AKB
Asociácia kybernetickej bezpečnosti

# Výhody a nevýhody regulácie - alebo, ako zákon o kybernetickej bezpečnosti ovplyvní podnikanie?

ITAPA 2019

# Môže regulácia pomôcť kybernetickej bezpečnosti?

- Cieľom regulácie je dosiahnutie primeranej spôsobilosti subjektov odolať kybernetickým bezpečnostným hrozbám
- V rámci definície pojmu „informačná bezpečnosť“ môže regulácia napomôcť:
  - návrhom jednotných metód ochrany informácií
  - návrhmi na zlepšenie procesov manažmentu hrozieb a rizík, ktoré pôsobia na informačné aktíva,
  - vynútením aktivít zameraných na dosiahnutie dostatočnej úrovne ochrany informácií
  - tlakom na dosiahnutie stavu, kedy sú eliminované riziká vyplývajúce z hrozieb
- Ako?
  - právnymi prepismi, ktoré efektívne stanovia pravidlá chovania a dosiahnu

    žiaduce správanie zúčastnených subjektov

# Benchmarking stavu kybernetickej bezpečnosti

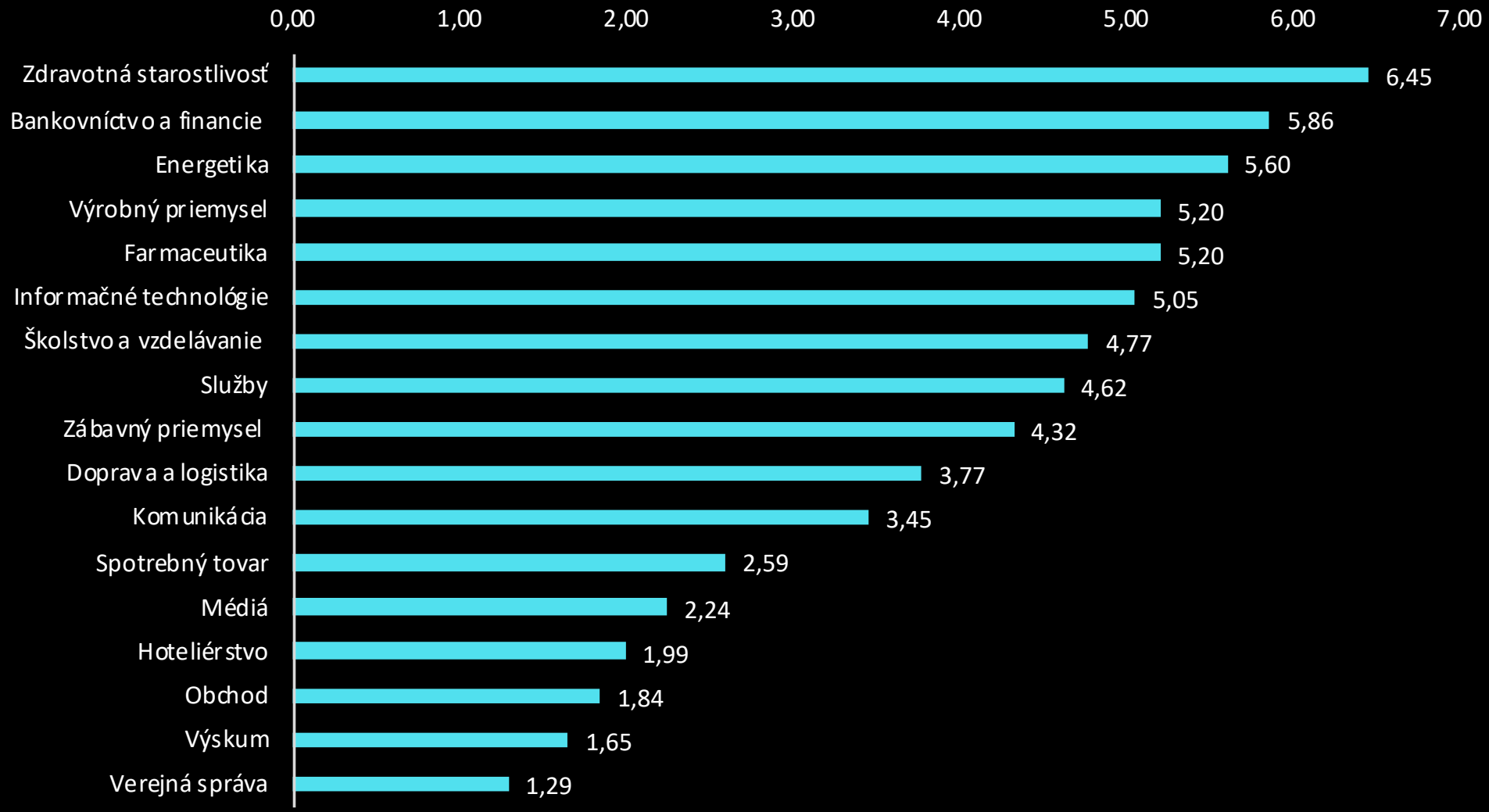
- Verizon: 2018 Data Breach Investigations Report
- Ponemon Institute LLC: The Cost of a Data Breach Report
- Positive Technologies: Cybersecurity threatscape 2019

| | | | | | |
|---|---|---|---|---|---|
| Zdravotná starostlivosť | Energetika | Bankovníctvo a financie | Výrobný priemysel | Farmaceutika | Služby |
| Školstvo a vzdelávanie | Médiá | Komunikácia | Zábavný priemysel | Hoteliérstvo | Informačné technológie |
| Doprava a logistika | Výskum | Verejná správa | Spotrebný tovar | Obchod | |

