

# *Celosvetový prieskum hospodárskej kriminality 2011 Slovensko*

Počítačová kriminalita v popredí

*Takmer 4000 organizácií  
v 78 krajinách pomohlo  
poskytnúť celkový obraz  
o podvodoch a ďalších  
trestných činoch*

*December 2011*



# Úvod

Dovoľujeme si prezentovať Vám výsledky **Globálneho prieskumu hospodárskej kriminality, ročník 2011**. Prieskumu sa zúčastnilo **3 877** respondentov zo **78 krajín**, vrátane 84 popredných spoločností a organizácií na Slovensku, a preto i naďalej zostáva najväčšou štúdiou svojho druhu na svete. Veríme, že štúdia poskytne vedeniu a predstaviteľom organizácií unikátny prienik do vnímania, prevencie a dopadu ekonomickej kriminality na podnikateľské subjekty vo svete.

Hospodárska kriminalita si nevyberá. Zasahuje organizácie po celom svete a žiadne odvetvie či organizácia nie sú voči nej imúnne. Jej následkom nie sú len zvýšené náklady, ale môže vážne poškodiť i značku a dobré meno firmy a spôsobiť tak stratu podielu na trhu. Keďže súčasná spoločnosť toleruje neetické správanie čoraz menej, organizácie si musia dôveru verejnosti budovať a udržiavať nepretržite.

Náš v poradí už šiesty celosvetový prieskum hospodárskej kriminality, na ktorom sa Slovensko zúčastňuje po tretíkrát, **poukazuje na vzrastajúcu hrozbu počítačovej kriminality**. Väčšina ľudí a organizácií v súčasnosti čoraz viac spolieha na internet a iné technológie. Týmto správaním sa však vystavujú potenciálnym útokom podvodníkov z celého sveta. Úniky informácií, krádeže citlivých údajov, počítačové vírusy alebo hackerstvo sú relatívne novým, ale o to nebezpečnejším druhom hospodárskej kriminality. Náš prieskum poukazuje na ich rozsah, dopad a na spôsob, akým ovplyvňujú organizácie po celom svete.

V rámci prieskumu sme hľadali odpovede na otázky týkajúce sa počítačovej kriminality, jej hrozieb a spôsobov, akými sa organizácie snažia čeliť jej útokom. Zároveň sme do prieskumu zahrnuli aj niekoľko základných otázok týkajúcich sa hospodárskej kriminality ako takej, ktoré nám pomohli sledovať dlhodobé trendy hospodárskej kriminality a porovnať ich s tohtoročnými zisteniami.

Výsledky prieskumu sú rozdelené na dve základné sekcie:

- počítačová kriminalita – jej vplyv na organizácie, ich pripravenosť čeliť tejto hrozbe a opatrenia, ktoré prijímajú v rámci boja proti počítačovej kriminalite; a
- súčasný stav hospodárskej kriminality – táto časť je zameraná na typy páchaných podvodov, spôsoby ich odhaľovania, páchatelov a postihy voči nim.

