SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Vybrané trendy informační bezpečnosti

Lukáš Mikeska

Ernst & Young

Úvod

Ernst & Young Global Information Security Survey je ve svém 15. ročníku jedním ze zajímavých zdrojů vhledu do stavu informační bezpečnosti ve světě

Posledního ročníku se 1,863 respondentů ze 64 zemí reprezentujících ty nejvýznamnější globální společnosti a obsahuje informace od mnoha respektovaných expertů na tuto oblast

Tato prezentace obsahuje výběr výsledků průzkumu, včetně jejich interpretace napříč všemi klíčovými odvětvími, ve kterých respondenti působí

Měnící se tvář informační bezpečnosti 2006-2012

Před rokem2006 byla informační bezpečnost zejména viděna jako část řízení finančních rizik a dopadů nových regulací (např. SOX 404)

Po roce 2006 musí informační bezpečnost:

- Chránit organizace v širším kontextu globalizovaného svět
- Prokazovat jasnou návratnost investic, což vyžaduje sladění řízení rizik a výkonnosti

Na pozadí globální finanční krize a změn v konkurenčním prostředí přerostla informační bezpečnost rámec pouhého řízení souladu s regulacemi.

V prostředí narůstajících hrozeb:

- Je primárním hybatelem ochrana značky a reputace
- Do ohnisku pozornosti je lepší využití technologií pro zvýšení bezpečnosti
- Organizace musí konstantně inovovat, restrukturalizovat se a přepracovávat své koncepce, aby uřídily nové požadavky a náklady

Globální ekonomika se stále zotavuje, trvají enormní tlaky na náklady a je citelný nedostatek zdrojů.

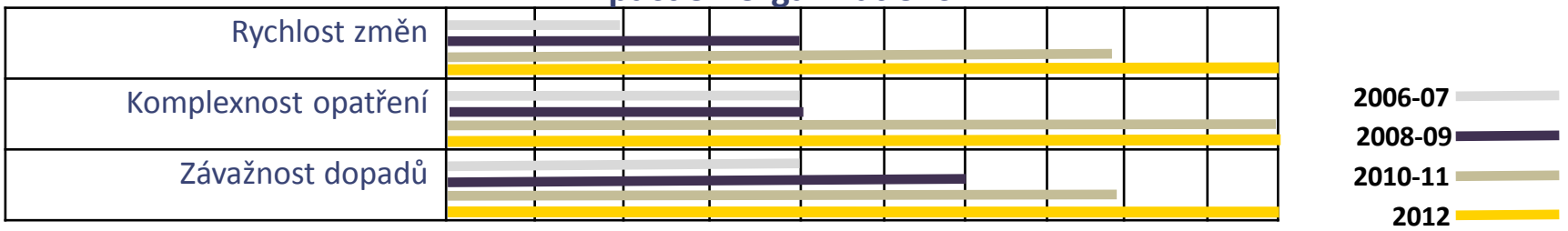
Společnosti si uvědomily, že:

- S globalizací jsou data všude
- Tradiční hranice a perimetry mizí a zaměstnanci posílají data do Internetu, nebo přenášení na mobilních zařízeních
- Zpracování dat se přesouvá do cloudu, což nutí informační bezpečnost značně přepracovat metody jejich ochrany

Rychlost a komplexita změn se zrychluje:

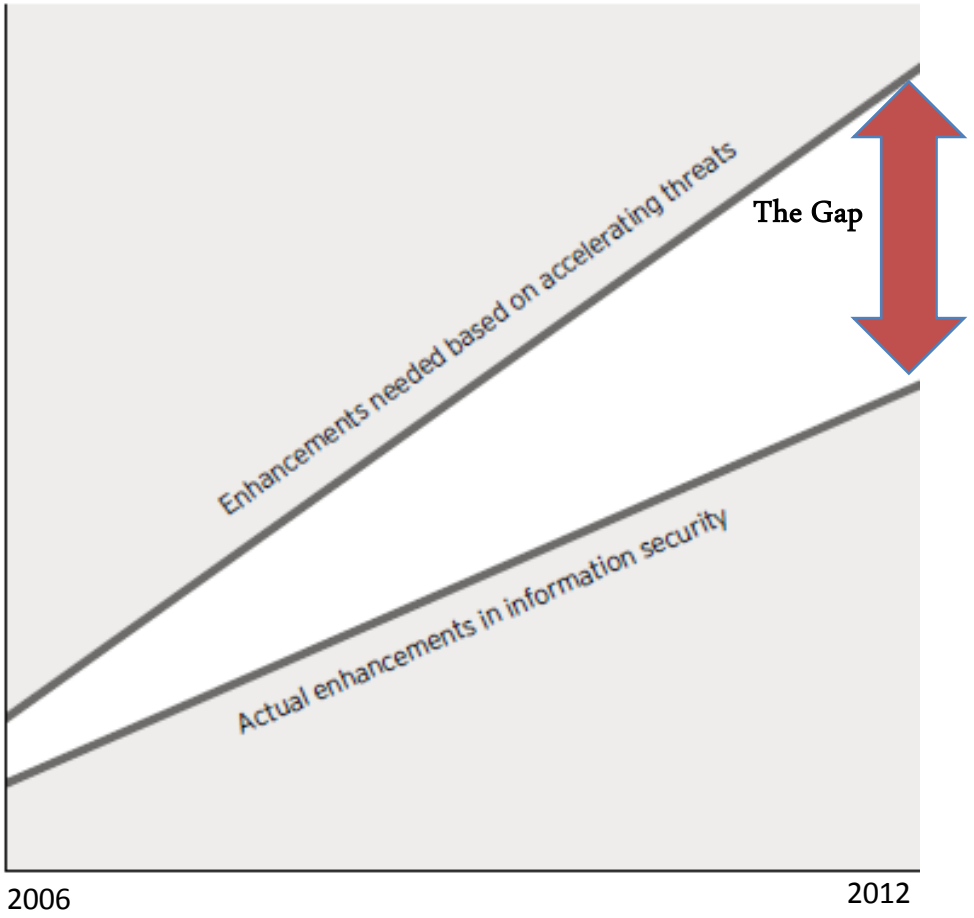
- Virtualizace, cloud, social media, „zmobilnění“ a další technologie otevírají dveře interním a externím hrozbám
- Nové trhy, ekonomická nestabilita, offshoring a zvyšující se regulatorní požadavky přidávají na komplexitě
- Organizace, které nestíhají držet krok se ocitají na kraji rostoucí bezpečnostní mezery