# Distribúcia jednotlivých kategórií incidentov

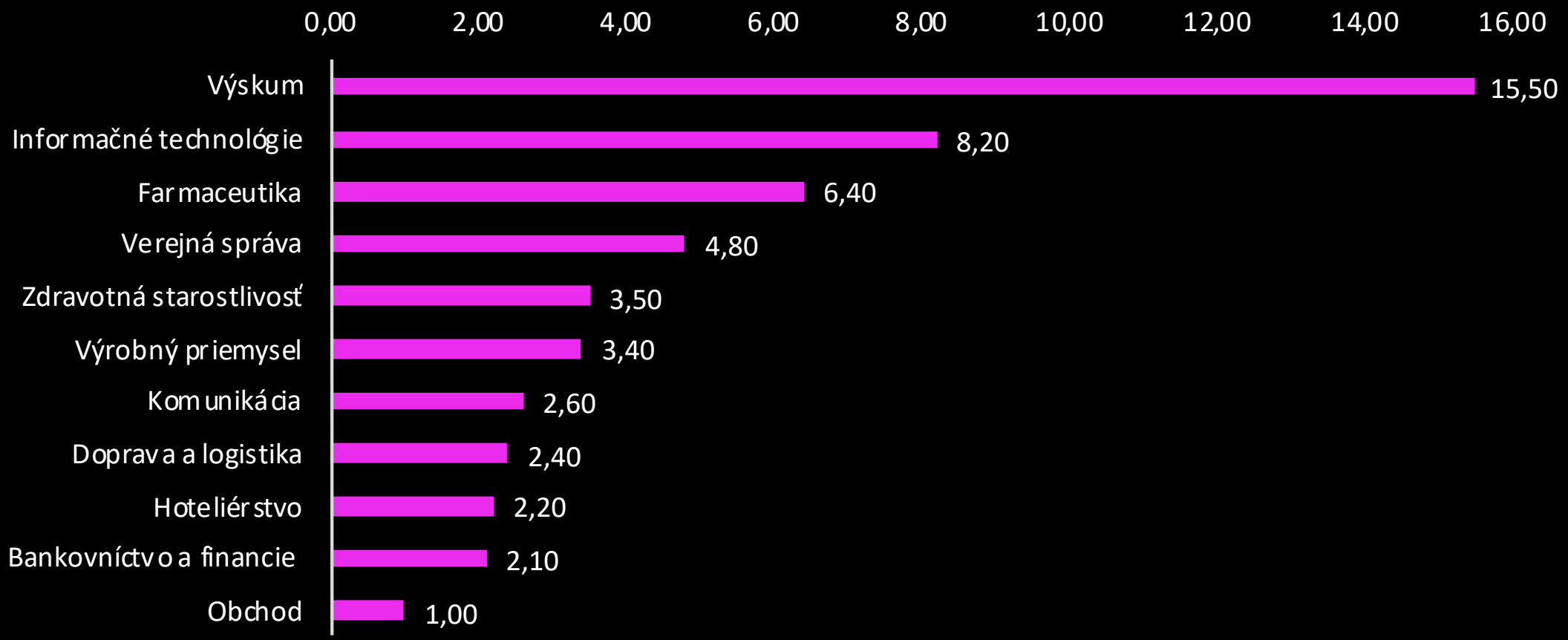

Zdroj: Verizon 2018 Data Breach Investigations Report

# Priemerné straty spôsobené incidentmi podľa odvetví




(Mil. USD)

