



cutting through complexity™

Sú vaše dáta v ohrození?

Pavol Adamec
Oracle Security Day, Bratislava

17.2.2011



Spomienky na minulosť ... Aký bude svet v roku 2010?

Politicky

- Rozsiahle vládne zásahy
- Protekcionizmus
- Elektronická špionáž
- Elektronická vojna
- Terorizmus
- Regionálne zoskupenia štátov

Ekonomicky

- Znižovanie nákladov prostredníctvom outsourcingu a offshoringu
- Outsourcing netradičných funkcií
- Zníženie investícií do inovácií
- Menej nových produktov a riešení
- Zneužitie technológií organizovaným zločinom

Právne

- Nárast regulácie a legislatívnej záťaže
- Vyššia miera penalizácie a výšky pokút
- Pokračovanie sporov medzi ochranou súkromia, informačnou bezpečnosťou a národnou bezpečnosťou

Socio-kultúrne

- Prelínanie reálneho a virtuálneho života
- Kybernetická šikana a prenasledovanie

Technologicky

- Zavádzanie cloud-computingu
- Závislosť na kritickej infraštruktúre

Zdroj: Information Security Forum, Máj 2009

Spomienky na minulosť ...

Kľúčové trendy 2010

1

- **Nárast záťaže regulácie** – Stále viac organizácií je nútených venovať viac času pochopeniu a reagovaniu meniacemu sa regulatórnemu prostrediu ako proaktívnemu riadeniu rizík.
 - Identifikácia a riadenie rizík .
 - Nová a novelizovaná legislatíva
 - Vzťahy s tretími stranami
 - Vládne investície

2

- **Meniaci sa smer hrozieb** – Bezpečnostné hrozby pokračujú v nepredvídateľnom vývoji.
 - Rozšírené vývoj škodlivého softvéru
 - Cielené útoky
 - Vnútorné hrozby

3

- **Globálna ekonomická kríza** – Kríza vyvolala rapídny rozvoj biznis modelov a re-prioritizáciu naprieč všetkými aspektmi podnikania.
 - Nové kanály dodania a nové usporiadania podnikania
 - Monetizácia existujúcich aktív (vrátane dát a informačných aktív)

A čo dnes?

Kľúčové výzvy pre CISO v roku 2011

Veľa sa toho nezmenilo:

- ... an increasingly demanding business environment ...
- ... a rapidly evolving threat landscape ...
- ... Empowered employees requiring agility, flexibility, mobility, and better collaboration ...

