

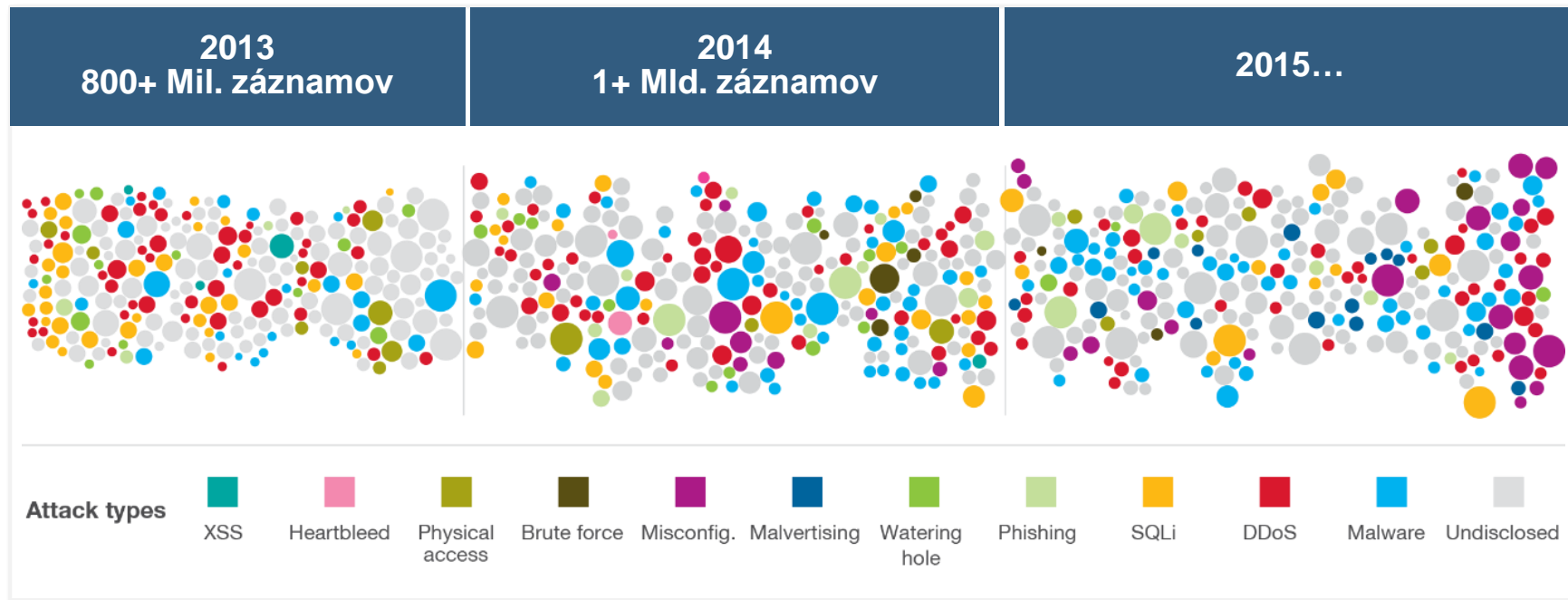
# Trendy v informačnej bezpečnosti - ochrana údajov: ako EÚ ovplyvní konanie firiem?