**Sirshar Qureshi**  
Partner, Forenzné služby, PwC

**Michal Kohoutek**  
Direktor, Forenzné služby, PwC

# Hlavné zistenia

## Počítačová kriminalita

- V minulosti štatisticky nevýznamná **počítačová kriminalita** figuruje v tohtoročnom prieskume na jednej z prvých troch priečok hospodárskych zločinov na Slovensku (17%) s hodnotou takmer na úrovni priemeru regiónu strednej a východnej Európy (18%) a celého sveta (23%). Aj napriek tomu, len 12% spoločností na Slovensku si myslí, že bude v priebehu nasledujúcich 12 mesiacov **čeliť počítačovej kriminalite**, čo je výrazne menej v porovnaní s krajinami strednej a východnej Európy (22%) a celosvetovým priemerom (26%).
  - Slovenské spoločnosti si čoraz viac uvedomujú nebezpečenstvo počítačovej kriminality. Až 95% respondentov uviedlo, že ich vnímanie rizika počítačovej kriminality sa buď zvýšilo alebo zostalo na rovnakej úrovni ako v minulom roku. K tomuto nárastu povedomia došlo aj napriek tomu, že viac než polovica respondentov na Slovensku, za posledných 12 mesiacov **neabsolvovala žiadne školenie k bezpečnosti výpočtovej techniky**.
  - V prípade ohrozenia počítačovou kriminalitou sa spoločnosti najviac obávajú **krádeže osobných údajov a práv duševného vlastníctva a poškodenia mena**.
  - Hrozba počítačovej kriminality už nie je vnímaná len ako hrozba prichádzajúca zvonku: až 43% respondentov považuje za rovnako pravdepodobné, že táto hrozba príde zvonku alebo zvnútra spoločnosti, alebo dokonca, že táto hrozba má výlučne interný pôvod. V tom, že za najpravdepodobnejší zdroj interného nebezpečenstva počítačovej kriminality sa považuje **oddelenie informačných technológií**, sa zhodujú respondenti nielen na Slovensku, ale aj v regióne strednej a východnej Európy a na celom svete.
  - Takmer 70% respondentov uviedlo, že disponujú **vlastnými prostriedkami na prevenciu a odhalenie** počítačovej kriminality a 44% tiež verí, že ich organizácia je schopná vyšetriť počítačovú kriminalitu interne. Predpokladáme, že tieto schopnosti sú väčšinou prisudzované oddeleniu informačných technológií, ktoré je však zároveň považované za najväčšiu internú hrozbu počítačovej kriminality. Je preto znepokojujúce, že iba 13% respondentov spolupracuje so špecialistami z oddelení forenzných technológií.
  - Iba 20% slovenských spoločností **prehodnocuje riziká počítačovej kriminality častejšie než raz za rok**. Aj napriek tomu, že to korešponduje s výsledkami v regióne strednej a východnej Európy a na celom svete, bolo by vhodné, aby spoločnosti prehodnocovali tieto riziká častejšie, aby udržali krok s rýchlosťou vývoja rizík informačných technológií.
- ### Súčasný stav hospodárskej kriminality
- Hospodárska kriminalita zostáva i naďalej vážnym problémom ovplyvňujúcim organizácie na celom svete, vrátane Slovenska. 21% spoločností na Slovensku sa za uplynulých 12 mesiacov stretlo s minimálne jedným prípadom hospodárskej kriminality. Tento výsledok je mierne pod priemerom krajín strednej a východnej Európy (30%) i celého sveta (34%).
  - Avšak výsledky nášho prieskumu poukazujú na skutočnosť, že mechanizmy na odhalenie podvodov zavedené v spoločnostiach na Slovensku nie sú vždy dostatočné či efektívne, a preto mnohé prípady hospodárskej kriminality môžu zostať neodhalené:
    - Aj napriek tomu, že existuje priamo úmerný vzťah medzi frekvenciou vykonávaných hodnotení rizík podvodu a počtom odhalených podvodov, 49% slovenských respondentov uviedlo, že alebo vôbec nehodnotí riziká podvodu, alebo nevie, či sa v ich organizácii takéto hodnotenie vykonáva. Keďže tento výsledok presiahol svetový priemer (41%), môže to byť zároveň vysvetlením pre pomerne nízky počet odhalených prípadov podvodu na Slovensku. Je znepokojujúce, že 70% respondentov, ktorí nevykonávajú posúdenie rizika podvodu, nevie, čo posúdenie zahŕňa a nepozná dôvody, prečo ho organizácia nevykonáva.
    - 61% slovenských spoločností **nemá zavedený mechanizmus informačnej linky** (tzv. whistle-blowing linka). Navyše, viac než polovica respondentov využívajúcich informačnú linku považuje tento nástroj za málo alebo úplne neefektívny. Tento výsledok je prekvapivý, pretože na základe našich skúseností fungujúca informačná linka pomáha odhaliť podvody práve tam, kde môžu byť iné detekčné prostriedky neúčinné.
  - Medzi tri najčastejšie typy hospodárskej kriminality patrí **sprenevera majetku, počítačová kriminalita a korupcia a úplatky**. Na Slovensku sa firmy najčastejšie stretávajú so spreneverou majetku (94%), ktorá takisto prevláda aj v krajinách strednej a východnej Európy (69%) a celosvetovo (72%). V porovnaní s výsledkami prieskumu z roku 2009 došlo v tejto kategórii na Slovensku **k výraznému nárastu**, a to až o 49%.
  - **Korupcia a úplatky vzrástla** na Slovensku od roku 2009 o 7 percentných bodov na 17% a dosiahla tak rovnakú úroveň ako počítačová kriminalita. Porovnanie s priemerom v krajinách strednej a východnej Európy (36%) naznačuje, že skutočný výskyt prípadov podplácania a korupcie na Slovensku môže byť vyšší, avšak nebol odhalený.
  - Najväčšia hrozba z pohľadu hospodárskej kriminality prišla za posledných 12 mesiacov zvnútra organizácií - **z radov zamestnancov (2011: 61%; 2009: 30%)**. Až 73% interných podvodov spáchali na Slovensku pracovníci na nižších pozíciách, čo je výrazne viac než v krajinách strednej a východnej Európy (36%) a vo svete (39%). Najčastejšou reakciou spoločností bolo v prípade interného páchatela rozviazanie pracovného vzťahu, a to v **82% prípadov**.
  - Externí páchatelia sa podieľali na jednej tretine podvodov – **z toho zákazníci (67%) a predajcovia/sprostredkovatelia (33%)**. Organizácie na Slovensku ukončili obchodné vzťahy s externými páchatelmi v 67%, čo predstavuje nielen nárast zo 45% v roku 2009, ale preyšuje aj priemer v krajinách strednej a východnej Európy (53%) a celosvetový (39%) priemer.
  - Aj keď výsledky prieskumu naznačujú pozitívny vývoj ukazujúci, že organizácie na Slovensku sa neboja radikálne zakročiť voči interným i externým páchatelom podvodov, odporúčali by sme, aby organizácie svoje úsilie prejavili aj v oblasti prevencie. Programy „**poznaj svojich zamestnancov a obchodných partnerov**“, ktoré by mali byť aplikované ešte pred uzatvorením pracovného, respektíve obchodného vzťahu, sú jednoznačne menej nákladné, než riešenie dôsledkov podvodu.

# Počítačová kriminalita v popredí

## Čo je počítačová kriminalita?

Celosvetový prieskum hospodárskej kriminality 2011 je zameraný na finančnú kriminalitu a podvodné aspekty spojené s počítačovým zločinom. Pre účely prieskumu bol tento zločin definovaný ako:

„Počítačová kriminalita je hospodárska trestná činnosť páchaná prostredníctvom počítačov a internetu. Typickými príkladmi počítačovej kriminality sú šírenie vírusov, nelegálne sťahovanie médií, „phishing“ a „pharming“ a krádeže osobných informácií, ako napríklad údajov o bankovom účte. Nepatria sem bežné podvody, pri ktorých sa počítač využije ako vedľajší nástroj pri páchaní trestnej činnosti. Počítačová kriminalita zahŕňa len prípady, v ktorých je počítač, internet alebo použitie elektronických médií a zariadení hlavnou, nie vedľajšou zložkou činu.“<sup>1</sup>

Uvedená definícia počítačovej kriminality sa môže javiť ako dosť všeobecná, zdá sa však, že mnoho ľudí považuje túto oblasť za jav širších rozmerov, čím vytvára priestor rôznym interpretáciám. Neexistencia jednotnej celosvetovej definície počítačovej kriminality môže mať za následok to, že mnohé organizácie si nemusia plne uvedomiť jej hrozbu a ani jej možné dopady na činnosť spoločnosti. V dôsledku toho je počítačovú kriminalitu ťažšie odhaliť a bojovať proti nej.

<sup>1</sup> Definícia PwC a jej akademického partnera profesora Petra Sommera

## Počítačová kriminalita na scéne

Keď sme sa v našich predchádzajúcich prieskumoch pýtali respondentov, či sa už stretli s počítačovou kriminalitou, miera kladných odpovedí bola veľmi nízka a štatisticky nevýznamná, a preto sme zistenia súvisiace s počítačovou kriminalitou v predchádzajúcich dvoch prieskumoch zahrnuli do kategórie ‘ostatné typy podvodov’.

Vzhľadom k narastajúcim obavám z počítačovej kriminality, sme sa tento rok zamerali práve na túto oblasť. Z respondentov, ktorí sa s hospodárskou kriminalitou stretli, **každý šiesty** uviedol, že za uplynulých 12 mesiacov bol v ich spoločnosti zaznamenaný **minimálne jeden prípad počítačovej kriminality**. Počítačová kriminalita sa tak tento rok stala jedným z najčastejšie sa vyskytujúcich typov hospodárskej kriminality nielen na Slovensku (17%), ale aj v krajinách strednej a východnej Európy (18%) a na celom svete (23%).