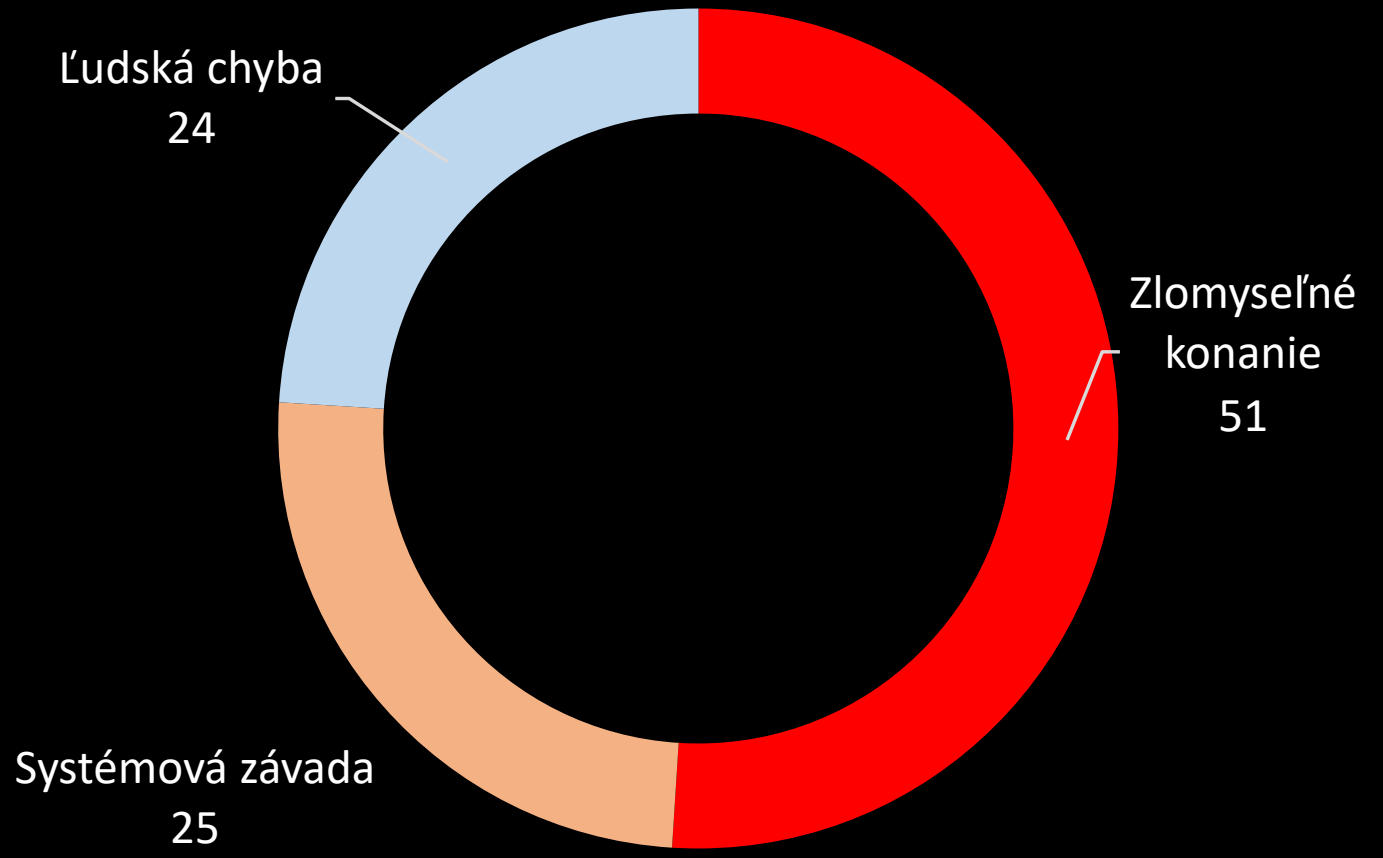
# Úbytok trhových výnosov odvetví spôsobených incidentmi




(%)

# Typické príčiny incidentov

- Príčiny incidentov sa líšia podľa zdroja
- Spôsob riešenia incidentu spôsobeného vonkajším útočníkom alebo zlomyseľným zamestnancom sa podstatne líši od riešenia incidentu spôsobeného ľudskou chybou alebo zlyhaním systému
- V tohtoročnej správe boli preskúmané tri základné príčiny incidentov a náklady s nimi spojené




(%)

# Komponenty nákladov súvisiacich s incidentom

- Štúdia sa zamerala na hlavné procesné aktivity, spojené s nákladmi na detekciu incidentov reakciu na incidenty a nápravu ich dopadov.

Štyri hlavné nákladové položky:

- Detekcia a eskalácia

- Notifikácia

- Odozva na incident

- Obchodné straty

# Detail kategórií nákladov v kontexte incidentov

## Detekcia a eskalácia

- Forenzné a analytické činnosti
- Testovanie a auditné služby
- Riadenie krízového tímu
- Oznámenia výkonnému manažmentu a regulátorovi

## Notifikácia

- e-maily, listy, odchádzajúce telefónne hovory, oznámenia dotknutým osobám
- komunikácia s regulátormi, aplikácia regulačných požiadaviek, zapojenie externých odborníkov