JARNÁ ITAPA 2017



Ivan Makatura

# Nárast počtu, objemu a komplexnosti útokov je nespochybniteľný...



Priemerná doba detekcie pokročilého útoku

**201 dní**

Medziročný nárast počtu incidentov

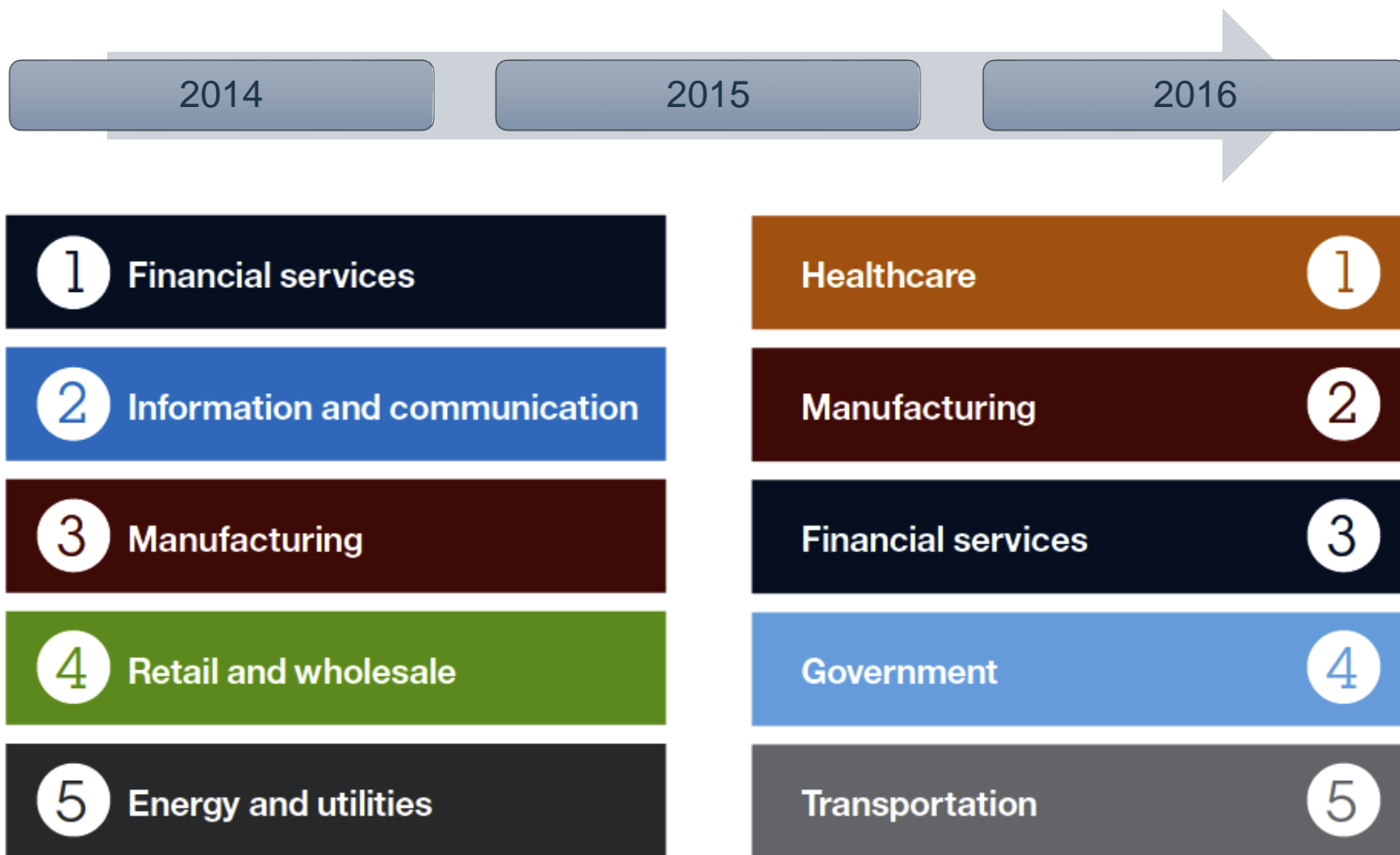