„V dnešnom svete technológií stále viac organizácií, v snahe zlepšiť svoje výkony a zefektívniť služby zákazníkom, využíva internet, mobilné a sociálne médiá. Táto skutočnosť má však aj svoje tienisté stránky. Spoločne s používaním nových technológií sa totiž zvyšuje riziko počítačových útokov. Jasne vidíme, že počítačová kriminalita je na vzostupe. Stále častejšie sa na nás spoločnosti obracajú s prosbou, aby sme im pomohli vyšetriť to, akým spôsobom došlo k úniku citlivých informácií a kto je za to zodpovedný.“

Pavel Jankech  
Senior manažér  
Forenzné technológie

## Je počítačová kriminalita skutočne len hrozbou zvonku?

Počítačový zločin bol všeobecne vnímaný ako hrozba prichádzajúca z vonkajšieho prostredia spoločnosti. Výsledky nášho prieskumu ukazujú, že v súčasnosti **43%** respondentov na Slovensku považuje za rovnako pravdepodobné, že útok príde zvonku alebo zvnútra, v niektorých prípadoch dokonca respondenti vidia túto hrozbu ako výlučne internú. Z uvedeného vyplýva, že vnímanie počítačovej kriminality sa mení od výhradne externej hrozby na internú, a že organizácie po celom svete začínajú rozlišovať aj **interné riziká počítačovej kriminality**.

## Počítačová kriminalita je „atraktívna“:

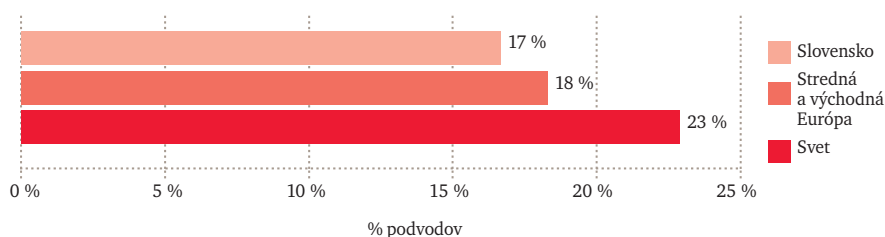
Páchateľ zvyčajne nie je prítomný na mieste činu, takže je menšia pravdepodobnosť jeho prichytenia.

Páchateľ sa môže nachádzať v inej krajine/jurisdikcii, takže možnosti vymáhania práva pri identifikovaní páchatela a jeho potrestaní môžu byť obmedzené.

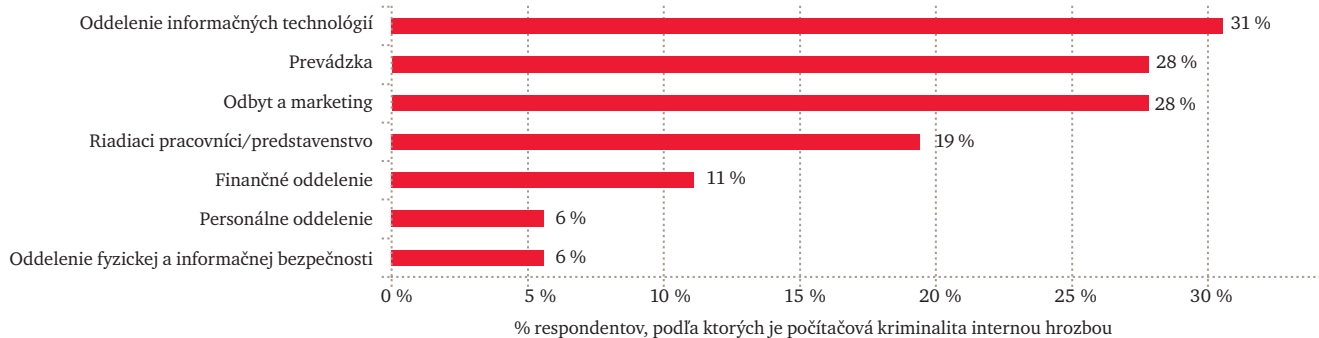
Vzhľadom na geografické, právne a politické prekážky sa páchatel môže vrátiť na „miesto činu“ bez vážnejších obáv, že dôjde k jeho odhaleniu.

Rýchly vývoj v oblasti informačných technológií komplikuje organizáciám držať krok v prevencii počítačovej kriminality.

Graf 1: Percento respondentov, ktorí sa za posledných 12 mesiacov stretli s počítačovou kriminalitou



Graf 2: Percento vnímania najpravdepodobnejšieho zdroja internej počítačovej kriminality



## Sú údaje vašej organizácie v bezpečí?

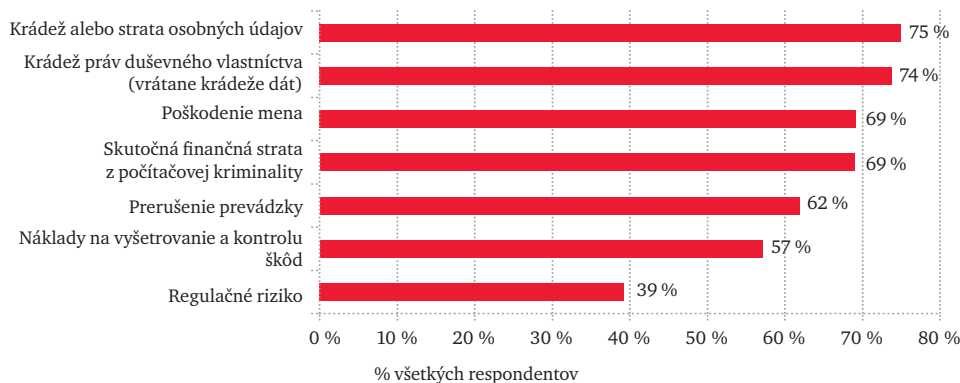
V prípade ohrozenia počítačovým zločinom sa až 75% slovenských spoločností obáva krádeže alebo straty osobných údajov. Významnou obavou spoločností na Slovensku sú aj dôsledky ako krádež práv duševného vlastníctva, poškodenie mena a skutočná finančná strata.

Vzhľadom k týmto rastúcim obavám z dôsledkov hospodárskej kriminality, najmä z poškodenia dobrého mena, je veľmi dôležité, aby spoločnosti svojím správaním demonštrovali, že patria medzi najbezpečnejšie subjekty na trhu. Takýmto správaním si nielenže posilnia svoje vlastné konkurenčné výhody, ale súčasne prispievajú k budovaniu bezpečného podnikateľského prostredia.