Forrester, Twelve Recommendations For Your 2011 Security Strategy, december 2010

2010 – „hospodárska kríza“ = 2011

Viaceré indikátory ukazujú, že globálne výdavky na IT rastú

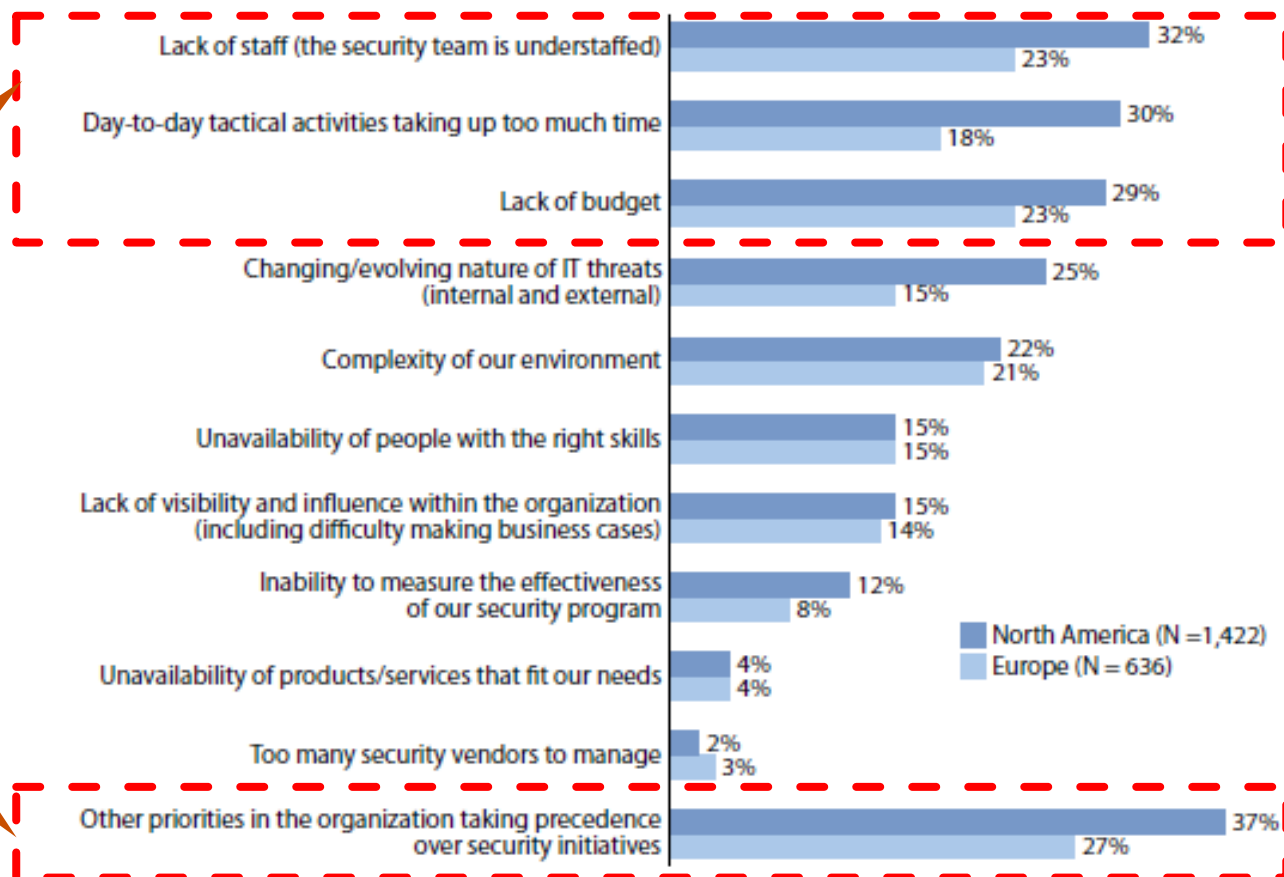
- Gartner predikuje rast výdavkov na IT (vrátane telekomunikačných služieb) v roku 2011 o 5,1% oproti roku 2010
- Forrester predikuje rast výdavkov na IT v roku 2011 o 7,1% oproti roku 2010
- Predpokladá sa, že výdavky v roku 2011 prekročia predkrízovú úroveň, t.j. rok 2008
- Kto prežil krízu, ten prežil a začína sa pozerat' do budúcnosti

V podmienkach Slovenska tiež aspekt hospodárskej krízy doznal

- Verejná správa a súkromný sektor majú v SR zásadne odlišný charakter v IT rozpočtoch
- Súkromné spoločnosti prechádzajú od útlmového a šetriaceho režimu k rozvojovým projektom
- Viaceré spoločnosti ovplyvňujú integračné a konsolidačné projekty

Bezpečnosť prehráva na body

"Please rate the following IT security challenges in your firm."
 (Respondents selecting a "Major challenge" for the following)



Base: 2,058 North American and European IT executives and technology decision-makers

