



Ako rozoznať kvalitu od nekvality, alebo - roztrhlo sa vrece s „odborníkmi“...

EFOCUS



Ivan Makatura

IBM Slovensko, s.r.o.





**Čo je to informačná bezpečnosť?
A je vôbec potrebná...?**





Hokej

Futbal

Ekonomia

Politika

Bezpečnosť

Ochrana údajov

- Čo majú tieto činnosti na Slovensku spoločné?
 - Každý im rozumie... (Alebo si to prinajmenšom o sebe myslí...)

Typické subjektívne dôvody pre vykonávanie procesu „informačná bezpečnosť“



Zdroj: Ponemon's 2016 Application Security Risk Study

Incident vs. porušenie ochrany osobných údajov

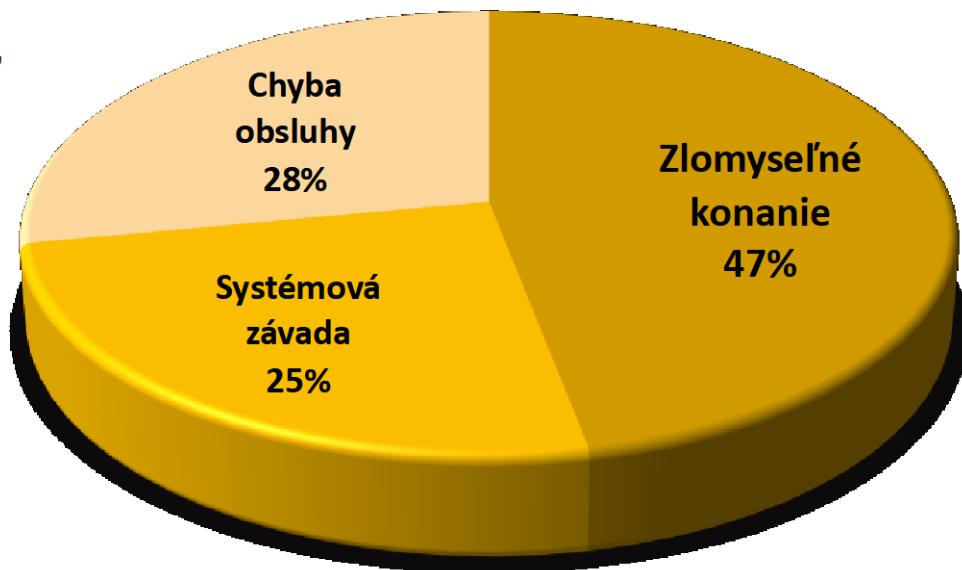
- **GDPR Čl. 4 (12):**

- „porušenie ochrany osobných údajov“ je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim;

- **WP29 Guidelines on Personal data breach notification:**

- „What should be clear is that a breach is a type of security incident“
- “Whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches”

Príčiny porušenia ochrany údajov v roku 2017:



Zdroj: Ponemon's 2017 2017 Cost of Data Breach Study

Ochrana informačných aktív v legislatíve



- Zákon č. 351/2011 Z.z. **o elektronických komunikáciách**
- Zákon č. 215/2004 Z. z. **o ochrane utajovaných skutočností**
- Zákon č. 185/2015 Z. z. **autorský zákon**
- Zákon č. 45/2011 Z. z. **o kritickej infraštruktúre**
- Zákon č. 300/2005 Z. z. **trestný zákon**
- Zákon č. 40/1964 Z. z. **občiansky zákonník**
- Zákon č. 275/2006 Z. z. **o informačných systémoch verejnej správy**
- Zákon č. 319/2002 Z. z. **o obrane SR**
- Zákon č. 492/2009 Z. z. **o platobných službách (& PSD2)**
- Zákon č. 272/2016 Z. z. **o dôveryhodných službách pre elektronické transakcie (& eIDAS)**

Požiadavky na riadenie rizík:

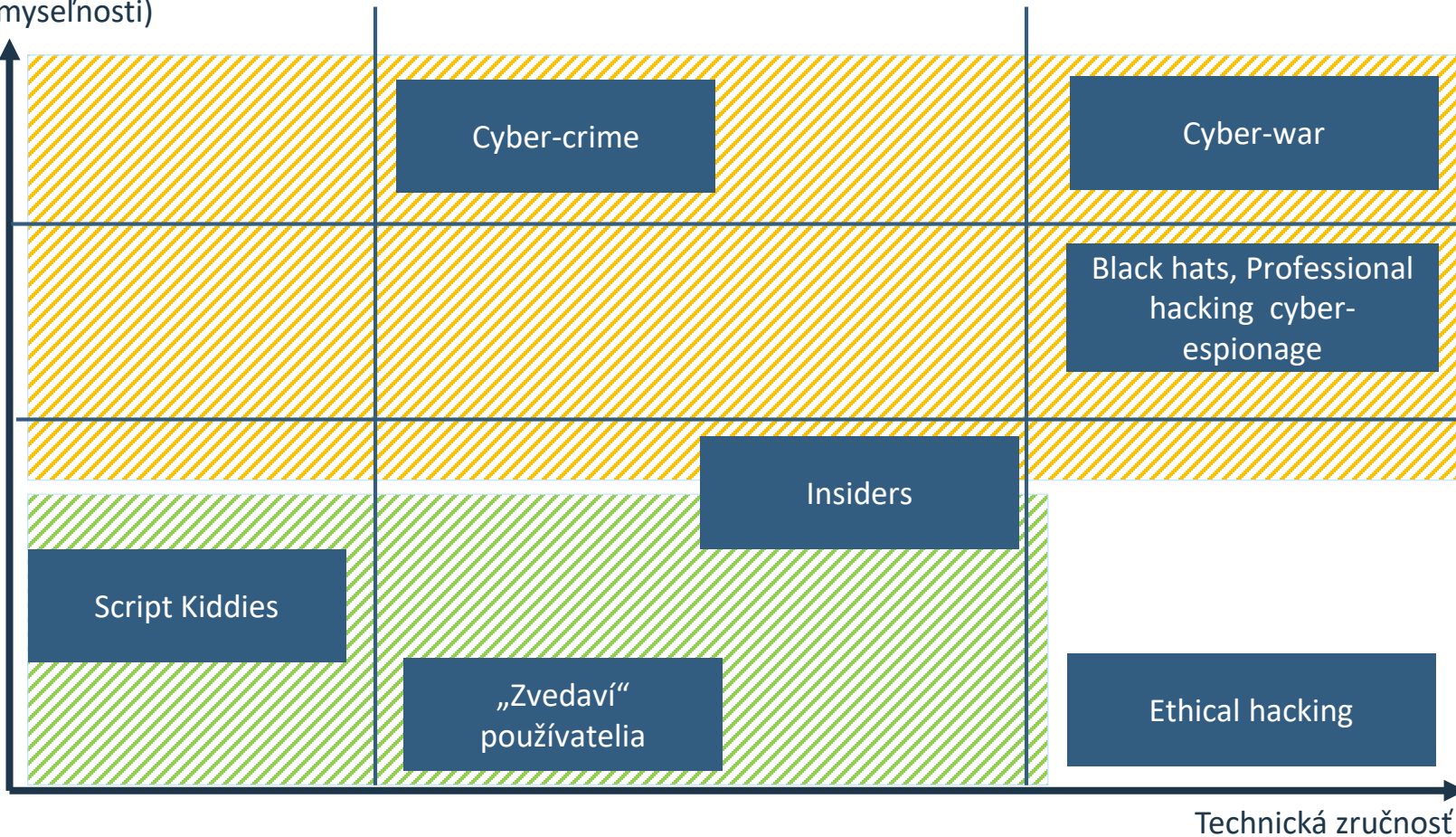
- Zákon č. 483/2001 Z. z. **o bankách**
- Zákon č. 69/2018 Z. z. **o kybernetickej bezpečnosti (& NIS)**
- Zákon č. 18/2018 Z.z. **o ochrane osobných údajov (& GDPR)**



Nezávisle od odvetvia

Profily útočníkov v kybernetickom priestore

Kriminálny potenciál
(miera zlomyseľnosti)





Máme nástroje, niet remeselníkov...



Rozpor medzi agilitou bezpečnosti a rozsahom hrozieb

Nová realita bezpečnosti:



Vyvážený pomer medzi rizikami a protiopatreniami



Efektivita nákladov prostredníctvom riadenia rizík

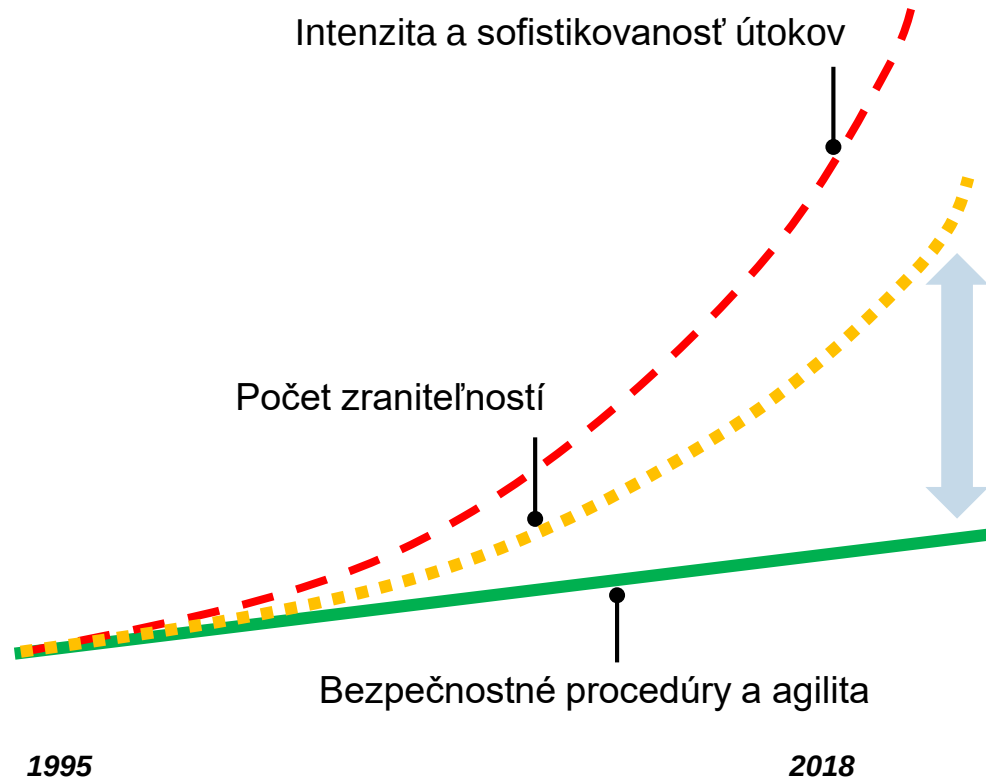


Automatizácia bezpečnostných procesov



Zručnosti podporené kognitívnou výpočtovou analytikou

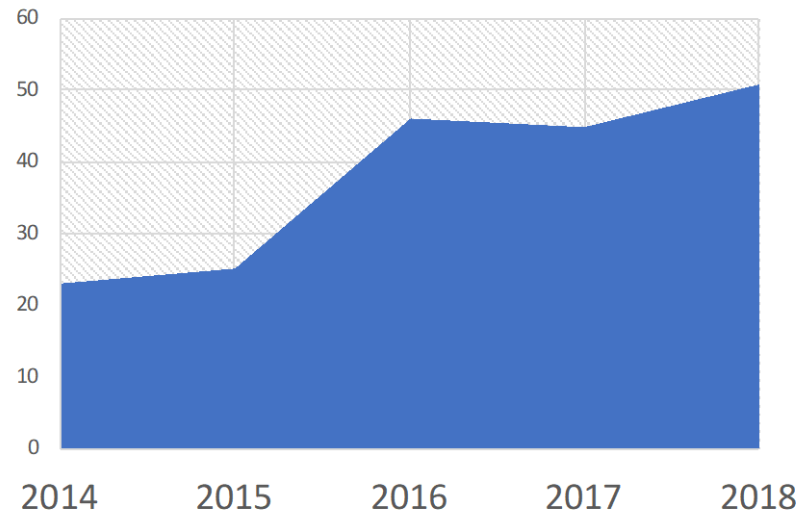
Bezpečnostné hrozby exponenciálne narastajú



Trend kvalifikácií a pracovnej sily v oblasti informačnej bezpečnosti

- **1,8 Mil.** je celosvetovo predpokladaný nedostatok profesionálov s bezpečnostnou kvalifikáciou do roku 2022
- **350 tis.** je v EÚ predpokladaný nedostatok profesionálov s bezpečnostnou kvalifikáciou do roku 2022
- **90 tis.** Je v EÚ predpokladaný rolí DPO do roku 2020
- **62%** organizácií neposkytuje primeranú úroveň odbornej prípravy pre profesionálov v oblasti kybernetickej bezpečnosti
- **41%** topmanažérov je presvedčených, že informačná bezpečnosť má vysokú prioritu

Nedostatok bezpečnostných kvalifikácií v %:



Prioritné oblasti s nedostatkom kvalifikácií:



31%
Bezpečnostné
analýzy
a vyšetrovanie



31%
Aplikačná
bezpečnosť

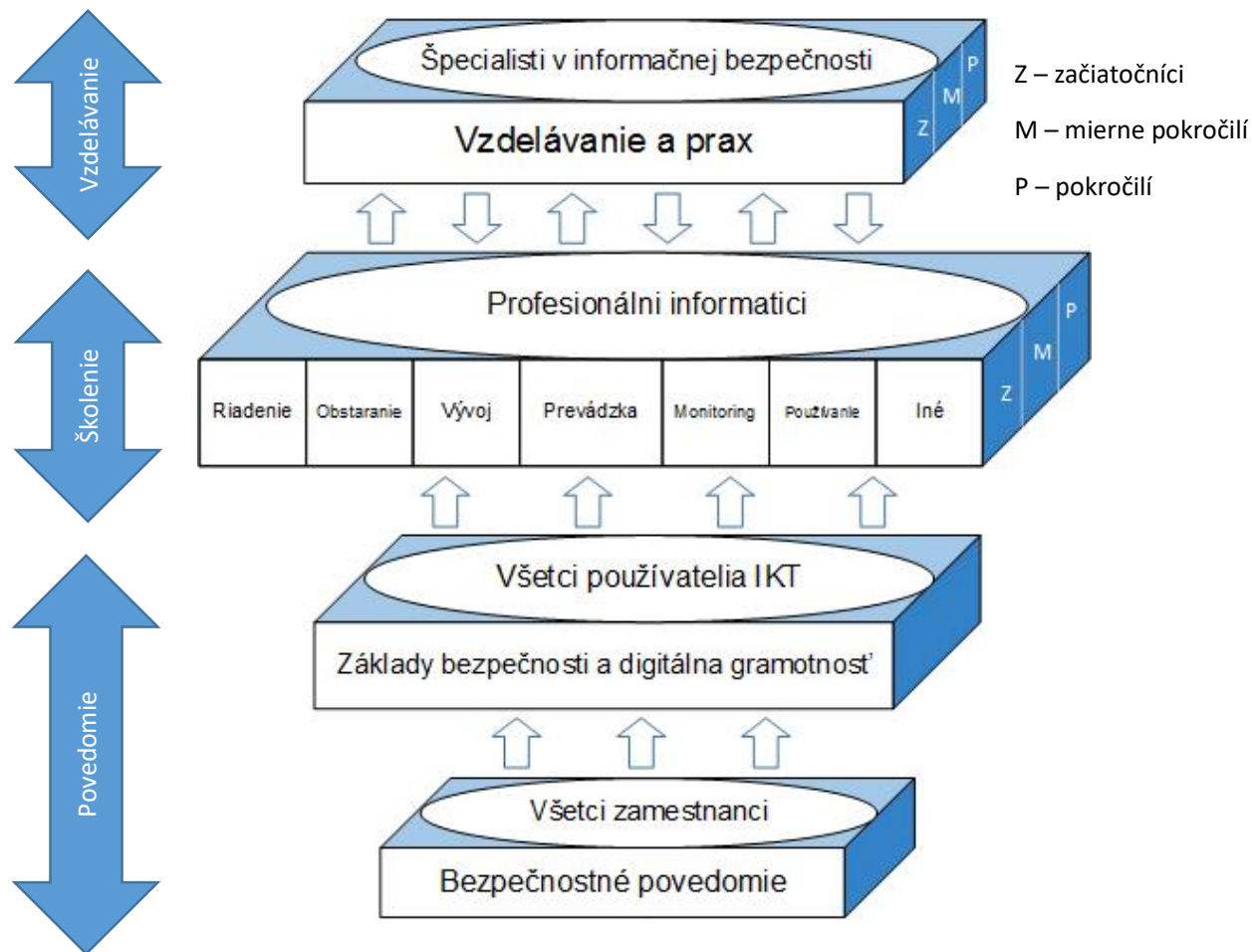


29%
Bezpečnosť
cloudových
služieb

Zdroj: ESG/ISSA The Life and Times of Cybersecurity Professionals 2017



Charakteristika vzdelávacích potrieb v informačnej bezpečnosti

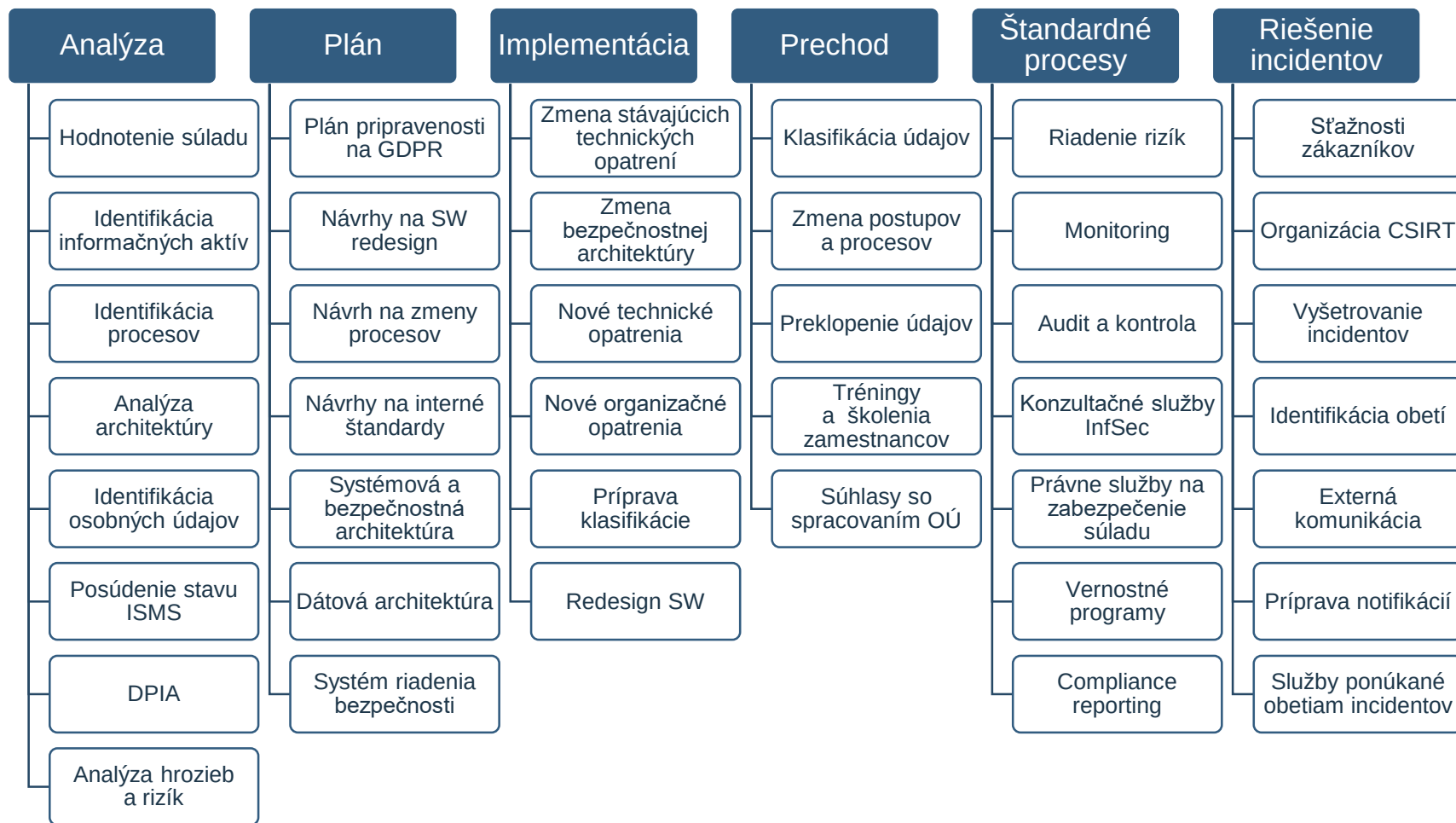


Zdroj: NIST Special Publication 800-16: Information Technology Security Training Requirements