**23%**

Priemerné náklady incidentu v USA

**3,79 Mil. USD**

Zdroj: IBM X-Force Threat Intelligence Report - 2016

# Distribúcia bezpečnostného rizika podľa odvetví



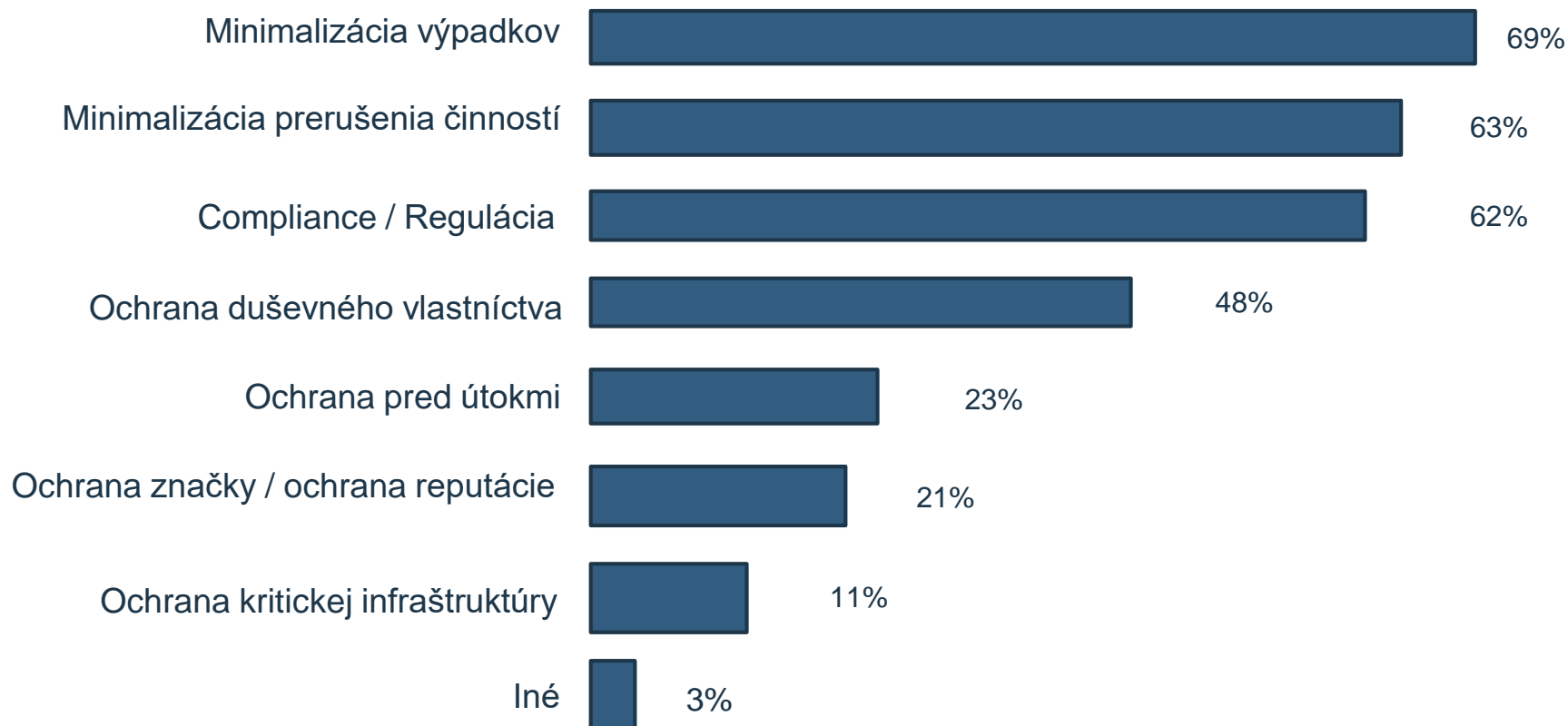
Zdroj: IBM X-Force Threat Intelligence Report - 2016