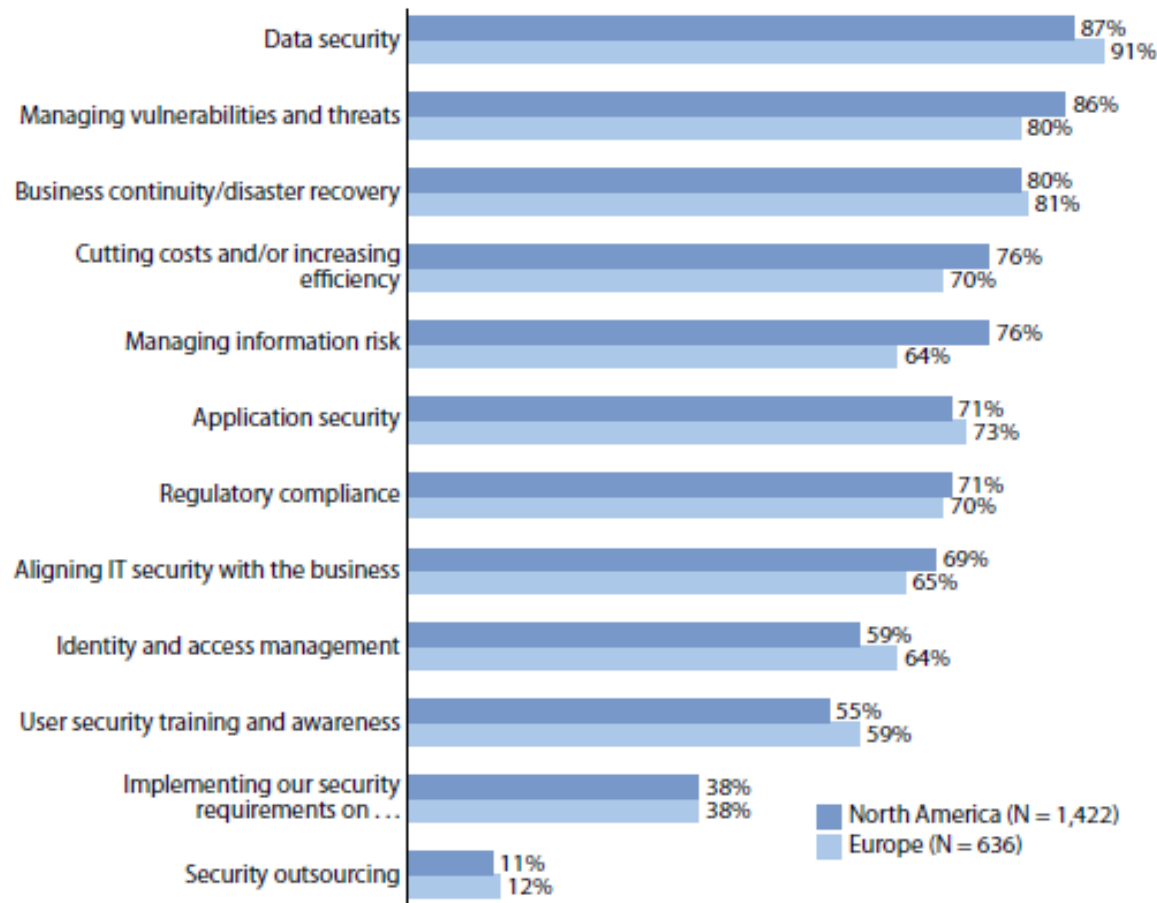
Source: Forrester's Forrsights Security Survey, Q3 2010

Iné priority posúvajú bezpečnosť na vedľajšiu koľaj

Výdavky na IT bezpečnosť

“Which of the following initiatives are likely to be your firm’s/organization’s top IT security priorities over the next 12 months?”

(Respondents selecting “high” or “critical priority”)



Base: 2,058 North American and European IT executives and technology decision-makers

Source: Forrester’s ForSights Security Survey, Q3 2010

Výdavky na IT bezpečnosť

2.1 Average Differences Reported Between 2009 Budgets and Actual Spending

LARGE ENTERPRISES				MIDRANGE ENTERPRISES			
N=51-122				N=21-77			
	Organizations budgeting in 2010	Average spending per employee	Average growth from 2009		Organizations budgeting in 2010	Average spending per employee	Average growth from 2009
IT SECURITY							
Firewalls/VPNs	65%	\$77	+5.6%	Firewalls/VPNs	77%	\$164	+1.9%
Security mgmt.	64%	\$79	+4.5%	Antivirus	76%	\$139	+0.4%
Antivirus	63%	\$62	+2.6%	E-mail/Web gateways	68%	\$414	+12.4%
E-mail/Web gateways	62%	\$60	+3.2%	Encryption	68%	\$284	+4.2%
Data loss prevention	61%	\$96	+8.4%	Data loss prevention	68%	\$234	+9.6%
Configuration mgmt.	60%	\$50	+3.0%	Security mgmt.	66%	\$216	+2.9%
Encryption	59%	\$50	+0.1%	Content monitoring	65%	\$304	+1.0%
Content monitoring	59%	\$41	+4.9%	Configuration mgmt.	59%	\$347	+6.6%
Authentication mgmt.	57%	\$36	+4.0%	Authentication mgmt.	57%	\$416	-1.0%
Access control	56%	\$82	+3.3%	Access control	54%	\$297	+8.7%
Identity mgmt.	56%	\$63	+2.3%	Identity mgmt.	52%	\$444	+2.9%
Rights mgmt.	50%	\$35	+1.5%	Rights mgmt.	35%	\$853	+4.0%

Zdroj: CIO Insight www.cioinsight.com, A Tale of Two Investment Trends, 2010

Kľúčové výzvy pre CISO v roku 2011

Rastúca komplexnosť business prostredia

- Outsourcing, komplexná výmena business dát, nové podnikateľské modely, požiadavky legislatívy a regulátorov, ...