Impact on organizations



Boj o zmenšení mezery– přehled průzkumu

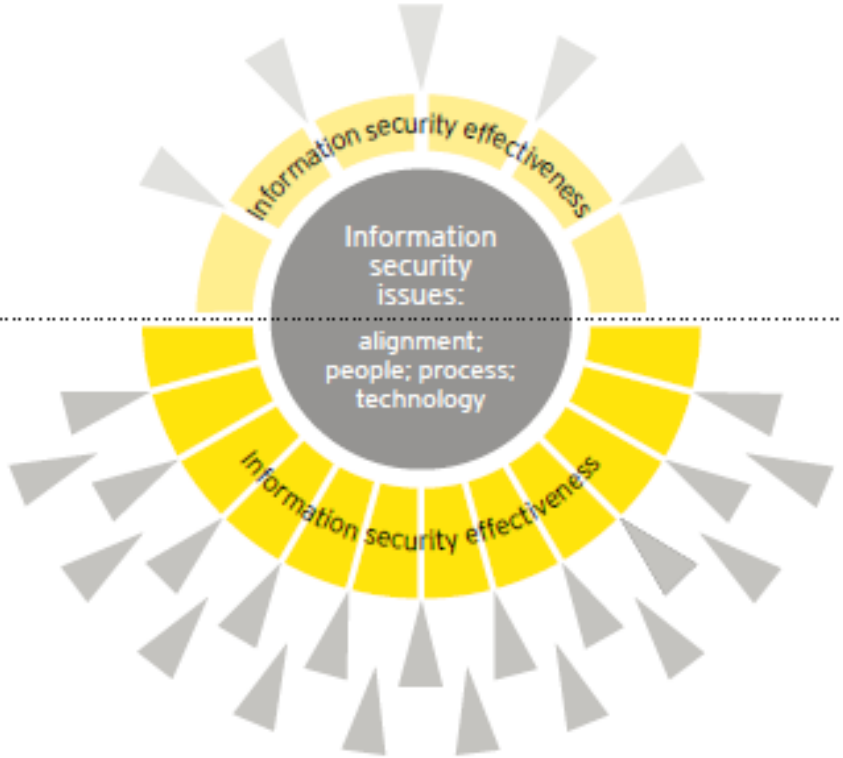
- Společnosti podnikly zásadní kroky, aby čelily bezpečnostním hrozbám a odstraňují zranitelnosti navýšením zdrojů, školeními, zlepšením IT governance a větší integrací.
- Nicméně množství a sofistikovanost hrozeb také narostla, což představuje pro informační bezpečnost značnou výzvu
- Výsledkem je zvětšující se mezera mezi tím, co je potřeba aby informační bezpečnost ve společnostech řešila a tím, na co stačí



Snaha držet krok s nárůstem rizik

Risk landscape:
2006-2011
Recognized threats impacting the organization

Risk landscape:
2012 and beyond
More, greater and new threats, impacting more quickly



- Pouze dobře promyšlený a integrovaný přístup k informační bezpečnosti, který maximalizuje přínosy správně cílených investic pomůže společnostem přinést ujištění, že dostatečně chrání svá data a životně důležité informace

Hlavní vybraná zjištění

- **Informační bezpečnost nenaplňuje očekávání**
  Jen 16% si myslí, že zcela pokrývá jejich potřeby
  70% je toho názoru, že pokrývá potřeby pouze částečně
- **Incidenty a hrozby na vzestupu**
  31% vidí nárůst bezpečnostních incidentů a jen 10% zaznamenalo pokles; V roce 2009, 41% vidělo nárůst externích útoků. V roce 2012, jejich podíl vzrostl na 77%
- **Rekce na rizika spojená s cloudem je pomalá**
  V roce 2010 jen 30% indikovalo (plán) využít cloudových služeb. V roce 2012 je toto číslo dvojnásobné. Avšak 38% uvádí, že neučinili žádné kroky směrem k řízení rizik s cloudem spojených s cloudem
- **Finanční výzvy**
  62% uvádí, že rozpočtová omezení jsou hlavní brzdou efektivního řízení informační bezpečnosti
- **Governance má vliv na vše**
  Okolo třetiny respondentů ladí strategii informační bezpečnosti s rizikovým apetitem organizace a s mírou tolerance rizika. Téměř dvě třetiny nemají definovaný formální rámce bezpečnostní architektury

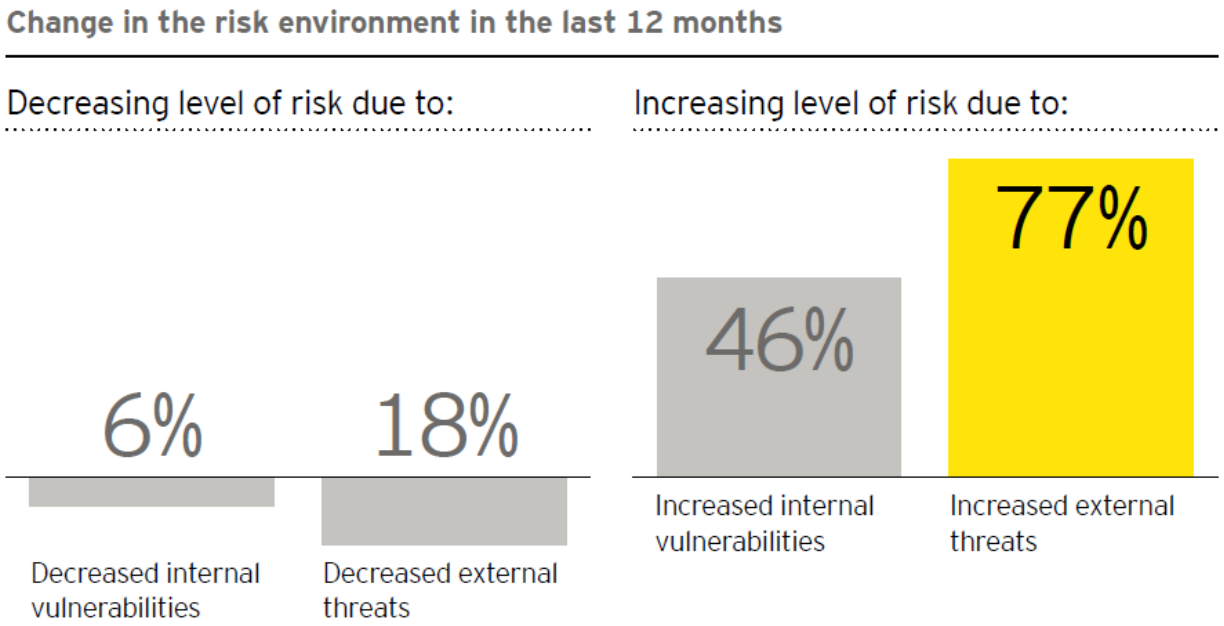
70%

of respondents indicate that their information security function only partially meets organizational needs and improvements are underway