*„Dôležitosť oblasti počítačovej kriminality spoločnostiam nezodrazníme diskusiami o technických detailoch akými sú šifrovanie, penetračné testovanie alebo nastavenie „firewallu“. Spoločnosti by sa mali zamyslieť nad tým, čo sa môže stať s ich dobrým menom, v prípade, že dôjde k strate dôležitých údajov.“*

Filip Volavka  
Senior manažér  
Forenzné technológie

Graf 3: Obavy z dôsledkov počítačovej kriminality na Slovensku



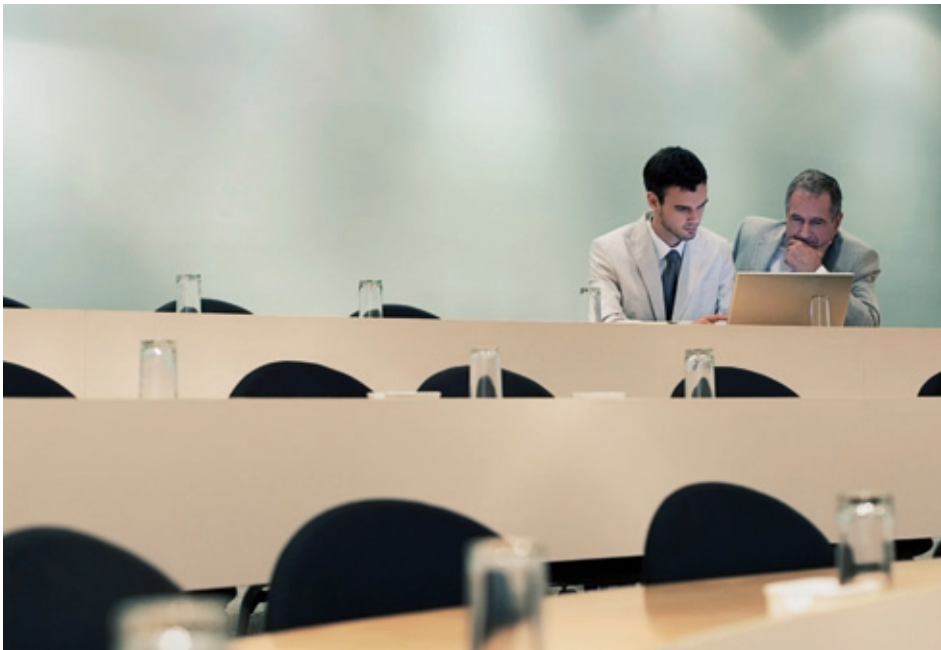
## Je vaša organizácia v ohrození?

Tak ako sme už spomínali, každý šiesty respondent, ktorí sa za uplynulých 12 mesiacov stretol s hospodárskou kriminalitou, uviedol, že išlo práve o počítačovú kriminalitu. Štvrtina respondentov si myslí, že riziko počítačovej kriminality má vzrastajúcu tendenciu a 69% zo všetkých respondentov sa v jej dôsledku veľmi alebo čiastočne obáva poškodenia mena spoločnosti. A aj napriek tomu, že organizácie si zjavne uvedomujú hroziace riziko, nepodnikajú dostatočné opatrenia v rámci prevencie, ale skôr sa zameriavajú až na reakciu.

Náš prieskum na Slovensku ukázal, že:

- 56% respondentov nedisponuje alebo nevie, či ich organizácia disponuje vlastnými prostriedkami na vyšetrovanie počítačovej kriminality;
- 87% respondentov nespolupracuje alebo nevie, či ich organizácia spolupracuje s odborníkmi v oblasti forenzných technológií;
- 52% slovenských respondentov neabsolvovalo za posledných 12 mesiacov žiadne školenie týkajúce sa počítačovej bezpečnosti; a
- 69% respondentov nemá alebo nevie, či ich organizácia má vypracovaný postup komunikácie s verejnosťou pre prípad, že by k nejakému incidentu došlo.





## Kto je v organizácii zodpovedný za riadenie rizika počítačovej kriminality?

Respondentov sme sa tiež spýtali na to, kto v organizácii by podľa nich mal byť v konečnom dôsledku zodpovedný za riadenie rizika počítačovej kriminality. Viac než polovica (51%) slovenských respondentov prisúdila hlavnú zodpovednosť riaditeľom oddelení informačných technológií. Ďalších 32% respondentov uviedlo, že podľa nich je to zodpovednosť generálneho riaditeľa a predstavenstva. Sme si vedomí toho, že riziko bezpečnosti informačných technológií je zvyčajne zodpovednosťou riaditeľa oddelenia informačných technológií, predpokladali by sme však, že generálny riaditeľ a predstavenstvo budú informovaní o skutočnostiach súvisiacich s počítačovou kriminalitou a budú ich pravidelne kontrolovať.

Nie je preto prekvapujúce, že zistenia nášho prieskumu poukazujú na skutočnosť, že ani generálny riaditeľ ani predstavenstvo nevykonávajú pravidelné hodnotenie počítačových rizík: iba 20% z nich posudzuje riziko počítačovej kriminality pravidelne, a to viackrát za rok, a 14% nepreveruje toto riziko vôbec.

Tieto čísla naznačujú, že vrcholové vedenie organizácií nekladie dostatočný dôraz na dôležitosť riadenia reálneho rizika počítačovej kriminality. Veríme, že v budúcnosti bude hlavnou charakteristikou organizácií súkromného i verejného sektora, ktoré budú skutočne rozumieť rizikám a príležitostiam počítačového sveta, práve generálny riaditeľ vnímajúci riziká a možnosti počítačového sveta.