Rýchlo sa meniaci charakter hrozieb

- nárast cieľených útokov, väčšia dostupnosť komplexných dát zamestnancom, ...

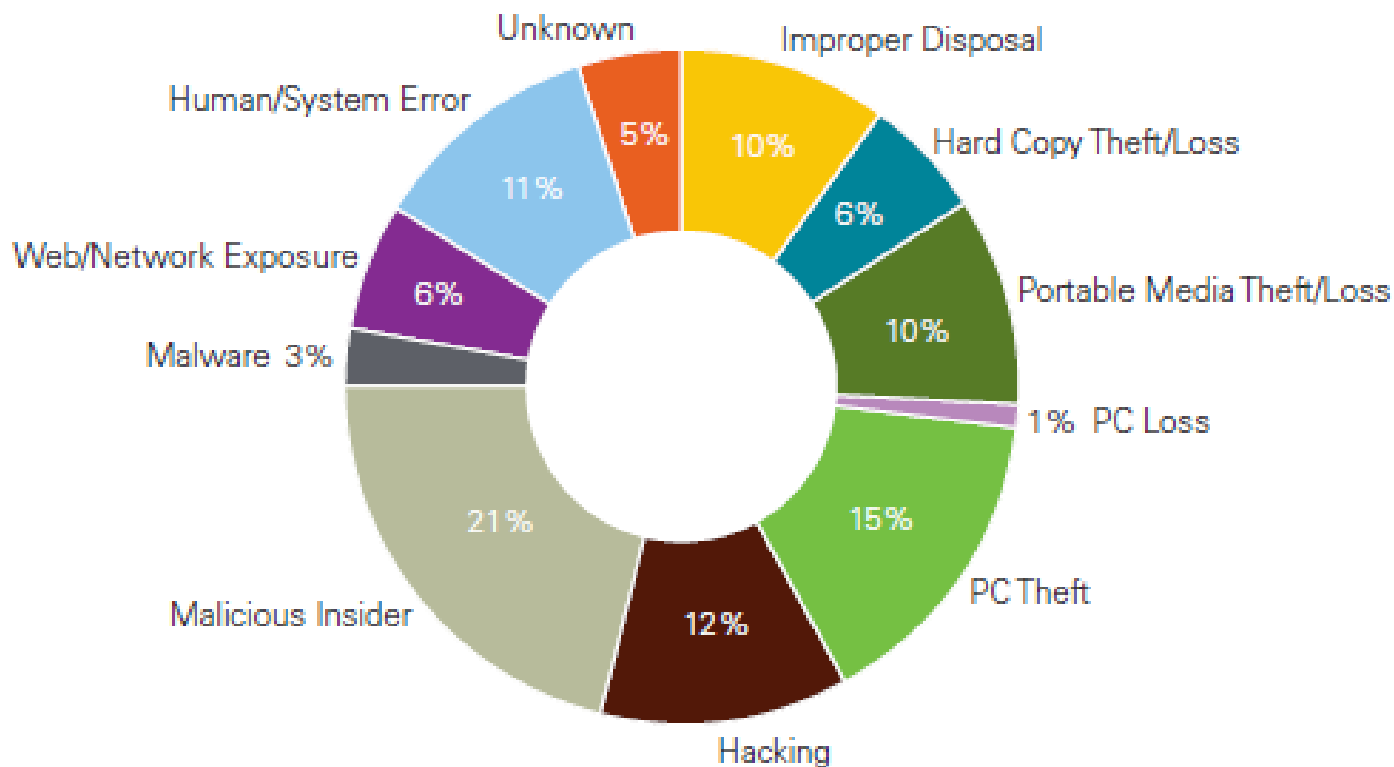
Mobilita, agilita, flexibilita ...

- tablety, smartphones, sociálne siete, cloud computing, tlak na time-to-market pre nové produkty ...