Hrozby a incidenty narůstají

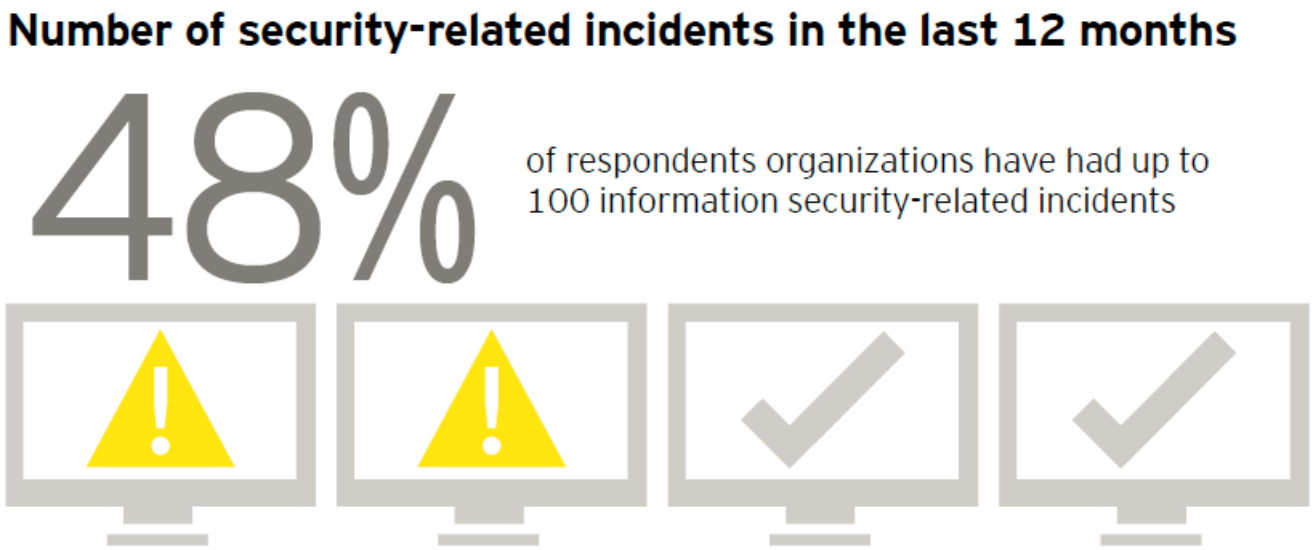
V roce 2009 41% respondentů pozorovalo nárůst externích útoků. Jejich poměř vyšplhal na 72% v roce 2011 a na77% v roce 2012.

Organizace pozorují nárůst interních zranitelností. V roce 2012 téměř polovina respondentů (46%) potvrzuje nárůst za posledních 12 měsíců.



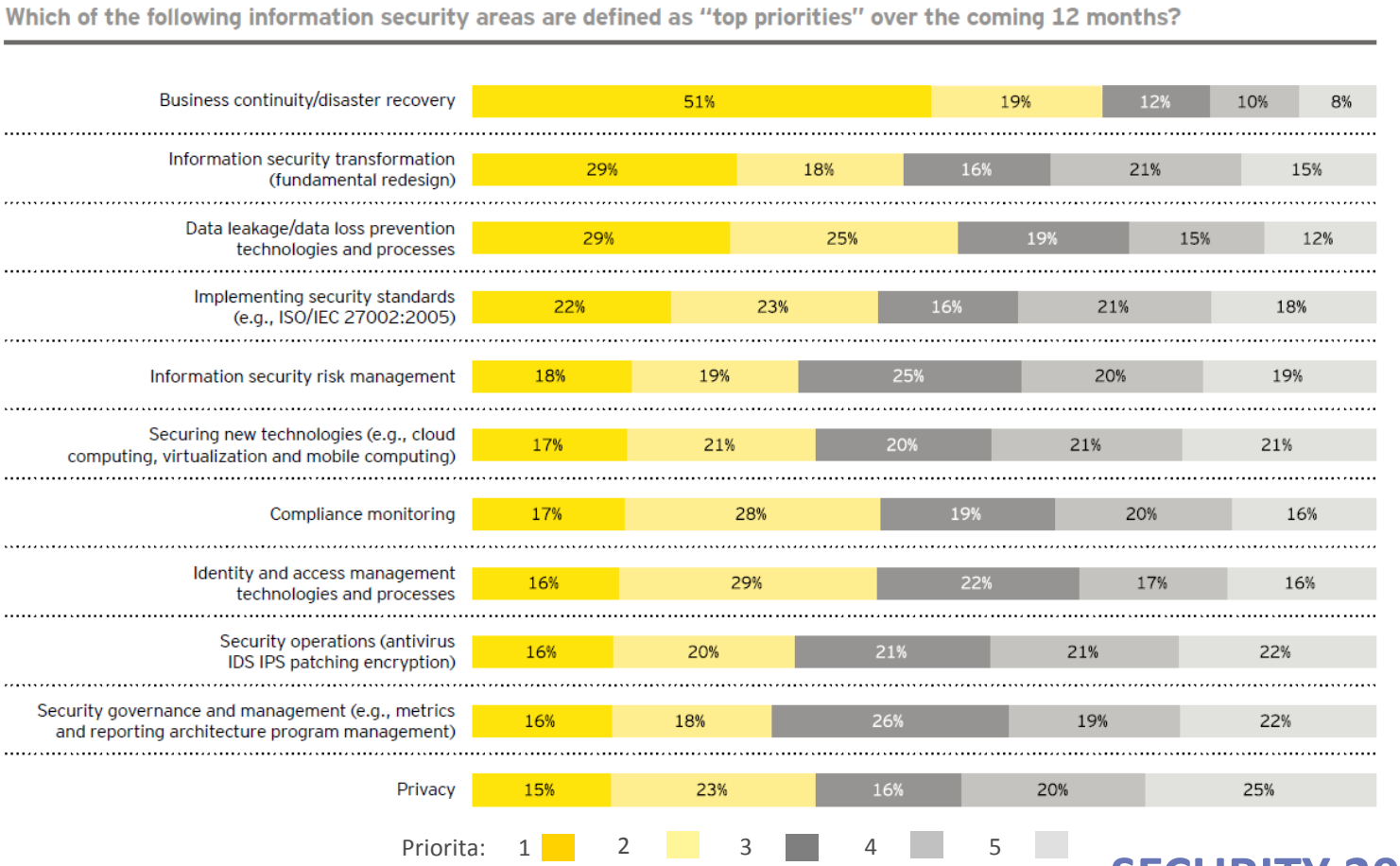
Hrozby jsou častější a sofistikovanější

S nárůstem množství a „chytrosti“ útoků roste také počet bezpečnostních incidentů. Téměř polovina respondentů uvedla, že zaznamenali v předchozím roce nejméně 100 incidentů.