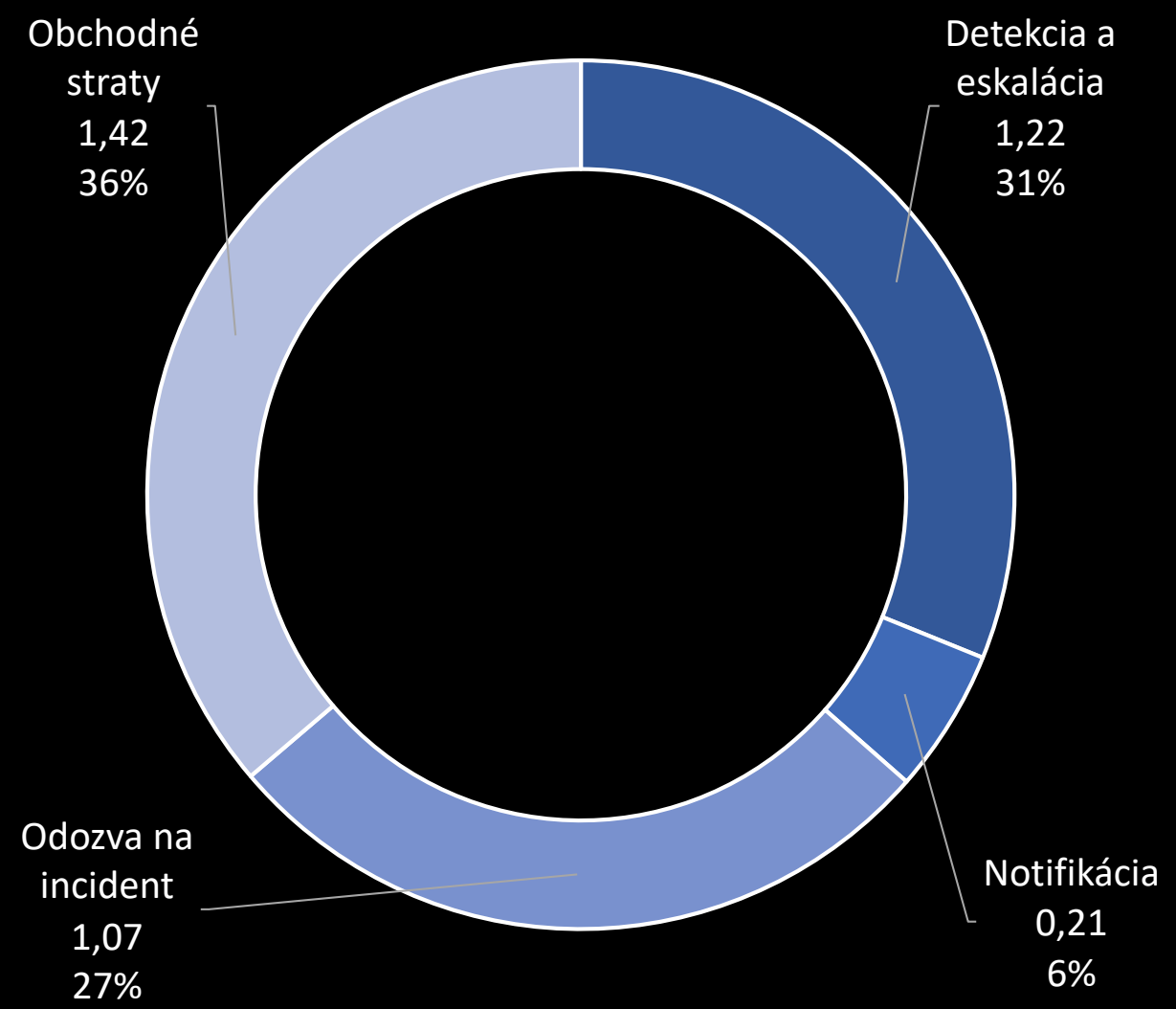
## Odozva na incident

- Činnosti technickej podpory / prichádzajúca komunikácia
- Služby ochrany identity
- Generovanie nových účtov , vydávanie kariet atď
- Výdavky na právne služby
- Dodatočné zľavy na produkty
- Regulačné zásahy (pokuty)