Zdroj: Forrester, Twelve Recommendations For Your 2011 Security Strategy, december 2010

KPMG Data Loss Barometer, 2010

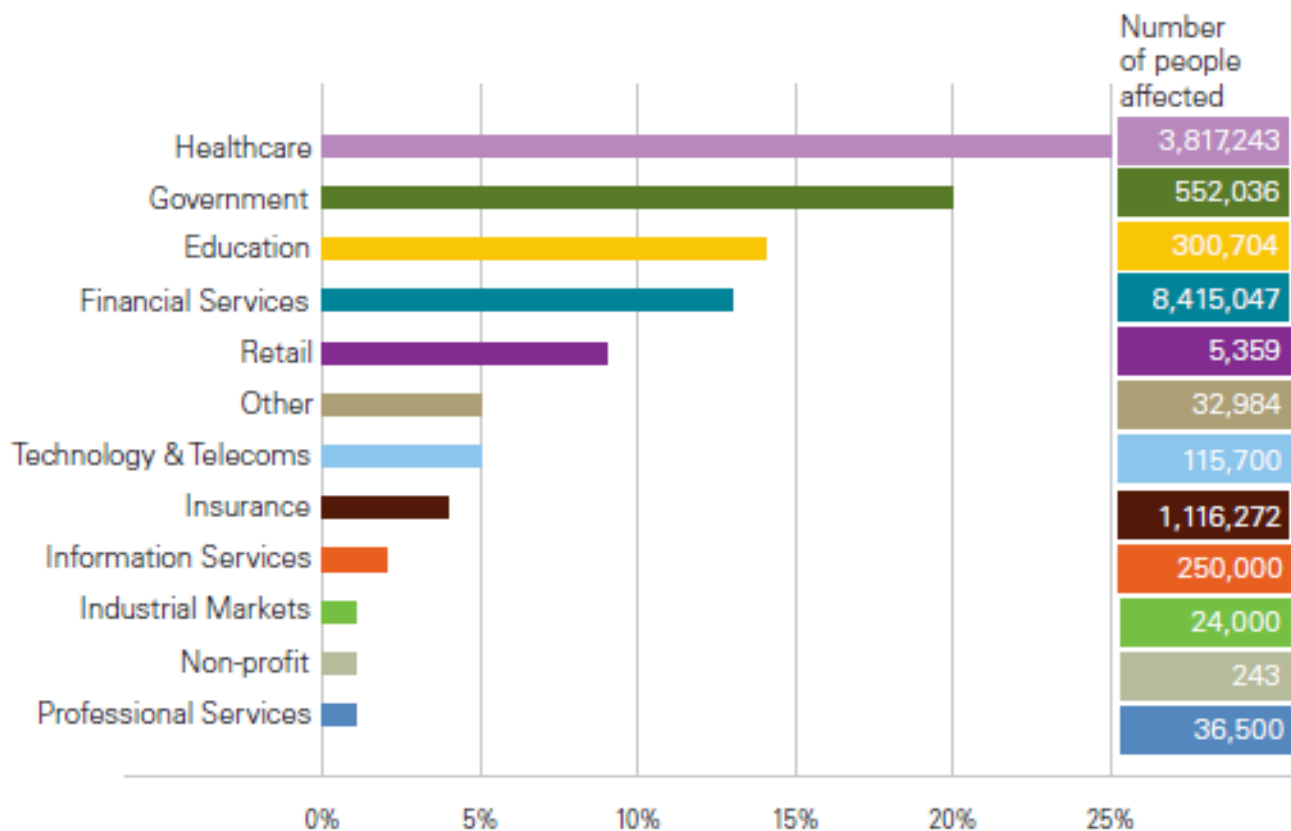
Podiel na celkovom počte incidentov strát údajov podľa spôsobu úniku



Where has all the data gone ...