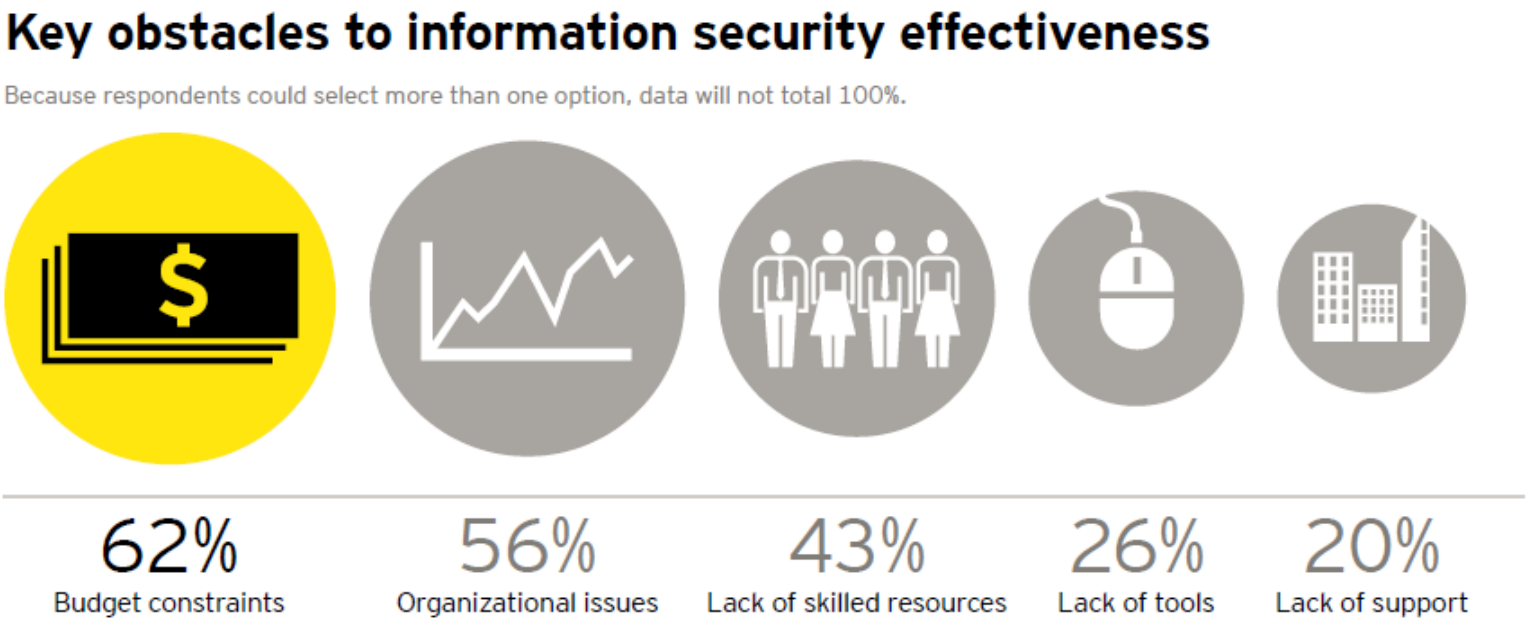
Priority odrážejí některé současné bezpečnostní potřeby

Business continuity, risk management a **zásadní transformace informační bezpečnosti** jsou na žebříčku priorit informační bezpečnosti na předních místech



„Staří známí“

Problémy jako rozpočtová omezení, organizační záležitosti a nedostatek správných zdrojů stále brání organizacím zmenšovat zmíněnou bezpečnostní mezeru



Problémy sladění

Narůstající bezpečnostní mezera je dále rozšiřována problémy se sladěním strategií, kdy si informační bezpečnost konkuruje s jinými prioritami managementu

- **Je potřeba širší sladění:** Informační bezpečnost zůstává oblastí taženou převážně z IT, než aby se stávala širší součástí obchodní strategie.
- **Zodpovědnost za Governance a monitoring:** Jen 38% má sladěnu strategii informační bezpečnosti s rizikovým apetitem organizace a s mírou tolerance rizik; Jen u 5% je zodpovědnost za informační bezpečnost svěřena do kompetence CRO (chief risk officer)
- **Neexistence širšího strategického rámce:** Téměř dvěma třetinám organizací chybí formální rámce bezpečnostní architektury, a ani se jej nechystají vytvořit

56%

of respondents say their information security strategy is aligned to their IT strategy

42%

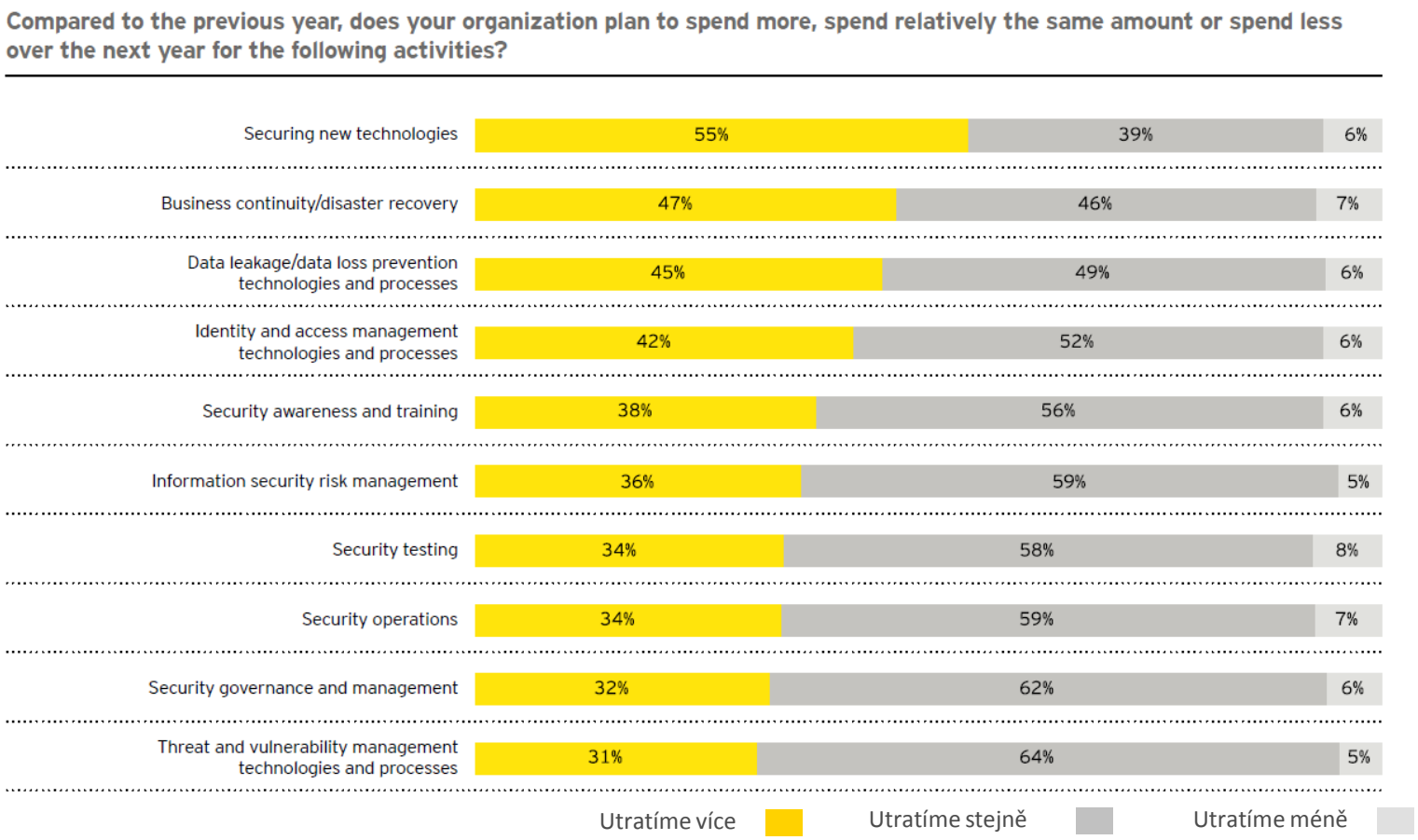
of respondents say that their information security strategy is aligned to their business strategy