**Je regulácia potrebná?**

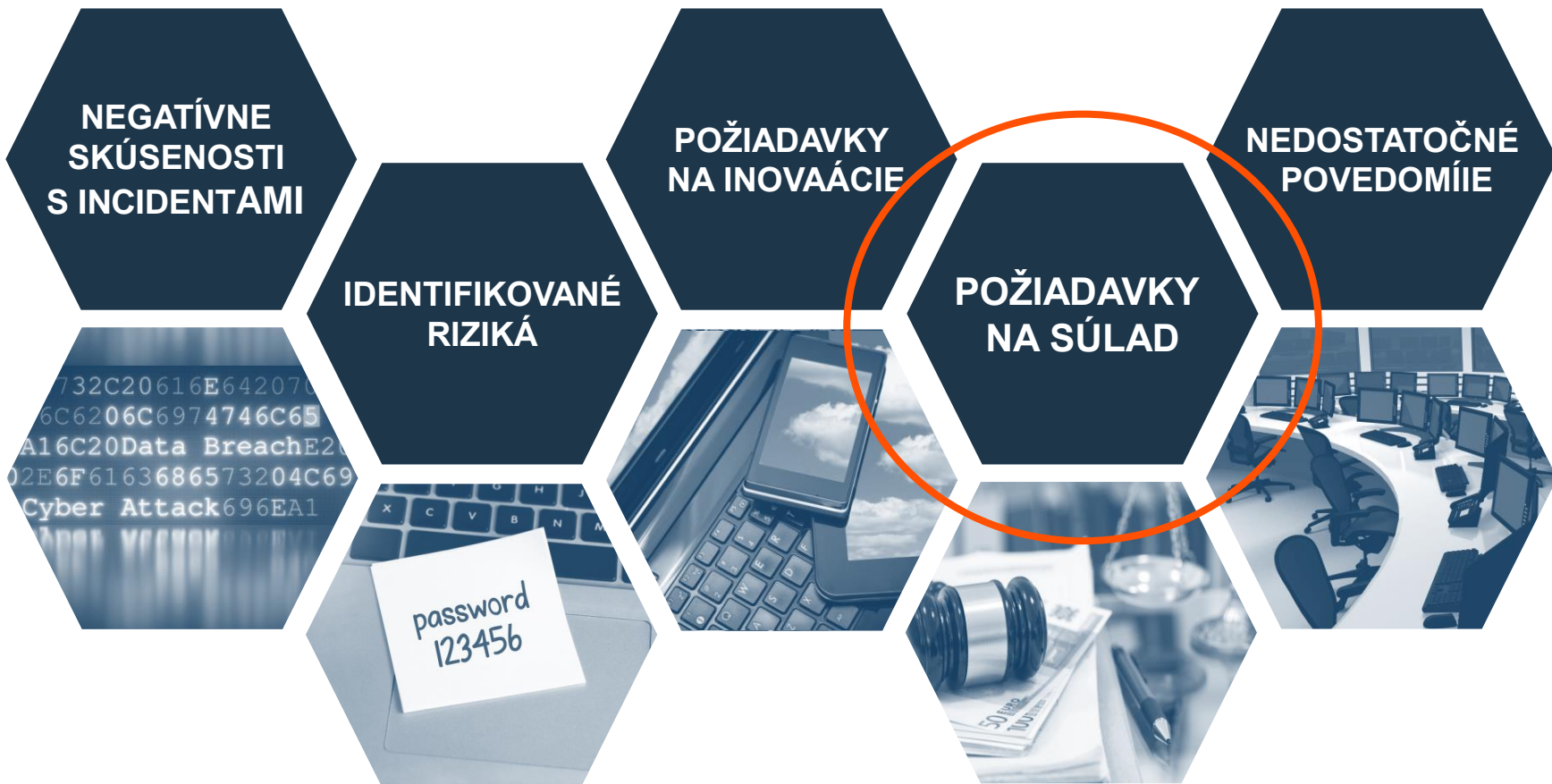


# Typické objektívne dôvody pre riadenie bezpečnostného rizika...

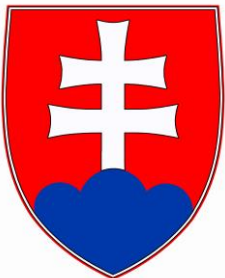


Zdroj: Ponemon's 2016 Application Security Risk Study

# Čo reálne poháňa bezpečnosť? (typické subjektívne dôvody)



# Požiadavky na ochranu informačných aktív v slovenskej legislatíve



- Zákon č. 122/2013 Z. z. o ochrane osobných údajov
- Zákon č. 483/2001 Z. z. o bankách
- Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu
- Zákon č. 351/2011 Z.z. o elektronických komunikáciách
- Zákon č. 215/2004 Z. z. o o ochrane utajovaných skutočností
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
- Zákon č. 300/2005 Z. z. trestný zákon
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
- Zákon č. 319/2002 Z. z. o obrane SR
- Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy  
... v znení neskorších predpisov...



- 
- Návrh zákona o kybernetickej bezpečnosti
  - Návrh zákona o výkone správy v oblasti informačných technológií verejnej správy (ITVS)
  - Pripravovaný zákon o ochrane osobných údajov

# Požiadavky na ochranu informačných aktív v európskej legislatíve



- Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zaistenie vysokej spoločnej úrovne bezpečnosti sietí a informácií v Únii

(The Network and Information Security Directive , ďalej len „**NIS**“)

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov

(The General Data Protection Regulation, ďalej len „**GDPR**“)

- Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu Únii

(Payment Services Directive 2, ďalej len „**PSD2**“)

- Nariadenie Európskeho parlamentu a Rady (EÚ) 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

(Regulation on Electronic identification and trust services for electronic transactions  
ďalej len „**eIDAS**“)