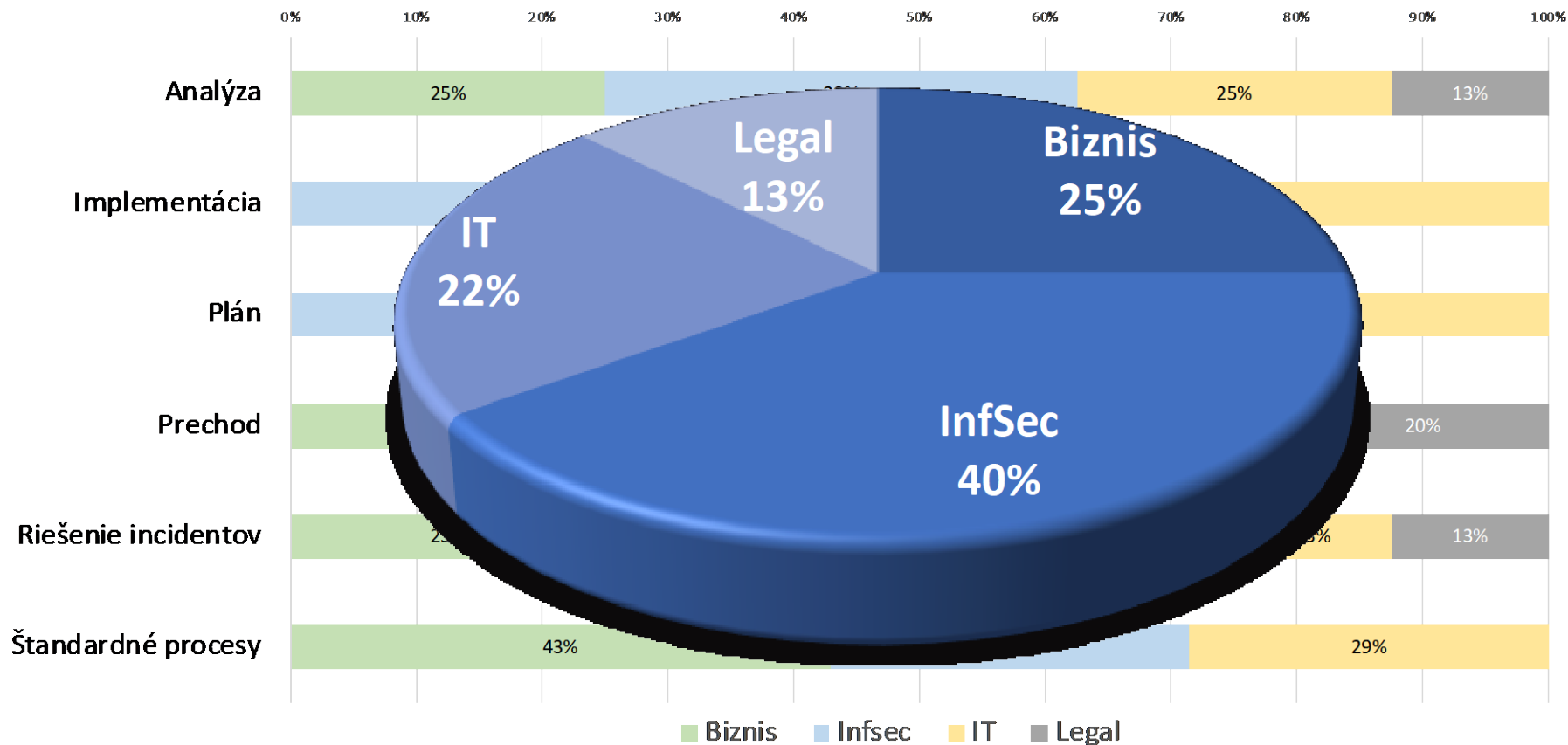
Požiadavky na kvalifikáciu pre jednotlivé kategórie

Úroveň znalostí	Laici	Odborní zamestnanci mimo IT	Manažéri mimo IT	IT manažéri	Informatici	Informačná bezpečnosť
Znalosť vybraných základných pojmov a ich významu	●	●	●	●	●	●
Použitie mechanizmov a procesov v bezpečnostných riešeniach		●	●	●	●	●
Legislatíva, súlad a etika ochrany údajov				●		●
Implementácia a uplatňovanie bezpečnostných mechanizmov a riešení				●	●	●
Návrh bezpečnostných mechanizmov a riešení					●	●
Návrh stratégií, analýza a hodnotenie bezpečnostných mechanizmov a riešení						●