38%

of respondents say their information security strategy is aligned to the organization's risk appetite

Investice narůstají, ale ne vždy v kritických oblastech

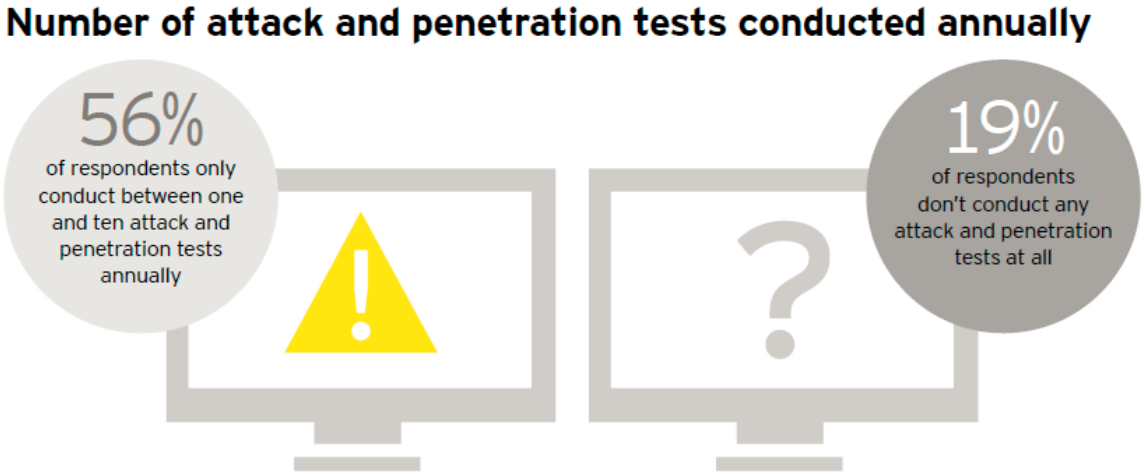
Financování v důležitých oblastech stále nedrží krok s výzvami, včetně řízení hrozeb a zranitelností a bezpečnostního testování



Zranitelnosti na vzestupu

Směsice neintegrovaných, komplexních a často nestabilních obranných mechanismů vytváří výrazné bezpečnostní díry. Organizace mají vzrůstající tendenci používat přechodná a náhradní řešení. Prostředí a procesy jsou pak nekonzistentní, obtížně testovatelné a složité na provoz, údržbu, aktualizaci a monitoring.

Téměř třetina respondentů uvádí, že množství hrozeb a zranitelností v jejich bezpečnostní architektuře v posledním roce vzrostlo, zejména kvůli zastaralým kontrolním mechanismům



Chybějící strategie informační bezpečnosti

Mnoho organizací uznává důležitost informační bezpečnosti a věnuje zdroje na zlepšení v této oblasti. Stále je ale dost také těch organizací, které v tomto směru nevyvíjejí žádné úsilí.

Výrazná část respondentů nemá vypracovánu strategii informační bezpečnosti, program sledování hrozeb a žádnou míru ujištění o způsobu řízení informační bezpečnosti u svých dodavatelů

Information security strategies

13%	of respondents do not have an information security strategy
37%	of respondents have no threat intelligence program in place
17%	of respondents do not ensure that external partner, vendors or contracts are protecting their organization's information
4%	of respondents do not assess the efficiency or effectiveness of their information security program

Využití cloudu – dychtivost i nejistota

Zpracování a ukládání dat v cloudových řešeních se rychle stává preferovaným řešením pro podporu iniciativ jako je inovace dodavatelských řetězců, aktivnější zapojení zákazníků nebo zvýšení zaměstnaneckých inovací. Pohotové, rychlé a levné – většina organizací si uvědomuje, že se musí adaptovat, nebo ustoupit konkurenci

38%

of respondents say they have not take any measures to mitigate the risks of using cloud computing services

V roce 2010, jen 30% of organizací uvádělo, že (plánují) využít cloudových služeb. Tento podíl vzrostl na 44% v roce 2011 a další rok na 59% - téměř dvojnásobek.

Ale mnoho jich přiznává: úsilí vypořádat se s riziky cloudu je minimální, nebo žádné.

30%

of respondents say they are currently using or planned to use cloud computing services

