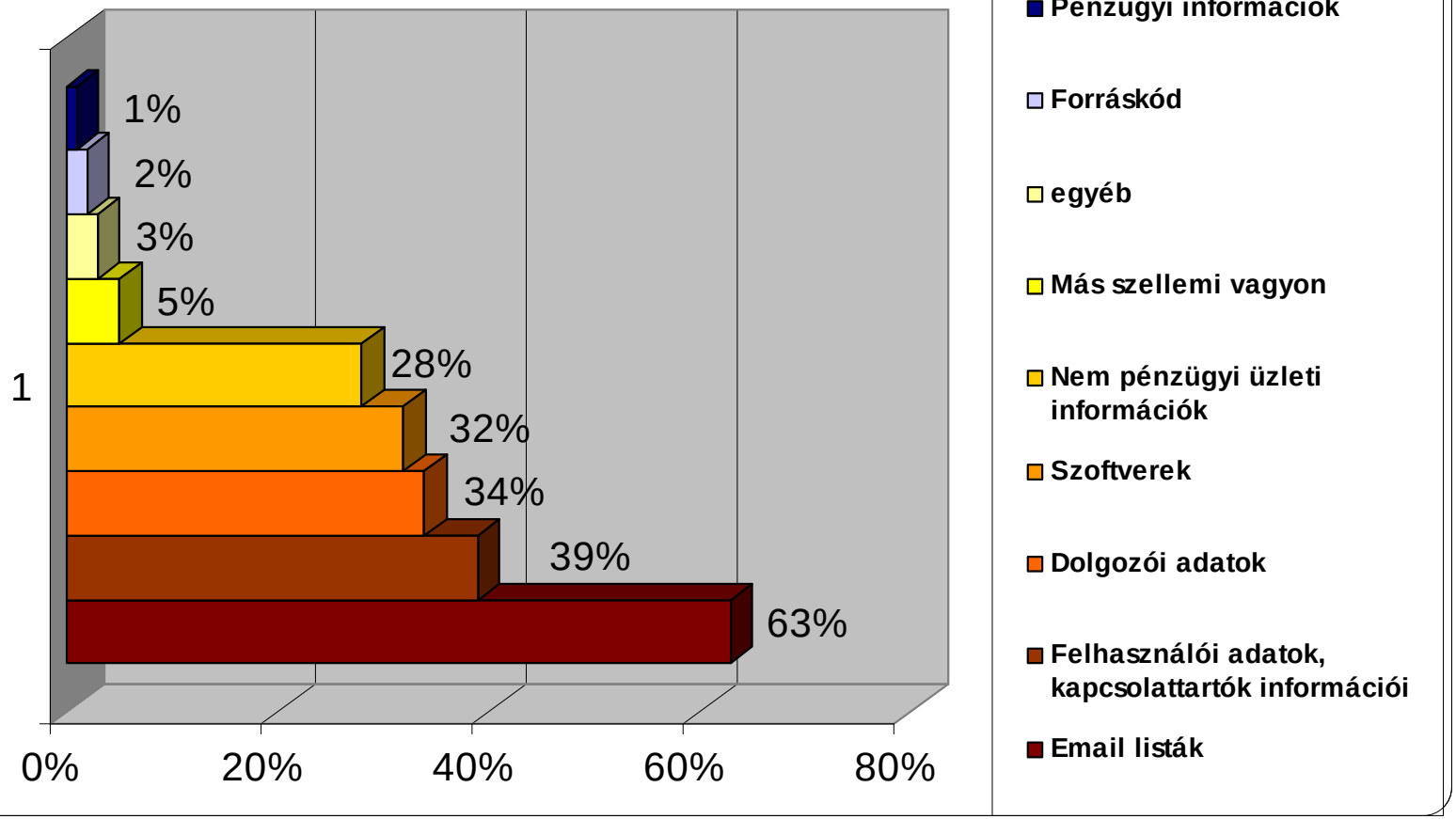
Ponemon study –
Kérdőíves DLP felmérés a kilépőkről



Ponemon study –
Kérdőíves DLP felmérés a kilépőkről

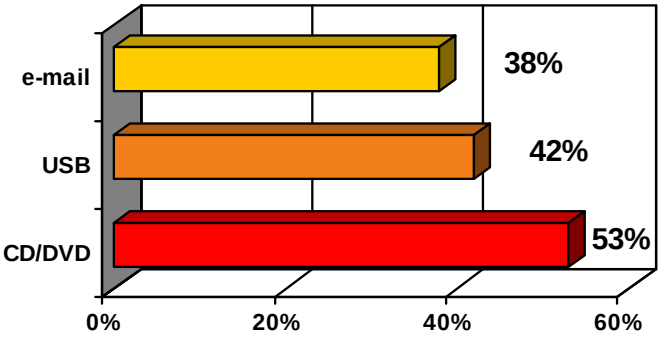
CDSYS
COMPLIANCE DATA SYSTEMS Kft.

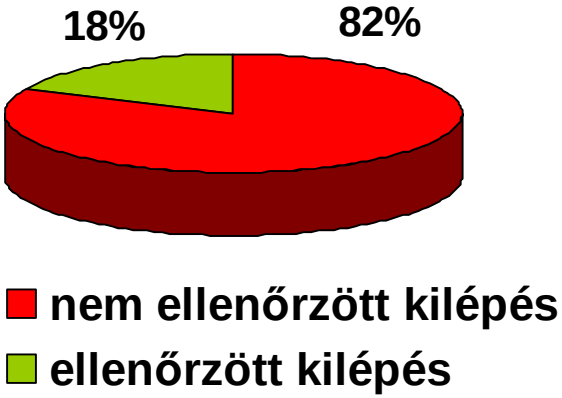
Milyen jellegű információkat, adatokat használt vagy tervez felhasználni az előző munkadó tulajdonából?



Ponemon – Kulcs megállapítások

- **A kérdőívre válaszolók közül**
  - **59% vitt el adatot a munkaadó engedélye nélkül.**
  - 38% küldte csatolt állományként a saját email címére,
  - 42% USB drive-ra és
  - 53%-a töltött le információt CD-re vagy DVD-re





- 82% állítja, hogy munkaadóik nem auditálták vagy ellenőrizték az elektronikus vagy papír alapú dokumentumokat, mielőtt elhagyták a munkahelyeiket

- 24%-uk azután is rendelkezett hozzáféréssel a hálózathoz, számítógéphez hogy már elhagyta a vállalatot.

Ráismer a saját vállalatára a példákban?

- Ráismer a saját vállalatára a példákban?
- Elképzelhető hogy elbocsátott alkalmazottaik hasonlóképpen cselekedtek?
- Valóban meg tudja akadályozni az adatok illetéktelen felhasználását; hogyan?
- Biztos benne, hogy alkalmazottai csak azokhoz az információkhoz férnek hozzá, amelyek a munkájukhoz elengedhetetlenül szükségesek?
- Biztos, hogy a működő eljárások, munkafolyamatok biztonsági szempontból is megfelelőek, személyes információ nincsen veszélyeztetve?