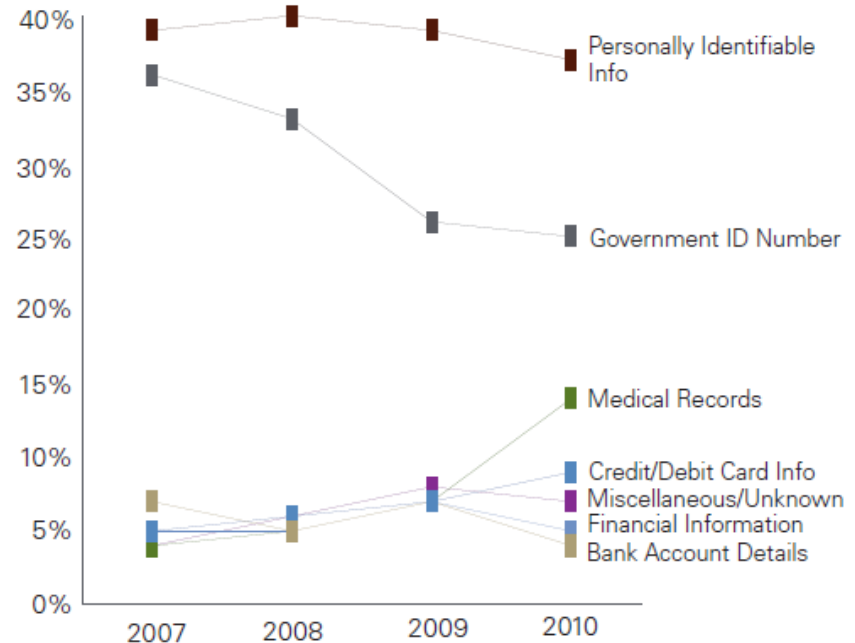
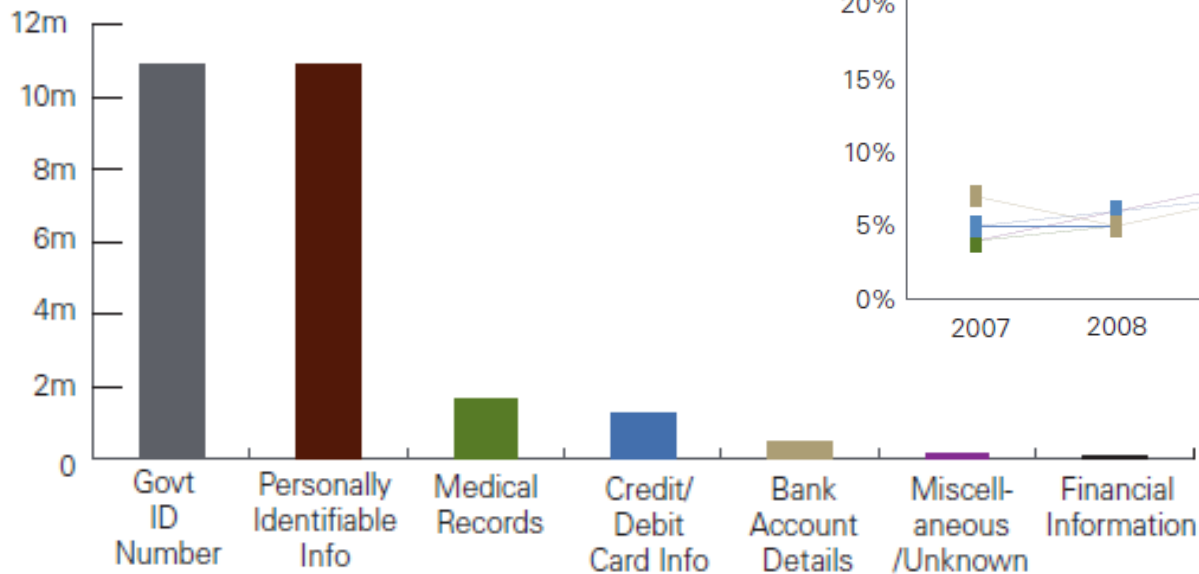
KPMG Data Loss Barometer, 2010