## Obchodné straty

- Náklady vzniknuté narušením kontinuity a straty zo zisku z dôvodu systémových prestojov
- Náklady vzniknuté stratou zákazníkov a získania nových zákazníkov (odchodovosť)
- Reputačné straty a strata dobrého mena

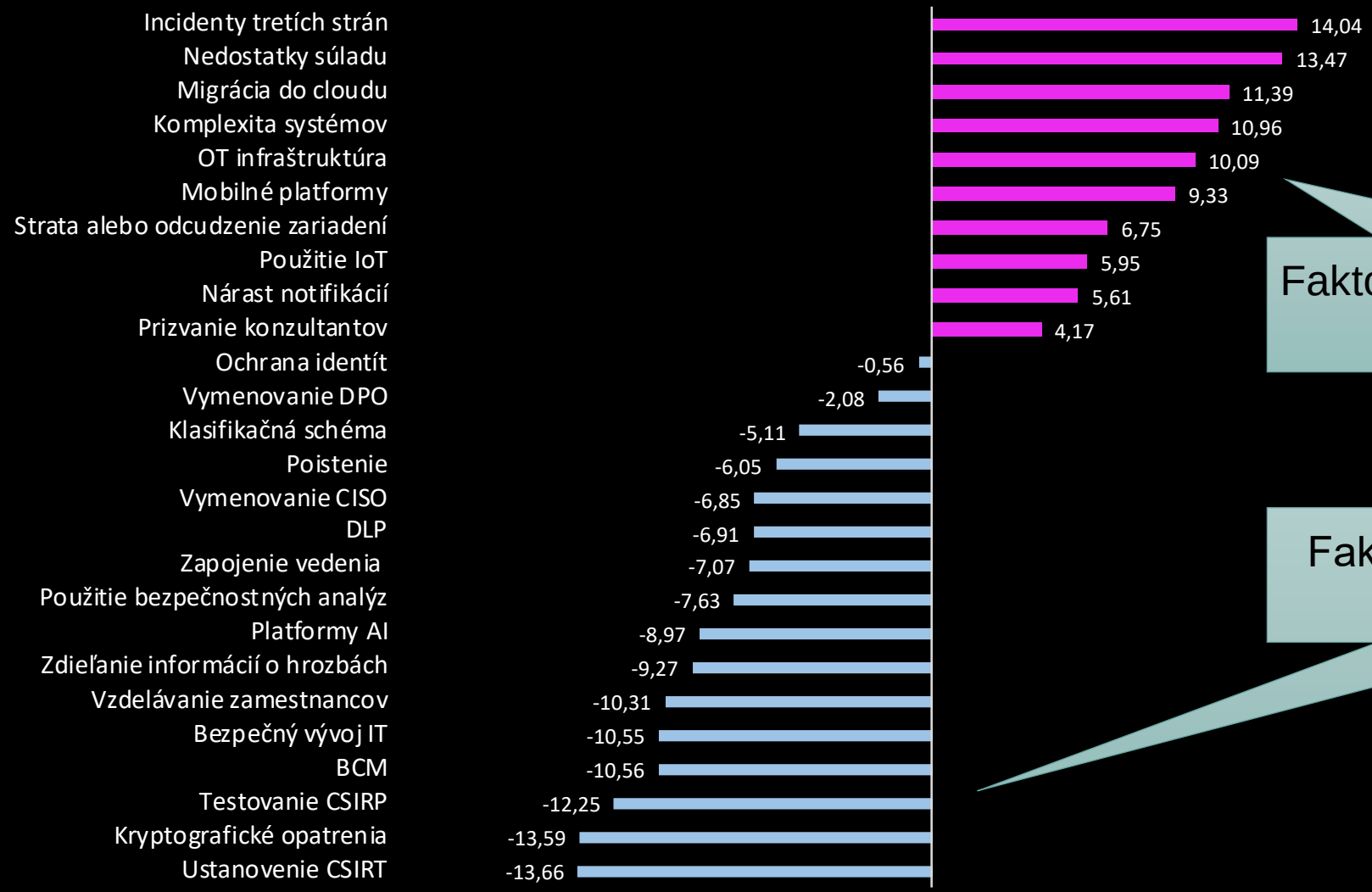
# Distribúcia nákladov podľa kategórií




(Mil. USD)