*„Generálni riaditelia a predstavenstvo stále považujú informačnú bezpečnosť za technickú záležitosť. Ide však o mylnú predstavu, ktorú je potrebné zmeniť. Rozsah finančného rizika a rizika poškodenia mena organizácie poukazujú na to, že bezpečnosť IT by mala byť jednou z oblastí, ktoré sa riešia na úrovni predstavenstva.”*

Tomáš Kuča  
Partner  
Oddelenie riadenia rizík

### Áké kroky by mali organizácie prijať, aby sa ochránili pred počítačovými útokmi?

- 1. Zapojenie vrcholového vedenia** – generálni riaditelia a predstavenstvo musia byť informovaní o počítačových rizikách. Je dôležité, aby poznali riziká a možnosti sveta výpočtovej techniky.
- 2. Posúdenie bezpečnosti a pripravenosti organizácie pre prípad, že by došlo k počítačovému podvodu** – na rozdiel od tradičnej hospodárskej kriminality, počítačová kriminalita napreduje rýchlo a prináša stále nové riziká, čo znamená, že organizácia jej musí neustále prispôsobovať svoje postupy.
- 3. Informovanosť** – organizácia musí mať jednoznačné a jasné informácie o svojom existujúcom a vznikajúcom počítačovom prostredí. Iba v takom prípade bude spoločnosť schopná prijať dôležité rozhodnutia a opatrenia.
- 4. Vytvorenie tímu pre prípad ohrozenia počítačovej bezpečnosti** – tento tím by mal byť schopný pohotovo a rýchlo reagovať na vzniknutú situáciu. Dobre fungujúci tím znamená každý prípad počítačovej kriminality v organizácii, posúdi jeho riziká a vyrieši ho.
- 5. Vzdelávanie všetkých zamestnancov** – organizácie by v rámci rozširovania povedomia o hrozbách počítačovej kriminality mali tiež prijímať ľudí s príslušnými skúsenosťami. Títo ľudia svoje znalosti zdieľajú aj s ostatnými zamestnancami, čím vytvoria organizáciu, ktorá sa vie lepšie chrániť pred rizikom počítačových podvodov.
- 6. Aktívny a jasný postoj k počítačovej kriminalite** – spoločnosti by mali verejne komunikovať aké preventívne a reaktívne opatrenia majú k dispozícii a urobiť jasné právne kroky proti páchatelom počítačovej kriminality.

# Súčasný stav hospodárskej kriminality

## Podvod – čomu čelíme?

Z 3 877 respondentov nášho celosvetového prieskumu **34%** (1 303 respondentov) uviedlo, že za posledných 12 mesiacov boli obeťami jedného alebo viacerých prípadov hospodárskej kriminality, čo predstavuje **4% nárast** v porovnaní s rokom 2009.

Na Slovensku bola úroveň uvádzaných činov hospodárskej kriminality nižšia. Celkom **21%** všetkých slovenských respondentov uviedlo, že ich organizácia za posledných 12 mesiacov čelila hospodárskej kriminalite. Tento výsledok je v porovnaní so zisteniami štúdie z roku 2009 takmer o **8 percentných bodov nižší**. I keď sa toto zistenie na prvý pohľad javí ako pozitívna zmena naznačujúca, že hospodárska kriminalita na Slovensku ustupuje, považovali sme za dôležité pochopiť súvislosti medzi počtom odhalených podvodov a efektívnosťou systémov, ktoré organizácie na odhalenie podvodov používajú.

## Snažia sa organizácie odhaliť podvody?

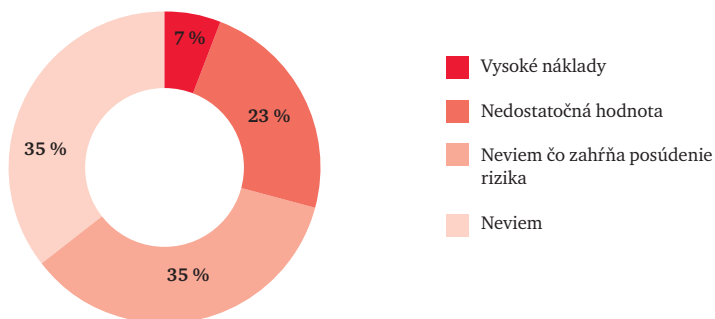
Základom úspešného boja proti podvodu je správne porozumenie možným rizikám a identifikácii prípadných medzier v systémoch spoločnosti. Jedným z najdôležitejších pomocníkov v tomto boji je práve pravidelné hodnotenie rizík podvodu.

Celosvetové výsledky potvrdili, že čím menej hodnotení rizík podvodu organizácia robí, tým menej prípadov podvodu odhalí. Platí teda známe pravidlo: „ **kto hľadá, ten nájde.**“

Takmer polovica (49%) respondentov na Slovensku uviedla, že **nehodnotí riziká podvodu alebo že nevie, či ich organizácia takú činnosť vykonáva**. Tento údaj prevyšuje celosvetový priemer (41%) a čiastočne môže vysvetľovať nízky počet uvádzaných prípadov podvodov na Slovensku.

Zároveň je znepokojujúce, že **70%** zo slovenských respondentov, ktorí nehodnotia riziká podvodov nevie, čo vlastne hodnotenie rizík podvodu zahŕňa alebo prečo sa v ich organizácii vôbec nevykonáva (Graf č. 4). Je zaujímavé, že len **7%** respondentov uvádza ako dôvod vysoké náklady.

Graf 4: Dôvody, prečo organizácie na Slovensku neuskutočňujú hodnotenie rizík podvodu



„Je nutné, aby spoločnosti pochopili výhody pravidelných hodnotení rizík podvodov a ich dôležitosť v boji proti hospodárskej kriminalite. Keďže v prípade podvodu ide o úmyselné konanie so zlým úmyslom, je zrejme, že je konané tak, aby uniklo odhaleniu. I keď manažérom, ktorí musia riešiť urgentné a kritické obchodné záležitosti, sa môže hodnotenie rizík javiť ako nevýznamná záležitosť, dobre navrhnutý a efektívny postup môže pomôcť odhaliť oblasti, kde by sa podvod mohol vyskytnúť a predpovedať správanie potenciálneho páchatela.“

Kateřina Halásek Dosedělová  
Senior manažérka  
Forenzná služba

Akým spôsobom boli teda prípady podvodu na Slovensku odhalené? Graf č. 5 ilustruje, že na Slovensku rastie význam nástrojov podnikovej kontroly pri odhaľovaní podvodov akými sú najmä: **interný audit (17%)**, **elektronické /automatizované hlásenie podozrivých transakcií (17%)** a **podniková bezpečnosť (17%)**:

## Čo je to elektronické a automatizované hlásenie podozrivých transakcií?

Elektronické a automatizované hlásenie podozrivej transakcie je bežným postupom pri odhaľovaní, vyšetrovaní a boji proti podvodom v sektore finančných služieb, kde sa používajú sofistikované nástroje na identifikovanie impulzov v systéme, ktoré napomáhajú organizácii pri vyšetrovaní podozrivých transakcií. Táto detekčná metóda je založená na elektronických automatizovaných systémoch bez nutnosti zásahu človeka. Ide snád o najefektívnejší nástroj pre využívanie v budúcnosti.