44%

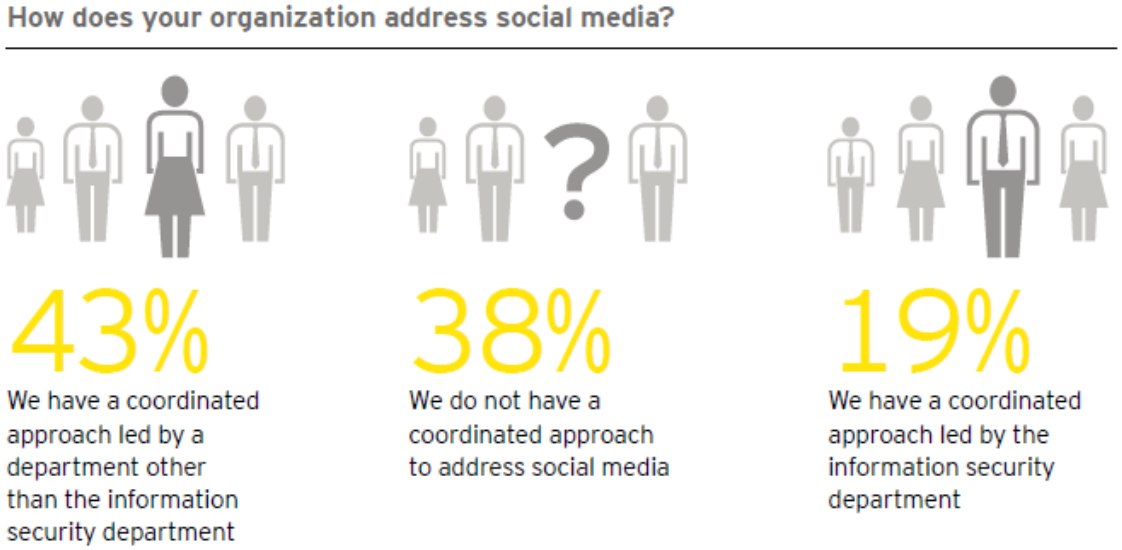
of respondents say they are currently using or planned to use cloud computing services

59%

of respondents say they are currently using or planned to use cloud computing services

Sociální média: šancí i rizik co hrdlo ráčí

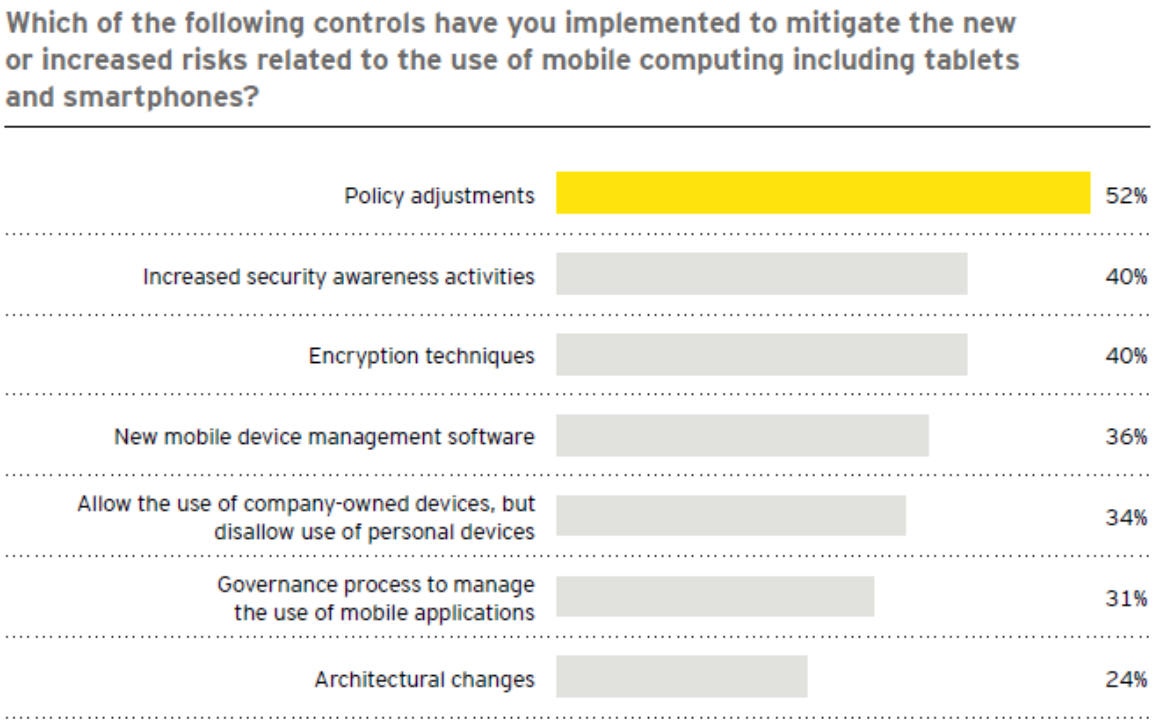
Všudypřítomná a nevyhnutelná, sociální média mění drasticky způsoby podnikání mnoha organizací. Ale 38% organizací nemá koordinovaný přístup k využívání sociálních médií, což vede k promarnění mnoha šancí, či
potenciálním bezpečnostním incidentům, které mohou zničit značku/dobré jméno takřka přes noc. Nejčastější taktikou respondentů je jednoduše omezit přístup na stránky sociálních médií – což je pravděpodobně neefektivní, když většina zaměstnanců má k dispozici vlastní zařízení a má přístup ke korporátním sítím téměř kdykoliv a odkudkoliv.



Mobily + tablety = rizika v pohybu

Analytici předpokládají, že v roce 2016 bude na světě10 mld. mobilních zařízení s přístupem na internet – více než jedno zařízení na každého obyvatele planety.

Množství tabletů využívané pro podnikání se během roku 2012 zdvojnásobilo. 44% organizací umožňuje používat firemní, či soukromý tablet.



Otázky do publika

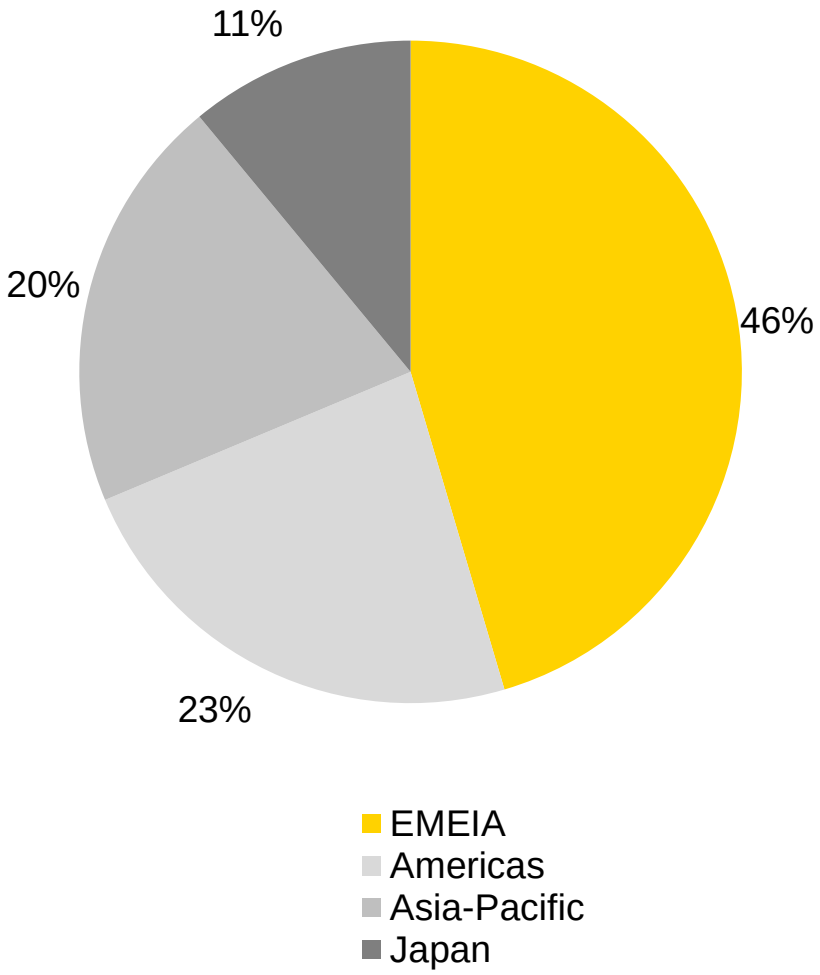
- Myslíte si, že bezpečnostní mezera (rozdíl mezi tím, co děláte a tím, co byste měli dělat) se zvětšuje nebo zmenšuje?
- Jak víte, že jsou vaše limitované zdroje zaměřené na oblasti a iniciativy kritické pro úspěšné řízení informační bezpečnosti?
- Jaká zlepšení jste provedli v oblasti procesů a funkcí v informační bezpečnosti; a jaká zlepšení jsou stále potřeba?
- Charakterizovali byste tyto změny jako evoluční, nebo revoluční? Do jaké míry vás tyto změny do budoucna připravily na řízení nových rizik?
- Jste v oblasti informační bezpečnosti více nebo méně sebejistí ve srovnání s dobou před jedním rokem? A ve srovnání se dvěma, třemi lety nazpátek?