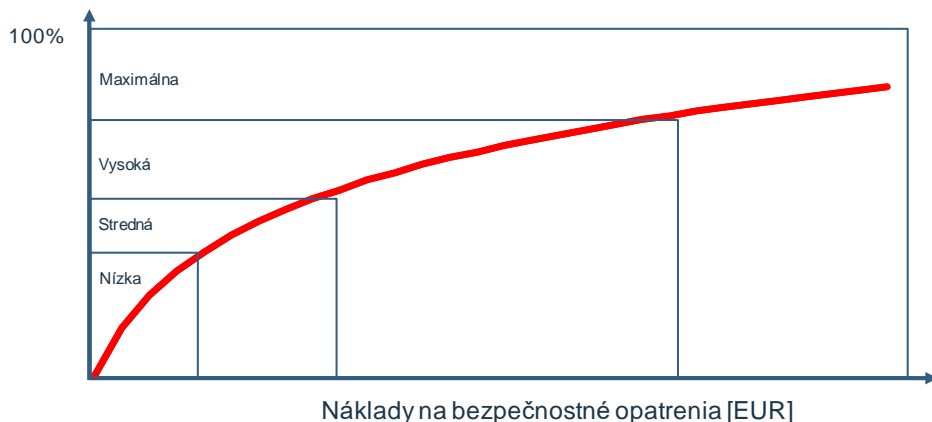


# Náklady vyvolané reguláciou



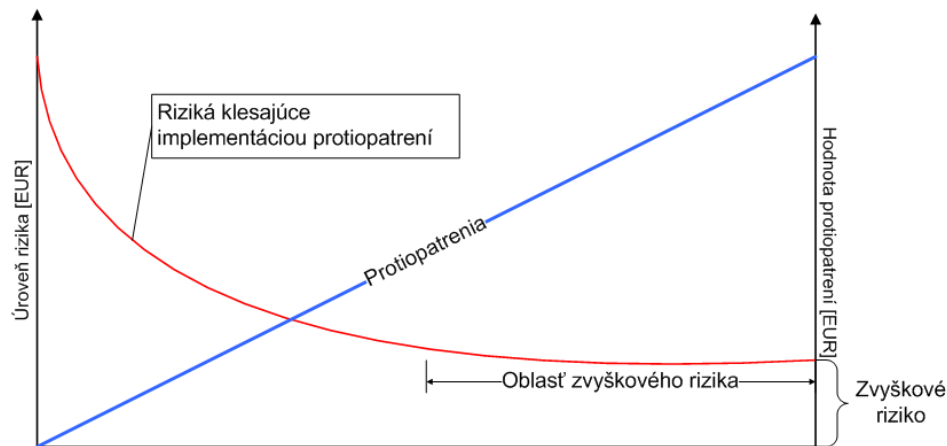
# Náklady vs. efektivita v informačnej bezpečnosti

Úroveň ochrany [%]