V porovnaní s rokom 2009 bolo na Slovensku výrazne menej podvodov odhalených pomocou externých alebo interných varovaní. Je prekvapujúce, že ani jeden prípad podvodu nebol odhalený prostredníctvom informačnej linky. Toto naznačuje, že slovenské spoločnosti buď nemajú zavedený tento systém, alebo ak ho majú, nefunguje efektívne:

- Slovenské spoločnosti si neuvedomujú výhody mechanizmu informačnej linky: 61% zo všetkých respondentov nemá tento mechanizmus zavedený.
- I keď si 48% respondentov, ktorých organizácie informačnú linku používajú, jej výhody uvedomuje, viac než **polovica** respondentov využívajúcich informačnú linku považuje tento nástroj za **málo alebo úplne neefektívny**.

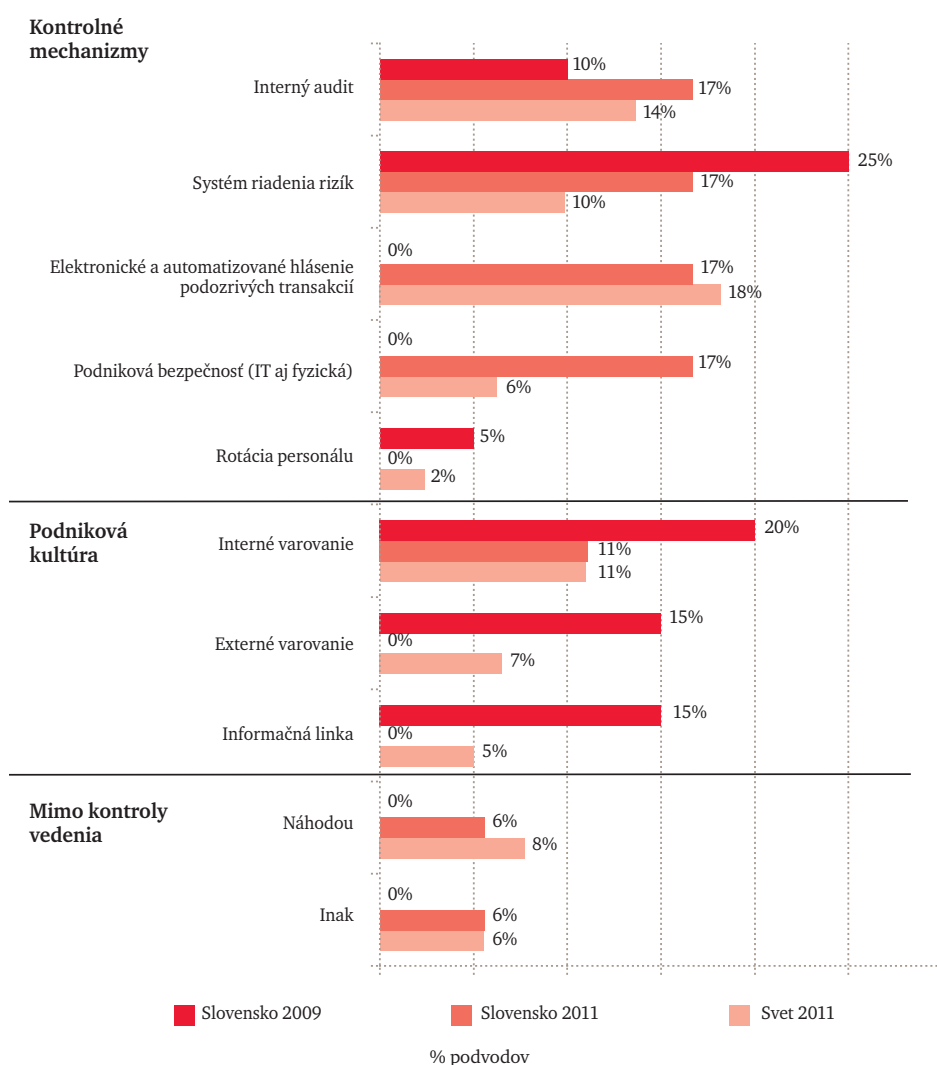
Toto zistenie je prekvapujúce, pretože v regióne strednej a východnej Európy výsledky prieskumu ilustrujú, že organizácie chápú **význam správne nastaveného systému informačnej linky**, ktorý im umožňuje lepšie nastaviť ich prístup k prevencii podvodov a korupcie. Z našich skúseností fungujúca informačná linka pomáha odhaliť podvody práve tam, kde môžu byť iné detekčné prostriedky neúčinné.

## Akým typom podvodov čelíme?

Hospodárska kriminalita sa prejavuje v rôznych formách, pričom niektoré sa vyskytujú častejšie a sú naliehavejšie než ostatné. Graf č. 6 znázorňuje rôzne typy hospodárskej kriminality, s ktorými sa respondenti na Slovensku v rámci posledných 12 mesiacov stretli:

Medzi tri najčastejšie uvádzané typy hospodárskej kriminality za posledných 12 mesiacov patrí sprenevera majetku, počítačová kriminalita a korupcia. So spreneverou majetku sa stretla prevažná väčšina respondentov na Slovensku (94%), v krajinách strednej a východnej Európy (69%) a i celosvetovo (72%).