Příloha: O průzkumu

Ernst & Young's 2012 Global Information Security Survey

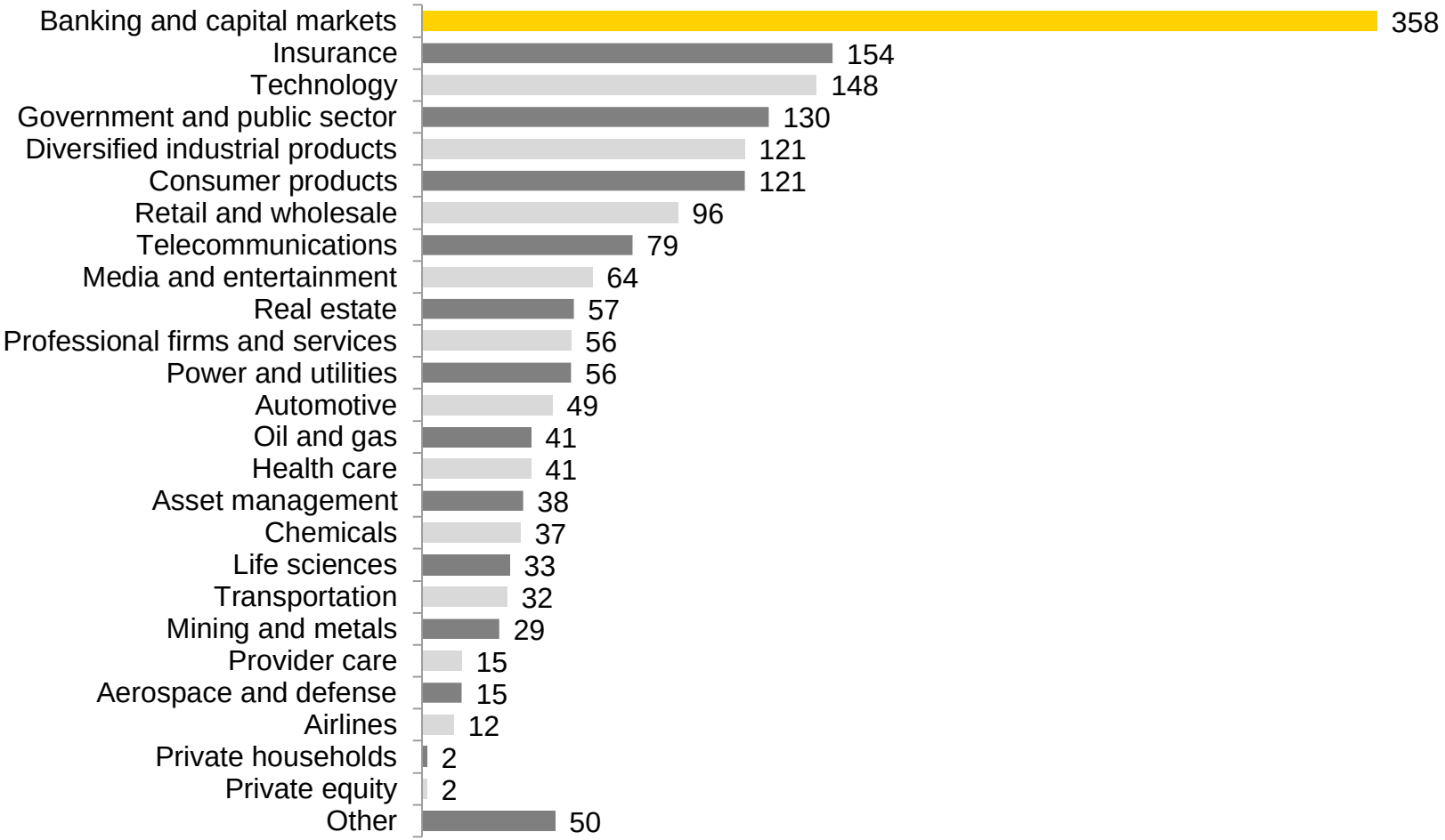
Survey participants by geography

1,863 respondents
from 64 countries



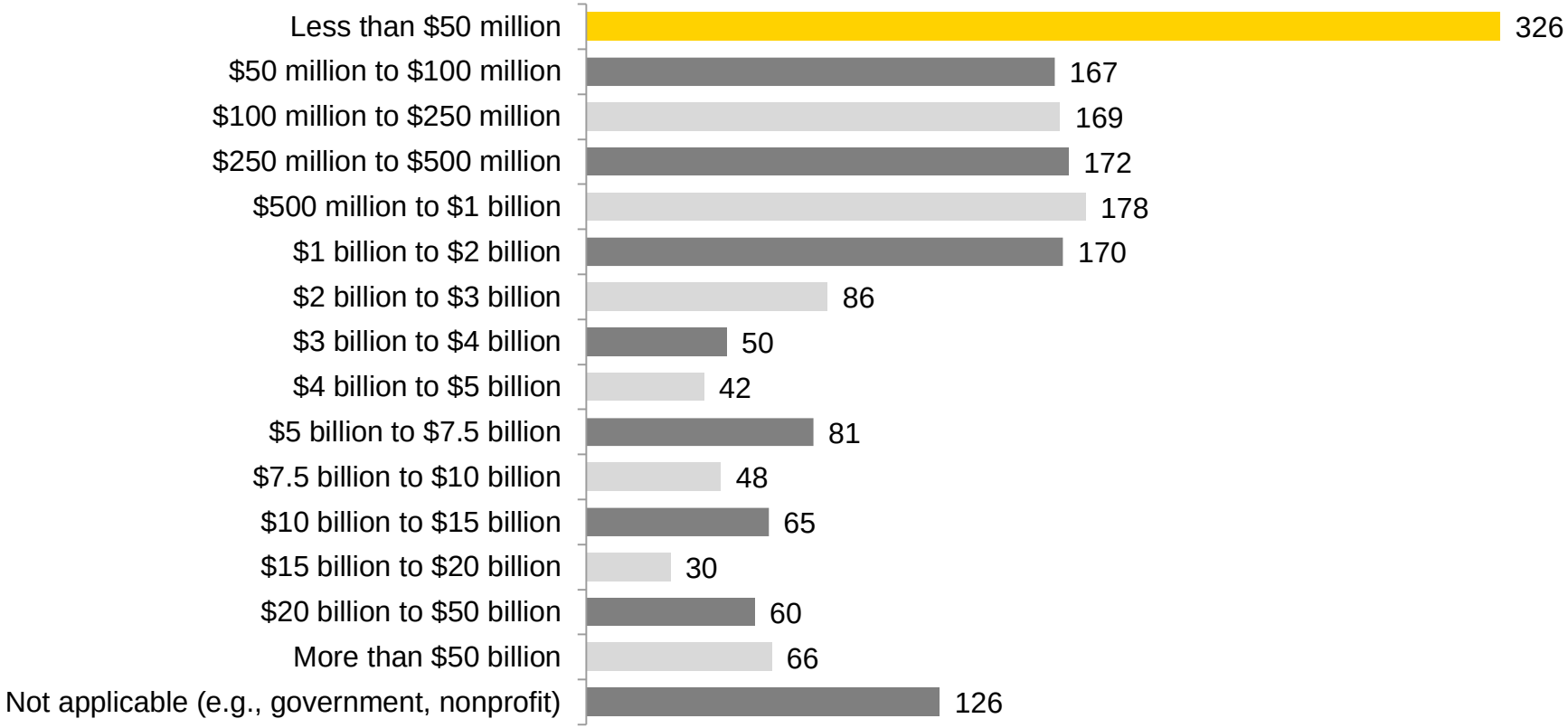
Ernst & Young's 2012 Global Information Security Survey

Survey participants by industry sector