# Faktory ovplyvňujúce náklady súvisiace s incidentom

(odchýlka od celosvetového priemeru - údaje normalizované na incident)

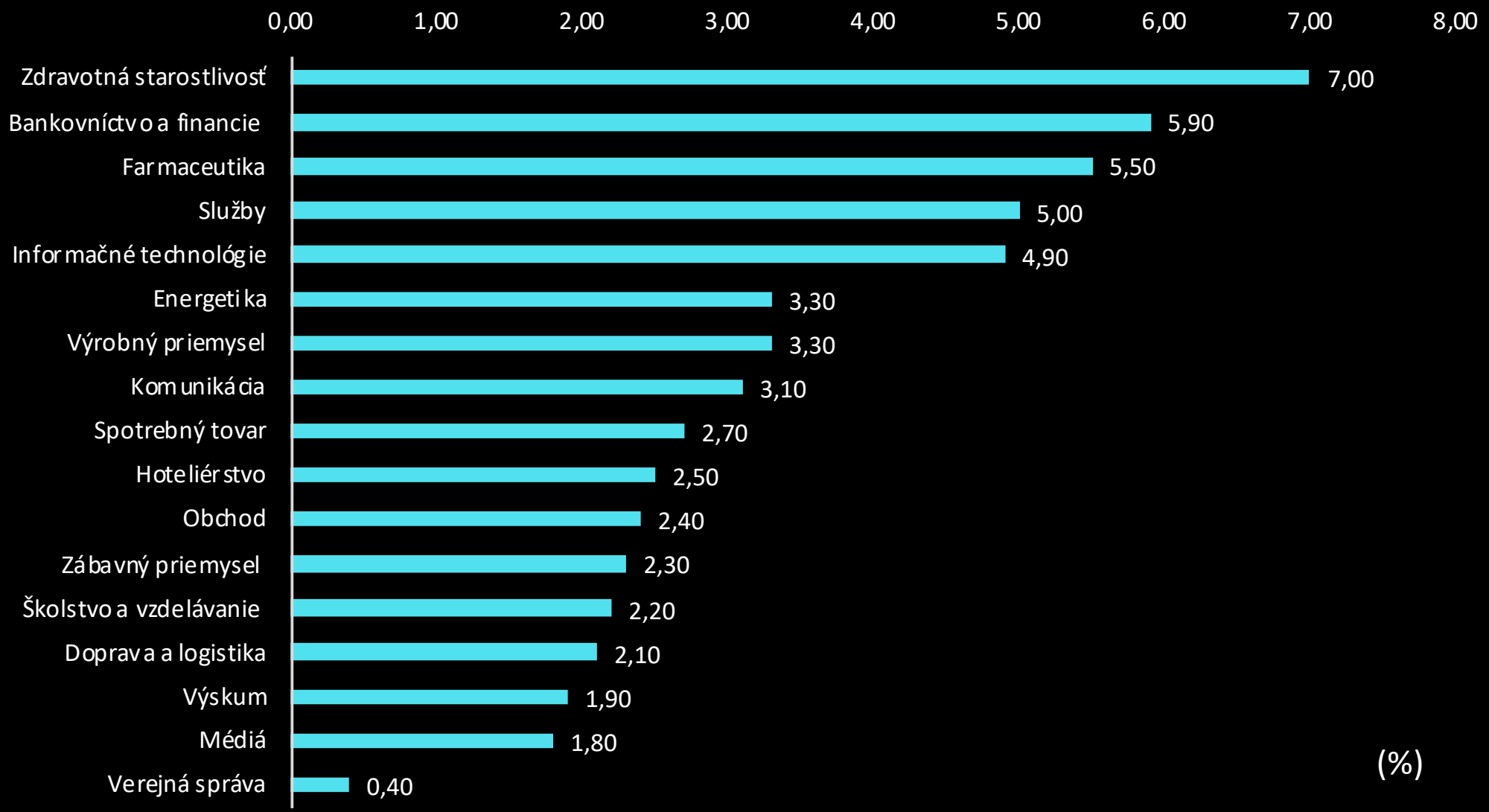



Faktory, ktoré potenciálne pôsobia na zvyšovanie nákladov

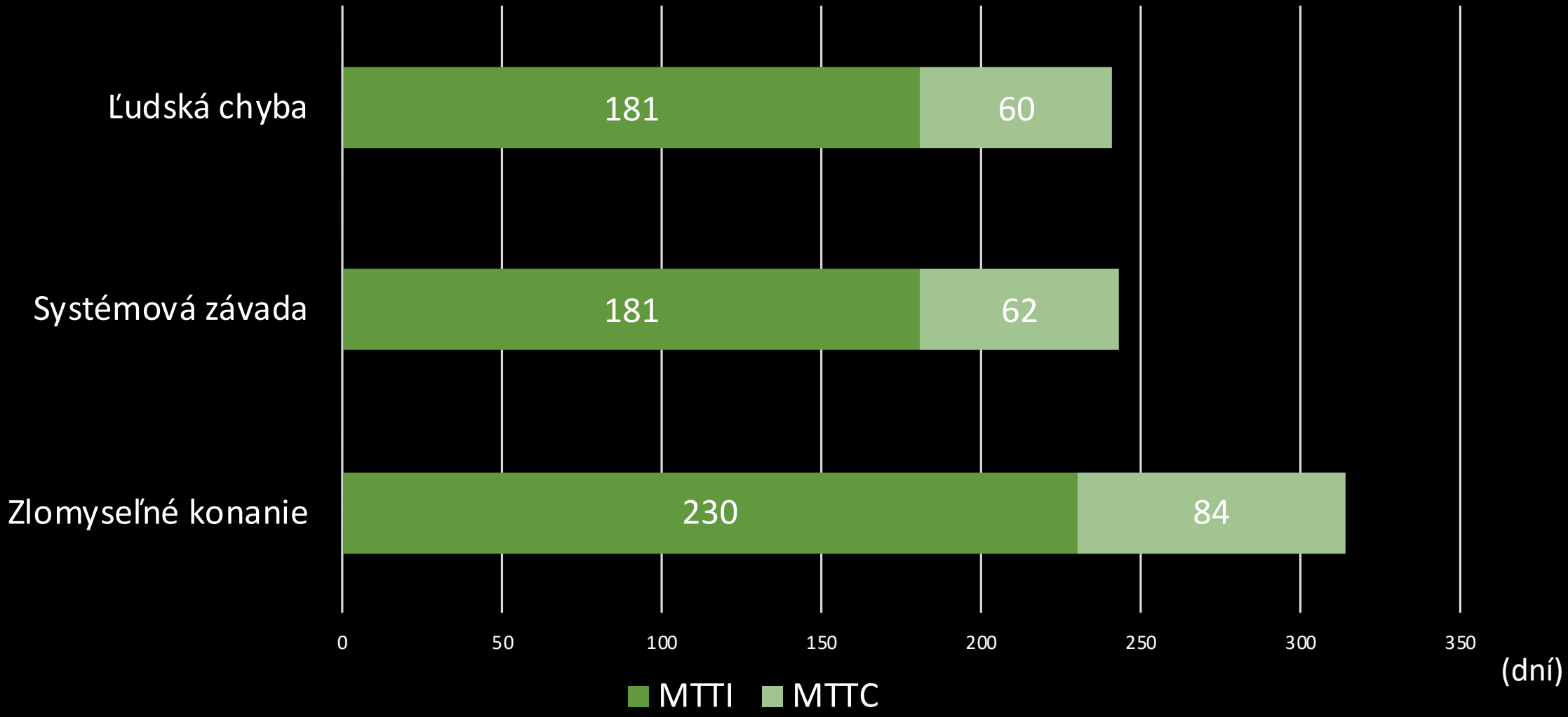
Faktory, ktoré ošetrujú (znižujú) potenciálne straty

(USD)