Dosiahnutie a udržanie súladu s GDPR

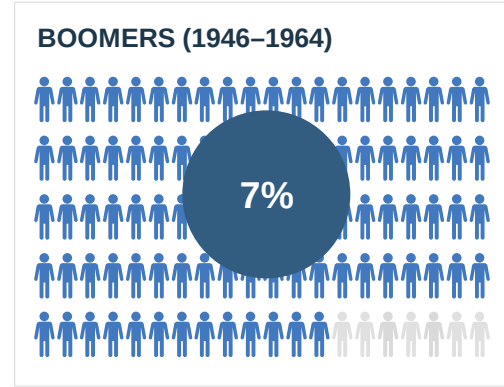
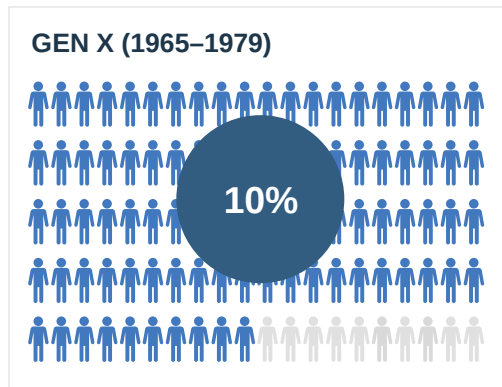
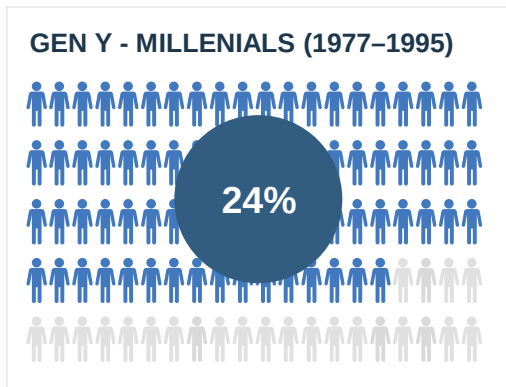


Distribúcia rolí v jednotlivých činnostiach súvisiacich s GDPR



Prijať, vychovať, alebo outsourcovať?

Zamestnanci bez akejkoľvek bezpečnostnej kvalifikácie:



- Mladá generácia o sebe typicky vyhlasuje, že je agilná a zvláda väčšie množstvo informácií
- Podľa štatistiky sú však kvalifikovanejší starší zamestnanci

Napriek tomu:

- **41%** zamestnancov je presvedčených, že ich organizácia by mala zamestnať a školiť skôr mladších zamestnancov než zamestnať ľudí s už primeranou úrovňou zručností

Riešením je zdieľanie zdrojov

- Organizácia môže zdieľať svoje bezpečnostné zdroje a využiť zdieľané cudzie zdroje
- Je možné vzájomne si „požičiavať“ odborné pracovné kapacity s inými podnikmi vo svojom odvetví
- Tomuto postupu relatívne bránia rôzne regulácie v oblasti zamestnanosti a daní.
- Efektívnejším spôsobom je využiť ponuku odborných spoločností, ktoré sa na trhu špecializujú práve na ochranu informačných aktív, t.j.
- použiť na vybrané procesy bezpečnosti obchodný model zvaný:

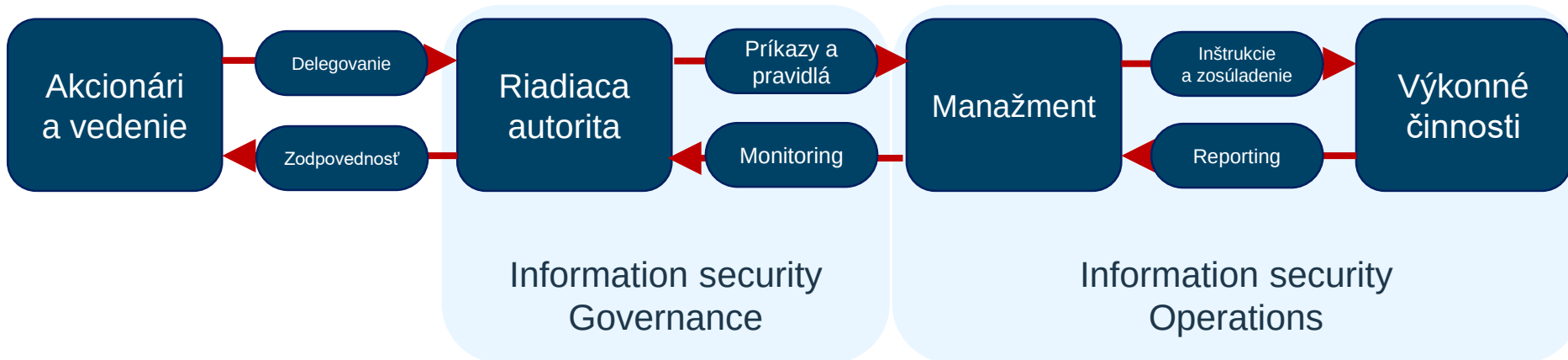
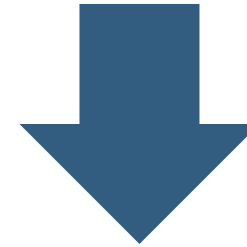
outsourcing



Kľúčové role a vzťahy v riadení bezpečnosti

Riadiaca úroveň

Výkonná úroveň



Zdroj: ISACA, isaca.org/cobit5



Čo je to kvalita a ako ju rozpoznať?