Graf 5: Metódy odhalenia

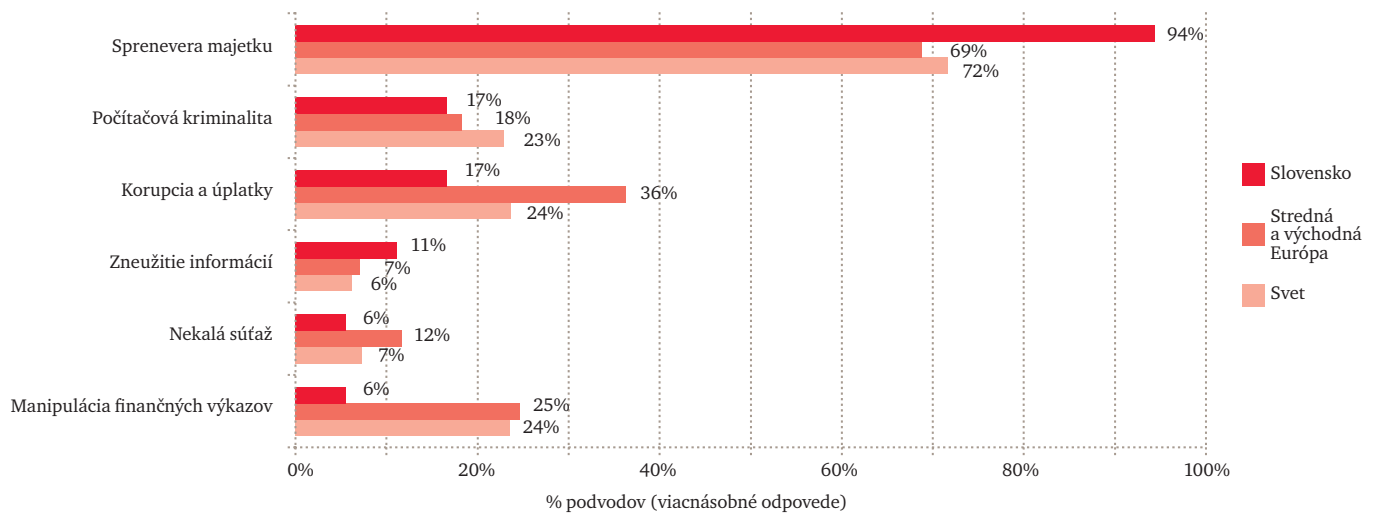


„Aby sme mohli zvýšiť efektívnosť systému informačnej linky, skôr než ho v organizácii zavedieme, musíme spoznať a správne zhodnotiť podnikovú kultúru, stanoviť ciele a spôsob komunikácie týchto cieľov a vybrať vhodné nástroje implementácie. Je takisto dôležité, aby sme mali jasný plán riešenia nahlásených prípadov podvodu a predstavu o tom, aký odkaz vyšleme ostatným zamestnancom.“

Efektívny systém informačnej linky nielenže zvýši pravdepodobnosť zabránenia podvodov, ale tiež dáva pozitívny signál obchodným partnerom a verejnosti a znižuje tak riziko poškodenia dobrého mena spoločnosti.”

Jiří Urban  
Senior manažér  
Forenzná služba

Graf 6: Typy hospodárskej kriminality



Pri porovnaní tohtoročných výsledkov s výsledkami prieskumu z roku 2009 sa výskyt sprenevery majetku výrazne zvýšil: **nárast o 49 percentných bodov na 94%**, zatiaľ čo manipulácia s účtovnými výkazmi poklesla z 45% na 6% a v rebríčku troch najčastejších typov hospodárskej kriminality ju nahradil „nováčik“: **počítačová kriminalita**<sup>2</sup> (17%).

Korupcia a úplatky **vzrástli z 10% na 17%** a na Slovensku jej výskyt dosiahol rovnakú úroveň ako počítačová kriminalita. Tento nárast nie je prekvapením. V prieskume z roku 2009 sme uviedli, že výsledok 10% je podľa nášho názoru nerealisticky nízke číslo a že predpokladaný skutočný výskyt musí byť vyšší. Porovnanie s priemerom regiónu strednej a východnej Európy **36%** v tohtoročnom prieskume poukazuje na fakt, že skutočný výskyt úplatkov a korupcie na Slovensku by mohol byť dokonca i vyšší.

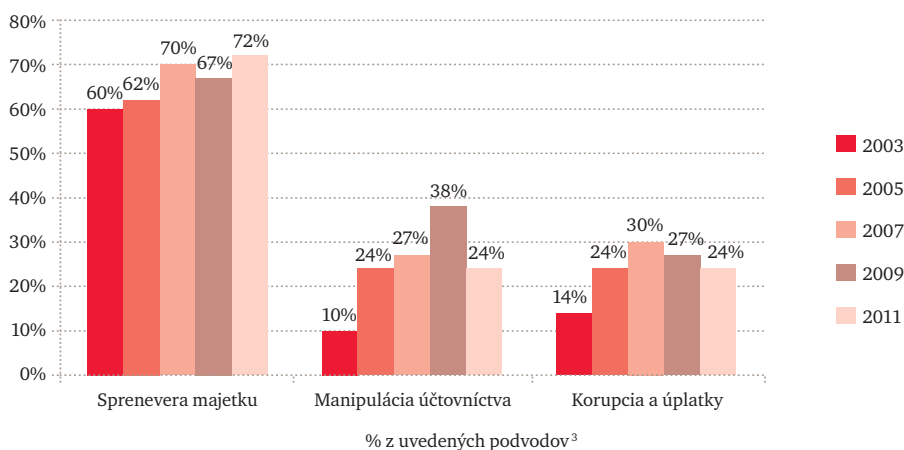
Celosvetový trend výskytu podvodov ilustruje Graf č. 7. Stále platí, že sprenevera majetku je najčastejším typom hospodárskej kriminality a v celosvetovom meradle zaznamenáva od roku 2003 nárast o **20%**.

Graf zároveň naznačuje, že **pokles prípadov manipulácie účtovných výkazov** na Slovensku je v súlade s celosvetovým trendom. Od roku 2009 poklesol výskyt tohto typu hospodárskej kriminality o **14 percentných bodov** a vrátil sa na úroveň z roku 2005.

Táto zmena môže mať viacero dôvodov. Podľa nášho názoru najvýznamnejšími faktormi, ktoré mohli tento stav ovplyvniť, sú:

1. Organizácie zaviedli prísnejšie kontroly, ktoré odrádzajú páchatela;
2. Je možné, že vrcholové vedenie organizácii už nie je pod takým tlakom ako pred dvoma rokmi, kedy organizácie bojovali o prežitie v neľahkom prostredí, a preto vedenie pocítovalo tlak pre manipulovanie účtovníctva;
3. Ďalším dôvodom pre pokles výskytu tohto typu hospodárskej kriminality od roku 2009 môže byť to, že hospodárska kriminalita nie je dôsledne odhaľovaná, a to v dôsledku celosvetového trendu znižovania počtu zamestnancov v organizáciách v posledných rokoch, čím sa mohol znížiť počet osôb zodpovedných za odhalenie a prevenciu hospodárskej kriminality; alebo
4. Ak vezmeme do úvahy zameranie tohtoročného prieskumu na počítačovú kriminalitu, mohlo sa stať, že niektorí respondenti, ktorí v minulých ročníkoch označili podvody prostredníctvom počítačov, elektronických zariadení, systémov a internetu ako účtovné podvody, ich tento rok klasifikovali ako počítačové podvody.