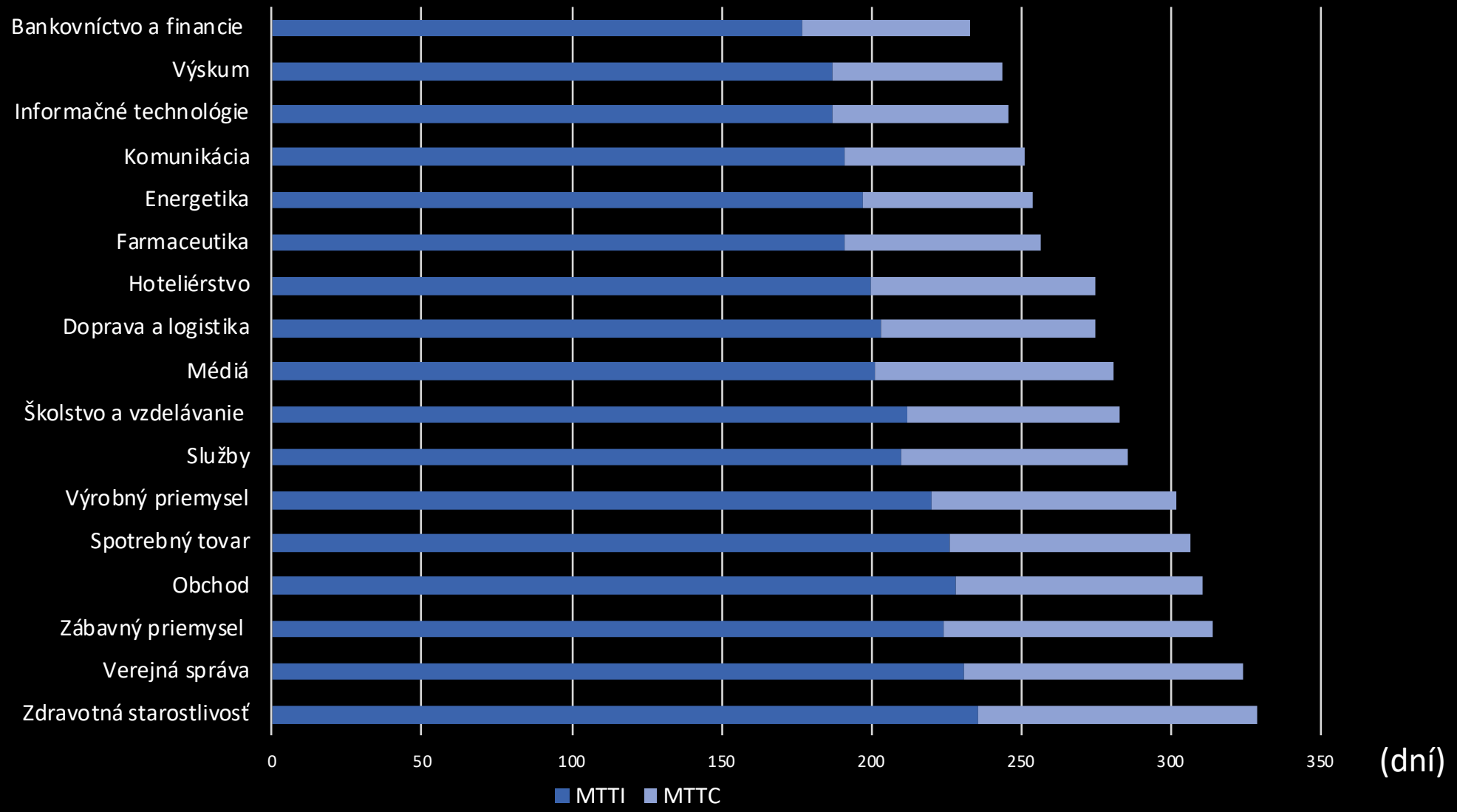
# Odchodovosť klientov podľa odvetví



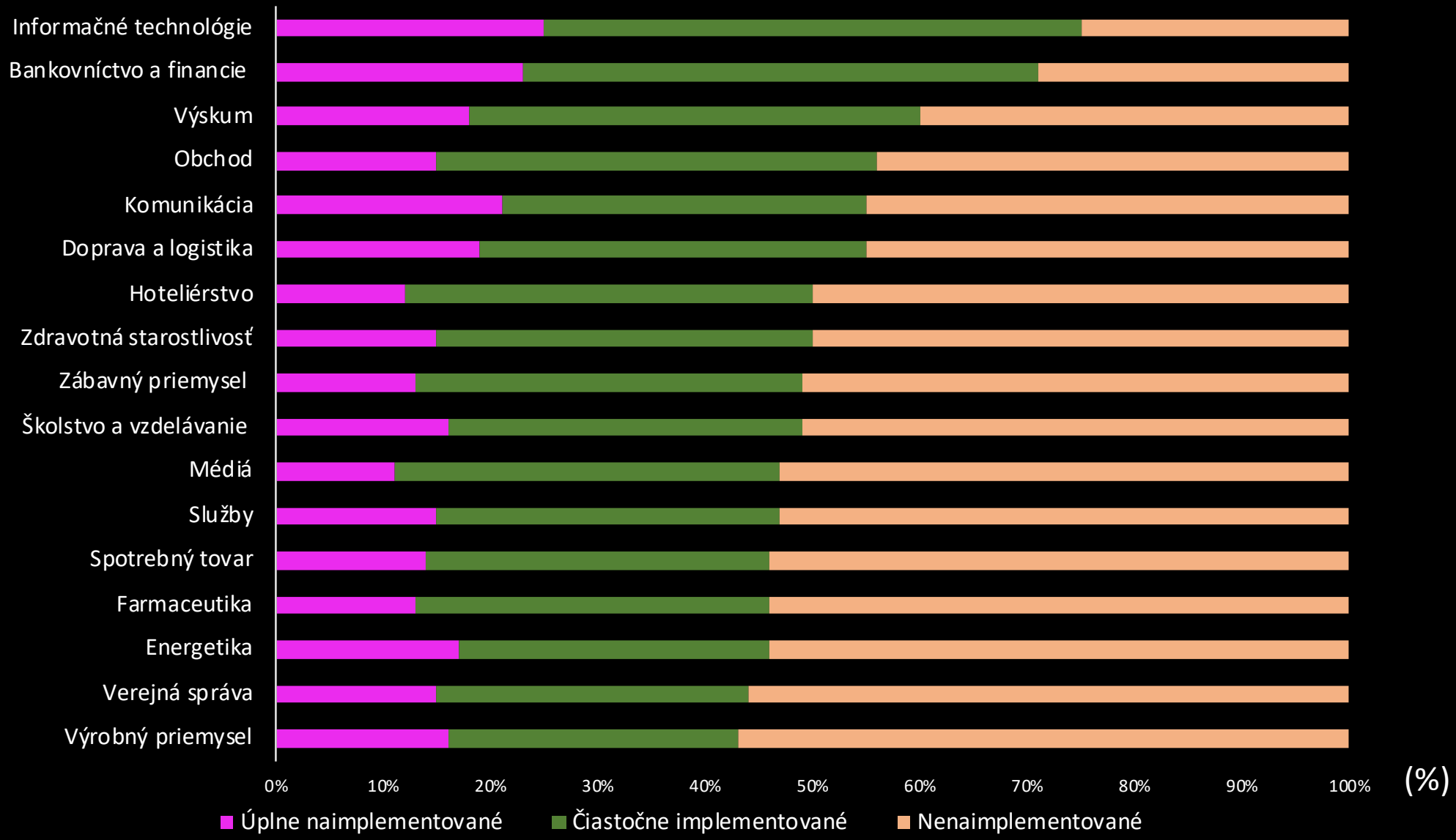
# Stredná doba identifikácie a riešenia incidentu podľa príčiny