Kvalifikácia, certifikácia a certifikačné schémy

- **Certifikácia** je proces posudzovanie zhody a spôsob preukázania primeraných záruk pre udržanie súladu, pre:
 - Organizáciu ako celok
 - Proces v organizácii
 - Produkt / výrobok
 - Technologický systém
 - Odbornú spôsobilosť fyzickej osoby
- **Certifikačný proces sú činnosti, na základe ktorých certifikačný orgán určí, že predmet certifikácie spĺňa špecifikované požiadavky spôsobilosti**
- **Certifikačný proces:**
podanie žiadosti... -> vyhodnotenie... -> rozhodnutie o certifikácii... -> dohľad...
-> dohoda o používaní certifikátu a certifikačných značiek... -> recertifikácia...





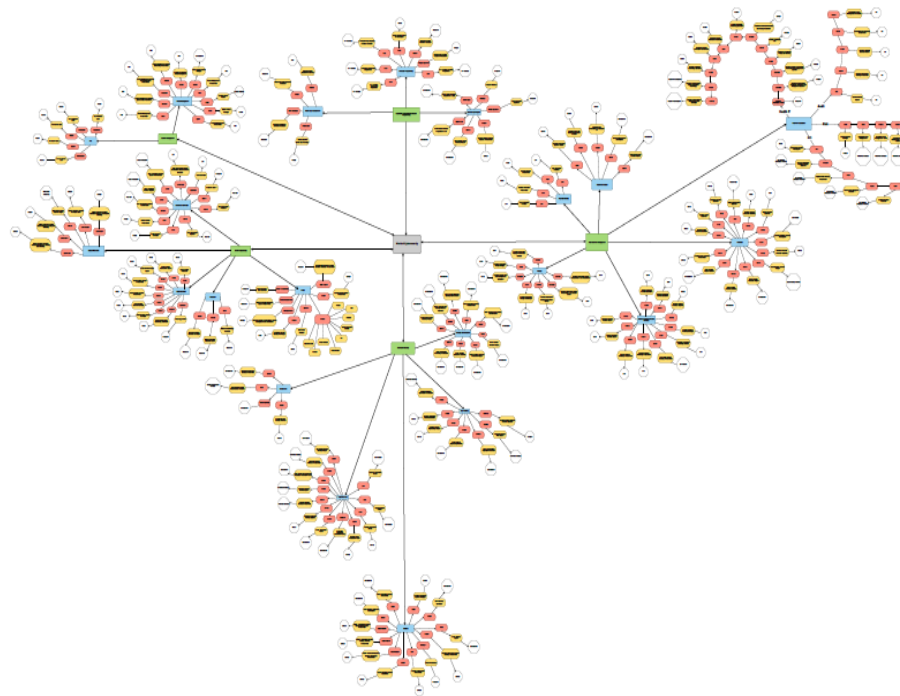
Kvalifikácia vs. posudzovanie zhody

- Aby vôbec mohla byť vykonávaná akákoľvek „certifikácia“, sú nutné tri podmienky:
 - **existencia všeobecne uznanej odbornej authority** - t.j. certifikačného orgánu ktorý navrhuje mechanizmus posudzovania, vykonáva posudzovanie, prípadne poveruje posudzovaním tretie strany
 - **existencia certifikačnej schémy** - t.j. všeobecne prijatého a akceptovaného mechanizmu a požiadaviek posudzovania
 - **existencia certifikačného systému** . t.j. súhrnu poznatkov a zdrojov realizácie certifikačného procesu podľa certifikačnej schémy (ktoré vedú k vydaniu certifikátu a k udržaniu spôsobilosti certifikovanej osoby / systému / produktu / procesu)
- **Snaha o umelé zavádzanie certifikačných schém, najmä zo strany samozvaných autorít je ekvivalentom „samokorunovacie“**



Certifikačné schémy v oblasti bezpečnosti a IKT

- Počet a komplexita certifikačných schém je veľká...
- Ako sa v tom vyznať?
 - Pochopiť princíp certifikácie
 - Rozhodnúť, aký predmet certifikácie hľadáte
 - Vyberať cielene vlastníctvo certifikátov podľa požadovanej domény
 - Opierať sa o uznávané certifikačné schémy



Príklad pre typický set certifikácií osoby a ich použitia v RFI

Kód kvalifikácie	Kvalifikácia	Minimálny počet
I1	ITIL v3	5
P1	Certified Information Systems Security Professional (CISSP)	4
P2	Global Information Assurance Certification (GIAC/SANS)	3
P3	Certified Ethical Hacker (CEH)	4
C1	Certified Information Systems Auditor (CISA/ISACA)	2
C2	Certified Information Systems Manager (CISM/ISACA)	2
C3	Certified in Risk and Information Systems Control (CRISC/ISACA)	2
S1	Certified SCADA Security Architect (CCSA) alebo iný ekvivalentný doklad expertnej úrovne znalostí v oblasti Supervisory Control and Data Acquisition	1
S2	Certified SAP Security Architect	2
M1	GIAC - Certified Web Application Penetration Tester (GWAPT)	2
M2	GIAC Reverse Engineer Malware (GREM)	2
M3	Offensive Security Certified Expert (OSCE)	2
M4	Offensive Security Certified Professional (OSCP)	2