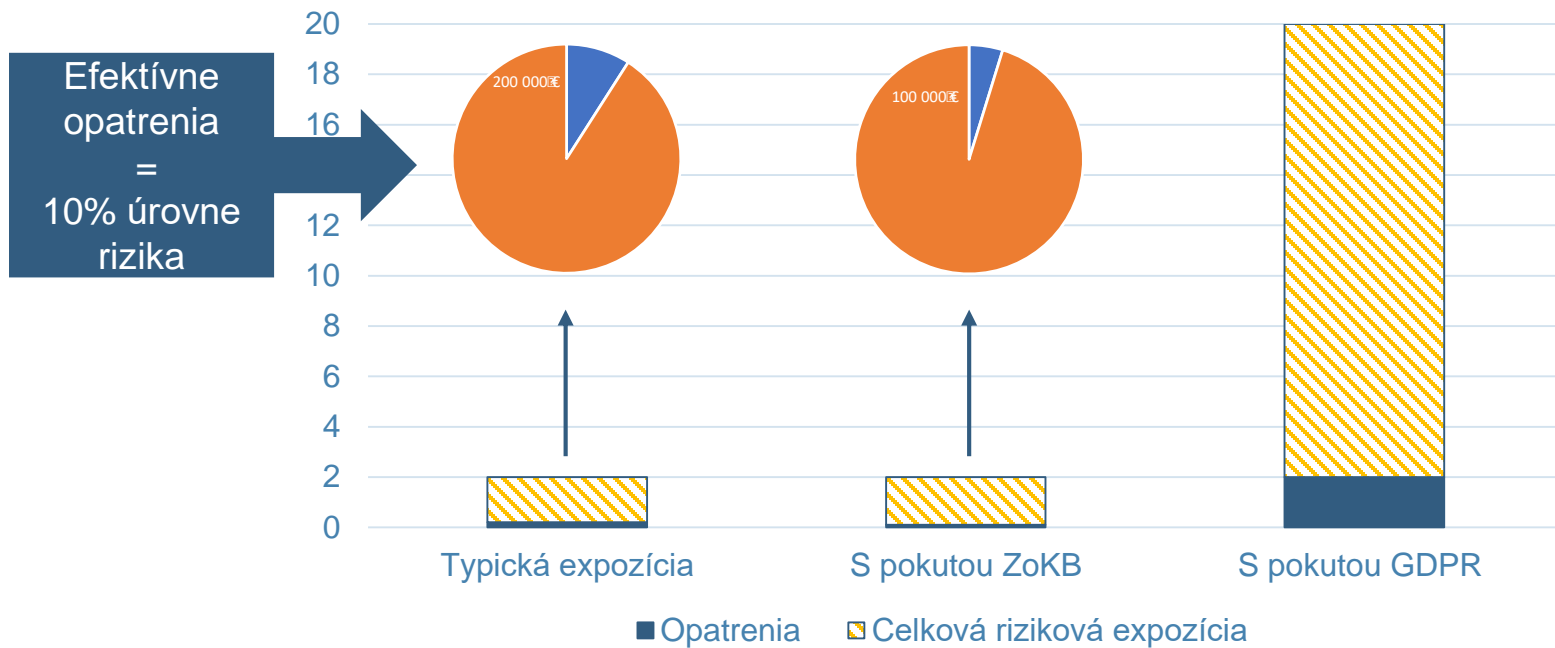
- Absolútna úroveň ochrany nie je dosiahnuteľná ani za predpokladu neobmedzených nákladov
- Je úlohou vlastníka rizík rozhodnúť o efektívite opatrení
- Cieľom regulácie je dosiahnuť žiadúce správanie zúčastnených subjektov

- Nulové riziko nie je dosiahnuteľné ani za predpokladu neobmedzených nákladov
- GDPR vyžaduje tzv. predbežnú konzultáciu zvyškových rizík (aká bude kompetencia ÚOOÚ v riadení rizík?)
- Štát nie je vlastníkom rizík, mal by teda v regulácii dodržiavať doktrínu „laissez-faire“ („nechajte nás konať“)



Zdroj: BSI Standard 100-2 IT-Grundschutz Methodology, v.1.0. Bundesamt für Sicherheit in der Informationstechnik

# Nadmerné pokuty neprispievajú ku ošetroreniu rizík, ale predstavujú nové riziko...

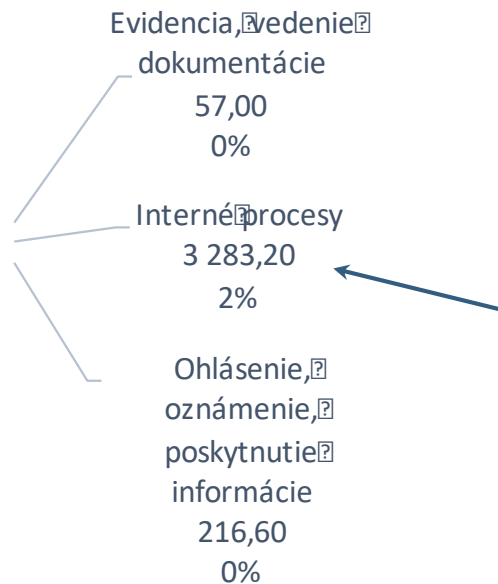


- GDPR namiesto zníženia rizík vytvára úplne nové hrozby, ktoré niekoľkonásobne prekročia hodnotu pôvodných identifikovaných rizík
- To môže spôsobiť zníženie prahu vnímania potreby ochrany údajov