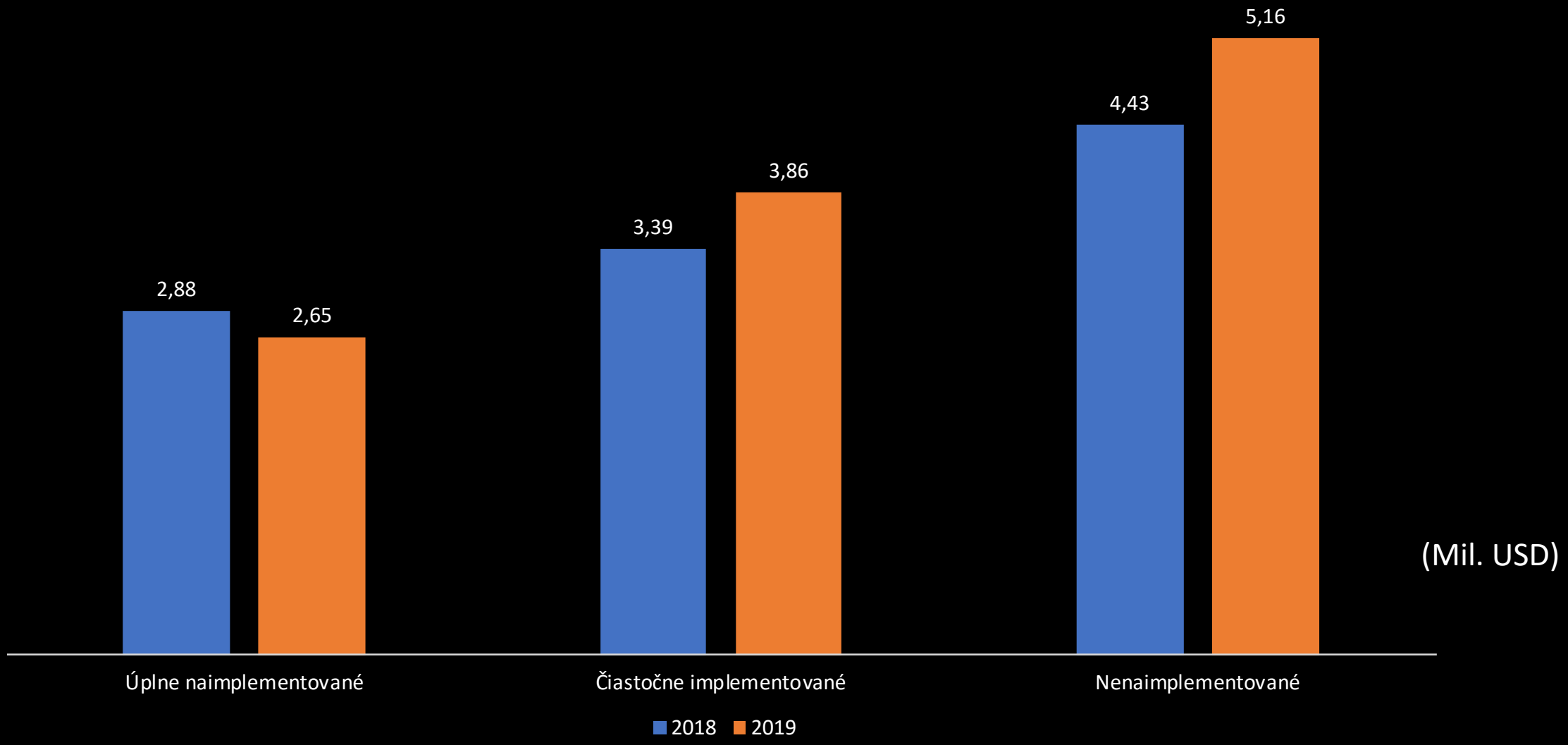
# Stredná doba identifikácie a riešenia incidentu podľa odvetví



# Stav technických bezpečnostných opatrení podľa odvetví



# Technické opatrenia znižujú potenciálne straty




(Mil. USD)

# Čo môže napomôcť zníženiu nákladov súvisiacich s incidentom?

- Technické opatrenia a automatizácia činností dokázateľne znižujú náklady vyplývajúce z procesu detekcie a riešenia incidentov
- Kognitívne systémy a prostriedky umelej inteligencie napomáhajú v detekcii a riešení incidentov
- Cieľom má byť zásadné skrátenie strednej doby identifikácie a riešenia incidentu (MTTI, MTTC)
- Dve nákladové položky „Detekcia a eskalácia“ a „Odozva na incident“ spolu predstavujú 58% nákladov súvisiacich s incidentom
- „Detekcia a eskalácia“ a „Odozva na incident“ sú typickými súčasťami procesu zvaného bezpečnostné operácie (Security operations)
- Bezpečnostné operácie sú IT službou - nedostatok zdrojov a kvalifikácií sú riešiteľné formou ich outsourcingu
- Benchmarking môže byť vhodným nástrojom, ktorý napomôže rozvoju spôsobilostí v KB

# Ako sa nedá dosiahnuť žiaduce správanie subjektov?

- Nezmyselnými a extenzívnymi regulačnými požiadavkami
- Neúmerne násilným presadzovaním požiadaviek
- Pokutami, ktoré vytvárajú novú hrozbu a odvádzajú pozornosť od pôvodných rizík

- Povinnosť, vynútená hrozbou sankcie je  tzv. vonkajšou motiváciou, ktorá likviduje vnútornú motiváciu
- Nezmyselné regulácie sú pre bezpečnosť kontraproduktívne (zvyčajným dôsledkom je obchádzanie pravidiel)

# Diskusia je vítaná... ☺


https://www.akb.sk

@makatura

makatura@akb.sk