KOMPONENTY SLUŽBY	POPIS	Požadované kvalifikácie
Posúdenie projektu z hľadiska bezpečnosti	• Posúdenie vyspelosti procesov • Analýza bezpečnostných rizík • Návrh bezpečnostnej stratégie • Návrh bezpečnostnej architektúry • Preskúmanie návrhu implementácií aplikácií a systémov z hľadiska bezpečnosti • Poskytovanie bezpečnostných konzultácií týkajúci sa infraštruktúry počas prípravy projektov	P1, P2, C1, C2, C3, S1, S2, I1



Tri éry bezpečnosti z historického pohľadu...



- **Ochrana perimetra:** bezpečnosť, ktorá vymedzuje

Pre 2005

- Udržiavanie chránených aktív v bezpečí obmedzovaním prístupu k nim



- **Výkonný monitoring:** bezpečnosť, ktorá napomáha pochopeniu

2005+

- Monitoring prístupu ku chráneným aktívam v reálnom čase,
- Analytika používaná na detekciu odchýliek, napomáhajúc špecialistom bezpečnosti riešiť najväčšie problémy ako prvé



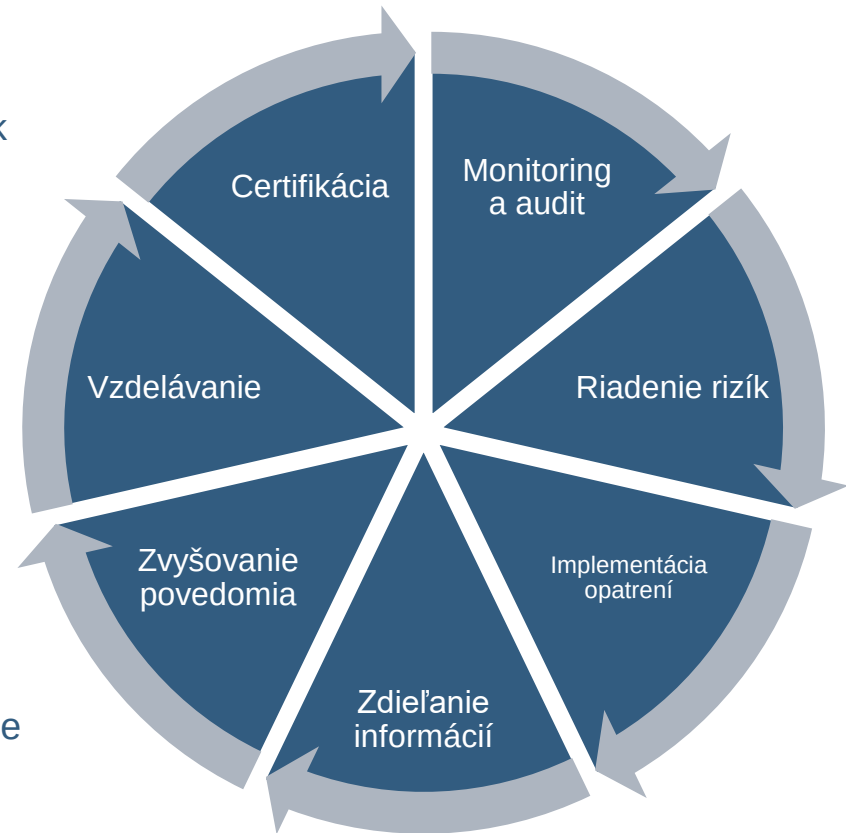
- **Kognitívna bezpečnosť:** bezpečnosť ktorá chápe, dôvodí a učí sa chápať

2015+

- Bezpečnostný monitoring už nepostačuje, pretože ten dokáže identifikovať a prioritizovať známe hrozby, nie však tie novo vznikajúce.
- Kognitívna bezpečnosť vyplňa medzeru tým, že dáva zmysel 80% dát, ktoré sú neštruktúrované – dosiahnuteľné v tisíckach dokumentov, správ, odborných materiálov, akademických prác, novinových článkov, blogov, odvetvových hlásení a ďalších zdrojov

Závery

- Pochopenie princípu certifikácií je základom pre posudzovanie zhody a preukázanie primeraných záruk
- Spoliehajte sa na certifikácie od uznávaných autorít
- Porušenie ochrany osobných údajov = bezpečnostný incident.
- Ochrana údajov = informačná bezpečnosť.
- Na reálne preukázanie primeraných záruk je potrebné certifikovať najmä procesy informačnej bezpečnosti a riadenia rizík
- Napriek tomu, že mladá generácia o sebe vyhlasuje, že je agilná, kvalifikovanejší sú starší zamestnanci
- Neustále narastajúce množstvo bezpečnostných informácií bude v blízkej budúcnosti možné zvládať len riešeniami, ktoré sú podporené kognitívnou výpočtovou analytikou



ĎAKUJEM

SLEDUJTE NÁS NA:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

 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.