# Odhadované finančné dopady Zákona o kybernetickej bezpečnosti

TCO = 1 rok

Počet dotknutých subjektov = cca 160



- Riadenie bezpečnostných rizík
- Bezpečnosť systémov a zariadení
- Riadenie prevádzky IT
- Riadenie kybernetických bezpečnostných incidentov
- Riadenie dostupnosti siete a informačného systému
- Monitorovanie, testovanie bezpečnosti a bezpečnostné audity













- Kalkulačka nákladov Ministerstva hospodárstva SR
- agregovaná kalkulácia nákladov všetkých povinností, ktoré vyplývajú podnikateľom z predkladaného materiálu (založená na metodike „Activity Based Costing“)



















**Ako môže regulácia pomôcť?**















# Požiadavky akademickej sféry na právnu úpravu IB

Požiadavka	ZoKB	GDPR
Regulácie nesmú byť v rozpore s teoretickými princípmi informačnej bezpečnosti		
Regulácie majú zlepšiť stav vzdelávania v informačnej bezpečnosti		
V rámci SR sa zvýši odborná spôsobilosť všetkých subjektov v interakcii s IKT		
Zavedené certifikačné schémy poslúžia ako metrika kvalifikácie		
Regulácie majú zabezpečiť implementáciu informačnej bezpečnosti prostredníctvom sústavy kvalifikácií		
Zákon má tlačiť na stratégiu v technickej normalizácii v oblasti IB		

# Požiadavky komerčných subjektov na právnu úpravu IB

Proces / Požiadavka	ZoKB	GDPR
<b>Riadenie rizík</b>		
<ul style="list-style-type: none"> <li>V SR vznikne ustálená a unifikovaná schopnosť riadenia bezpečnostných rizík</li> </ul>		
<ul style="list-style-type: none"> <li>Manažment rizík sa stane základným a hlavným východiskom pre meranie efektivity protipatrení</li> </ul>		
<ul style="list-style-type: none"> <li>Požiadavky na proces nesmú byť formálne (papierová bezpečnosť neznižuje úroveň rizík)</li> </ul>		
<ul style="list-style-type: none"> <li>Penalizácie budú primerané</li> </ul>		
<b>Bezpečnostná architektúra</b>		
<ul style="list-style-type: none"> <li>Kritické systémy a siete budú bezpečné a odolné proti všetkým známym narušeniam, náhodným alebo úmyselným</li> </ul>		
<b>Overovanie súladu</b>		
<ul style="list-style-type: none"> <li>Požiadavky regulácie musia byť auditovateľné</li> </ul>		
<ul style="list-style-type: none"> <li>Musí byť stanovená metrika pre auditing</li> </ul>		
<ul style="list-style-type: none"> <li>Musia byť stanovené minimálne kvalifikačné požiadavky pre auditorov</li> </ul>		

# Požiadavky komerčných subjektov na právnu úpravu IB

Proces / Požiadavka	ZoKB	GDPR
<b>Pravidlá reakcie na bezpečnostné incidenty</b>		
<ul style="list-style-type: none"><li>Pravidlá procesu reakcie na incidenty musia byť prehľadne definované</li></ul>		
<ul style="list-style-type: none"><li>Zákon musí prinášať výhody vo forme zlepšenia procesu:</li></ul>		
<ul style="list-style-type: none"><li>- systém včasnej reakcie</li></ul>		
<ul style="list-style-type: none"><li>- koordinácia reakcie (musí byť efektívna a zmysluplná, nie formálna)</li></ul>		
<b>Notifikácia incidentov</b>		
<ul style="list-style-type: none"><li>Má byť povinná až od určitej relevantnej hodnoty (threshold)</li></ul>		
<ul style="list-style-type: none"><li>Musí byť vhodne štatisticky spracovaná a použitá pre budúce zlepšenie stavu IB</li></ul>		
<ul style="list-style-type: none"><li>Obnoviť princíp „Single Point of Contact“</li></ul>		





# ĎAKUJEM

SLEDUJTE NÁS NA:



[ibm.com/security](https://ibm.com/security)



[securityintelligence.com](https://securityintelligence.com)



[xforce.ibmcloud.com](https://xforce.ibmcloud.com)



[@ibmsecurity](https://twitter.com/ibmsecurity)



[youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)



[ivan.makatura@sk.ibm.com](mailto:ivan.makatura@sk.ibm.com)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.