Podiel na celkovom počte incidentov podľa sektoru a počtu dotknutých osôb



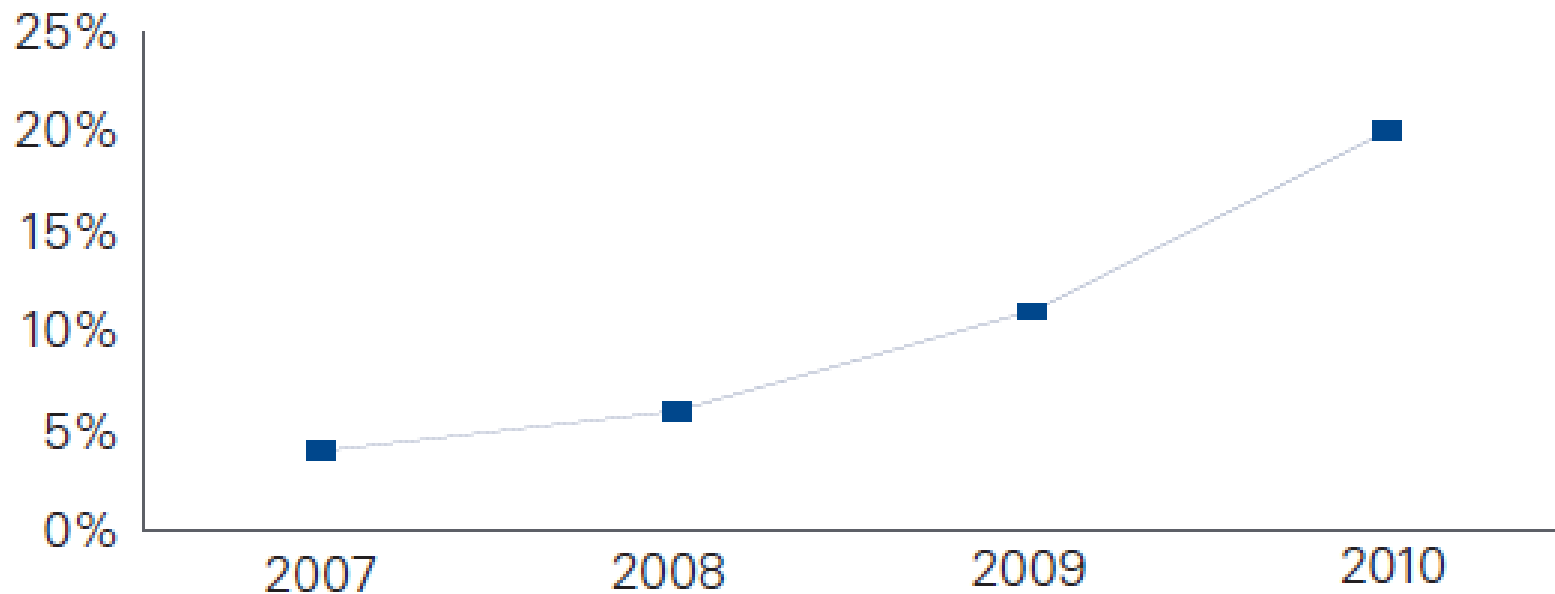
KPMG Data Loss Barometer, 2010

Počtu dotknutých osôb podľa typu uniknutého údaju



KPMG Data Loss Barometer, 2010

Podiel na vlastných zamestnancov na celkovom počte incidentov



Where has all the data gone ...

Prieskum KPMG v UK a Mishcon de Reya, analýza 100 prípadov krádeže údajov z posledných rokov:

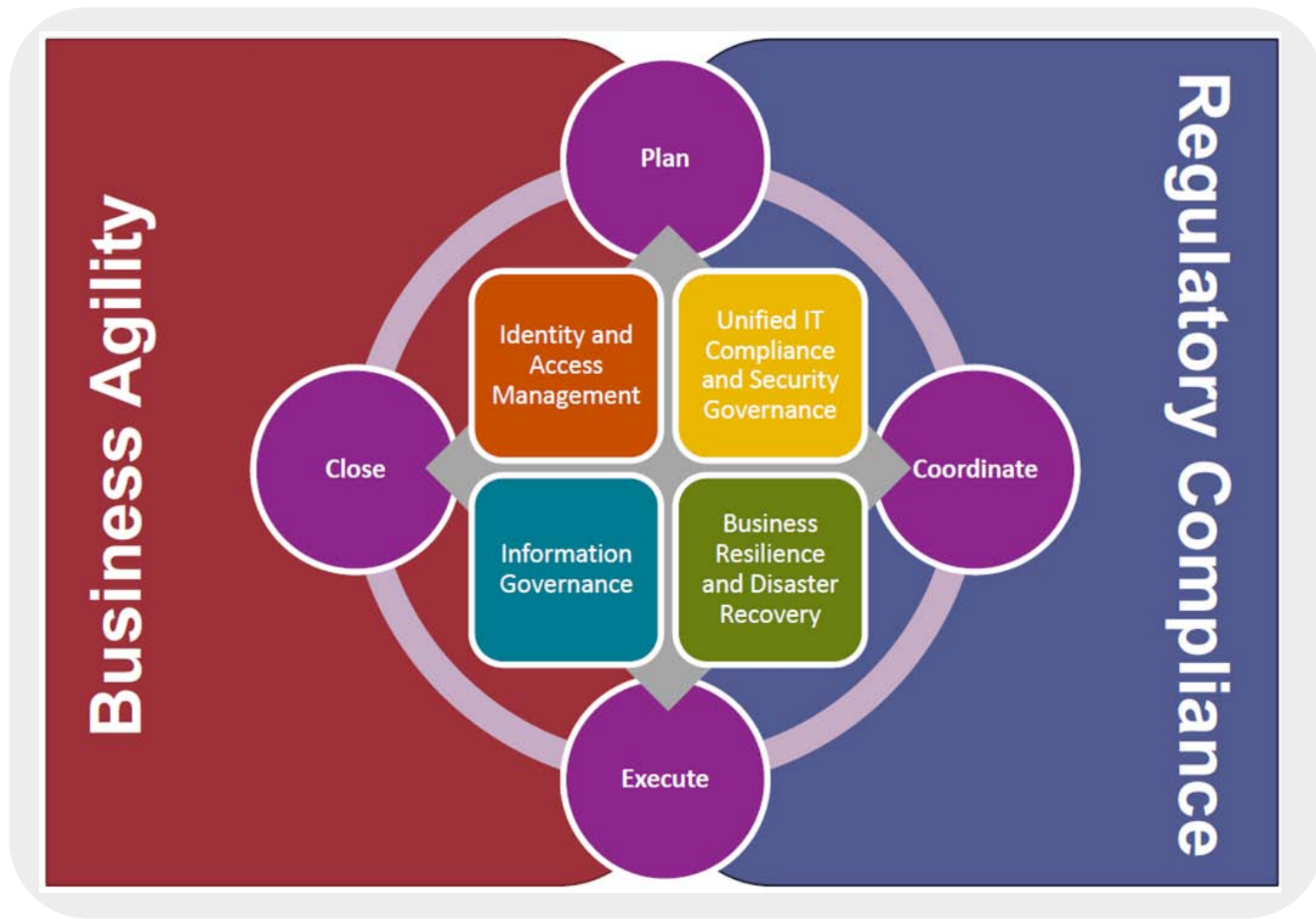
- Počet krádeží sa od roku 2006 do 2008 zdvojnásobil
- 90% krádeží spáchal jednotlivec
- Údaje nie sú kradnuté náhodne:
 - 70% páchatel'ov zmenilo „dres“ ku konkurencii
 - 23% si založilo vlastnú firmu, konkurujúcu pôvodnému zamestnávateľovi
 - 1% predalo údaje konkurencii
- 46% únikov sa udialo cez e-mail, 9% na elektronických médiách, 22% v tlačenej podobe
- V 93% prípadov bola krádež zistená až keď už páchatel' nepracoval u okradnutého zamestnávateľa

Čo CISO robí

- Koná reaktívne podľa novo identifikovaných zraniteľností
- Riziká komunikuje v jazyku technológií
- Pláta deravé systémy bezpečnostnými technológiami
- Dozvedá sa o nových projektoch ako jeden z posledných

Čo by mal CISO robiť

- Byť v kontakte so stratégiou a plánovaním v organizácii, aby podchytil zmeny v zárodku
- Mať prehľad o procesnom a dátovom modeli organizácie
- Pro-aktívne pracovať na stratégiách riadenia rizík pre mobilné riešenia, sociálne siete a vzťahy s tretími stranami
- Zladiť s IT štandardy pre bezpečné nasadenie a prevádzku kľúčových platforiem
- Systematizovať a konsolidovať postupy správy používateľov a prístupových práv
- Vytvoriť a udržiavať systém reakcie na incidenty
- Vytvoriť systém monitorovania rizík a prevádzkovej efektivity bezpečnosti



Ďakujem!

Presentation by

Pavol Adamec
Director, Risk & Compliance
KPMG in Slovakia
padamec@kpmg.sk
+421 2 599 84 111





cutting through complexity™

© 2011 KPMG Slovensko spol. s r.o., a Slovak limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International Cooperative (“KPMG International”).