Ernst & Young's 2012 Global Information Security Survey

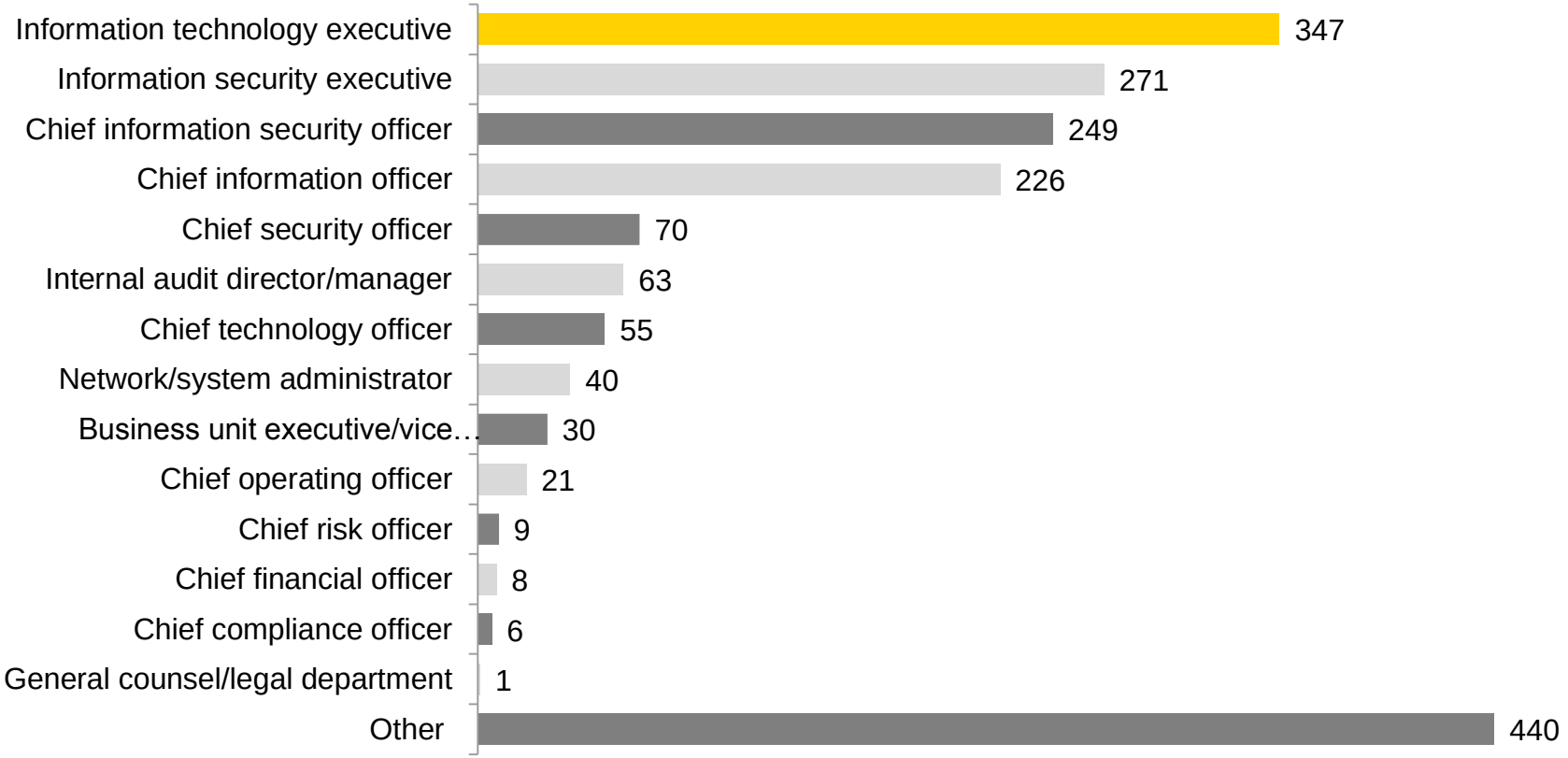
Survey participants by total annual company revenue



$ = US dollars

Ernst & Young's 2012 Global Information Security Survey

Survey participants by position



SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

Lukáš Mikeska
Ernst & Young
lukas.mikeska@cz.ey.com