Graf 7: Vývoj hospodárskej kriminality v celosvetovom meradle



<sup>3</sup> V prípade rokov 2011 a 2009 sa jedná o odpovede pokrývajúce posledných 12 mesiacov, zatiaľ čo roky 2007, 2005 a 2003 zobrazujú výsledky za posledných 24 mesiacov

<sup>2</sup> Keď sme sa v našich predchádzajúcich prieskumoch pýtali respondentov, či sa už stretli s počítačovou kriminalitou, miera kladných odpovedí bola veľmi nízka a štatisticky nevýznamná, a preto sme zistenia súvisiace s počítačovou kriminalitou v predchádzajúcich dvoch prieskumoch zahrnuli do kategórie 'ostatné typy podvodov'. Vzhľadom k narastajúcim obavám z počítačovej kriminality, sme sa tento rok zamerali práve na túto oblasť.



„Keďže správne rozhodnutia idú ruka v ruke s presnými informáciami, odporúčame, aby organizácie pred nadviazaním spolupráce s obchodnými partnermi zaviedli kontrolu konfliktu záujmu ako súčasť bežných obchodných postupov. Takéto posúdenie môže pomôcť nielen pri hodnotení potenciálnych rizík súvisiacich s tretími stranami akými sú dodávatelia či sprostredkovatelia, ale aj pri vyhodnotení rizika prichádzajúceho z interného prostredia. Posúdenie konfliktu záujmu môže byť zaradené i do procesu prijímania zamestnancov, a tým poskytne cenné informácie ešte skôr, než je uchádzač prijatý. Kontrolu konfliktu záujmu odporúčame pravidelne opakovať, aby sa hodnotili aj potenciálne riziká konfliktu záujmov u terajších zamestnancov.“

Eva Krištofová  
Manažérka  
Forenzná služby

## Podvody – odkiaľ prichádza riziko?

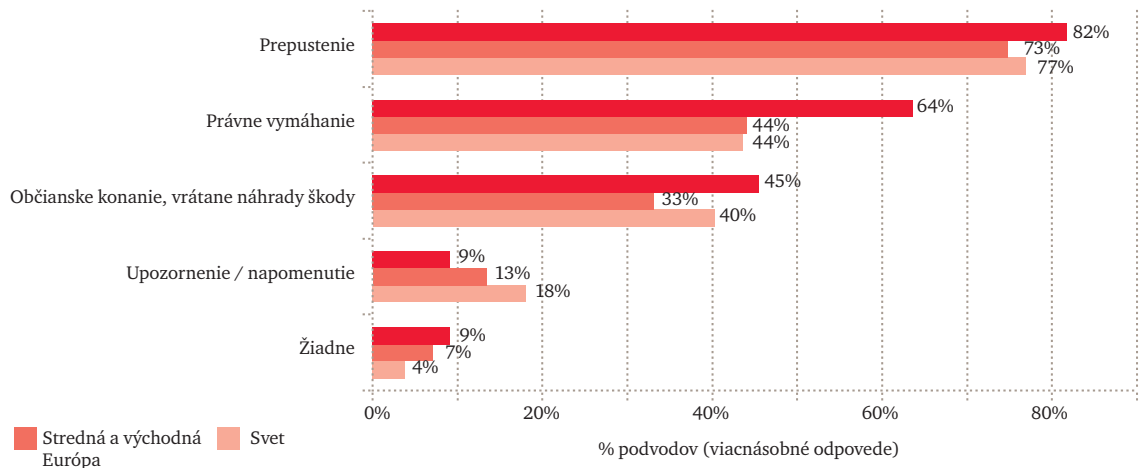
Výsledky prieskumu podporujú našu skúsenosť, že hlavná hrozba hospodárskej kriminality vychádza z radov zamestnancov. Až 61% páchatelov bolo identifikovaných ako interní páchatelia. Čo sa týka služobného zaradenia interných páchatelov, 73% respondentov na Slovensku uviedlo, že trestné činy spáchali zamestnanci na nižších pracovných pozíciách, čo značne prevyšuje priemer v krajinách strednej a východnej Európy (36%) a vo svete (39%). Toto môže byť vysvetlením pre vyššie percento výskytu sprenevery majetku na Slovensku, keďže tohto typu podvodu sa sčasti dopustia zamestnanci na nižších pozíciách.

V prípade, že došlo k odhaleniu interného páchatela, celkom 82% respondentov uviedlo, že ich organizácia **ukončila pracovný vzťah s páchatelom**, čo predstavuje prudký nárast od roku 2009 (35%) a takisto prekračuje úroveň v krajinách strednej a východnej Európy (75%) a vo svete (77%). Tento posun vnímame pozitívne, pretože naznačuje, že organizácie na Slovensku aktívne pristupujú k odhaleným podvodom a čoraz menej sú ochotné ich tolerovať.

V jednej tretine prípadov spáchali na Slovensku podvod **externé strany** – z toho **odberatelia (67%)** a **predajcovia/sprostredkovatelia (33%)**.

Podobne ako v prípade interných páchatelov, aj v tomto prípade slovenské organizácie preukázali nízku úroveň tolerancie: spolupráca bola s páchatelom ukončená v 67% prípadov, čo predstavuje nielen výrazný nárast v porovnaní s rokom 2009 (45%), ale aj v porovnaní s priemerom v regióne strednej a východnej Európy (53%) a celosvetovým priemerom (39%). I keď ide nepochybne o pozitívny znak, odporúčali by sme, aby organizácie zamerali svoju snahu aj na prevenciu. Konkrétne spoznanie zamestnancov a obchodných partnerov ešte pred uzatvorením zmluvného vzťahu je menej nákladné ako riešenie následkov podvodu.

Graf 8: Prehľad najčastejších opatrení voči interným páchatelom na Slovensku



## Podvody v budúcnosti

Tak ako v predchádzajúcich prieskumoch, aj tento rok sme sa respondentov spýtali, či si myslia, že je pravdepodobné, že ich organizácia bude musieť v nasledujúcich 12 mesiacoch čeliť niektorému z typov hospodárskej kriminality. Prieskum ukázal, že väčšina respondentov si stále myslí, že to nie je pravdepodobné.

Ďalej sme porovnali vnímanie vývoja jednotlivých typov hospodárskej kriminality v nasledujúcich 12 mesiacoch s počtom

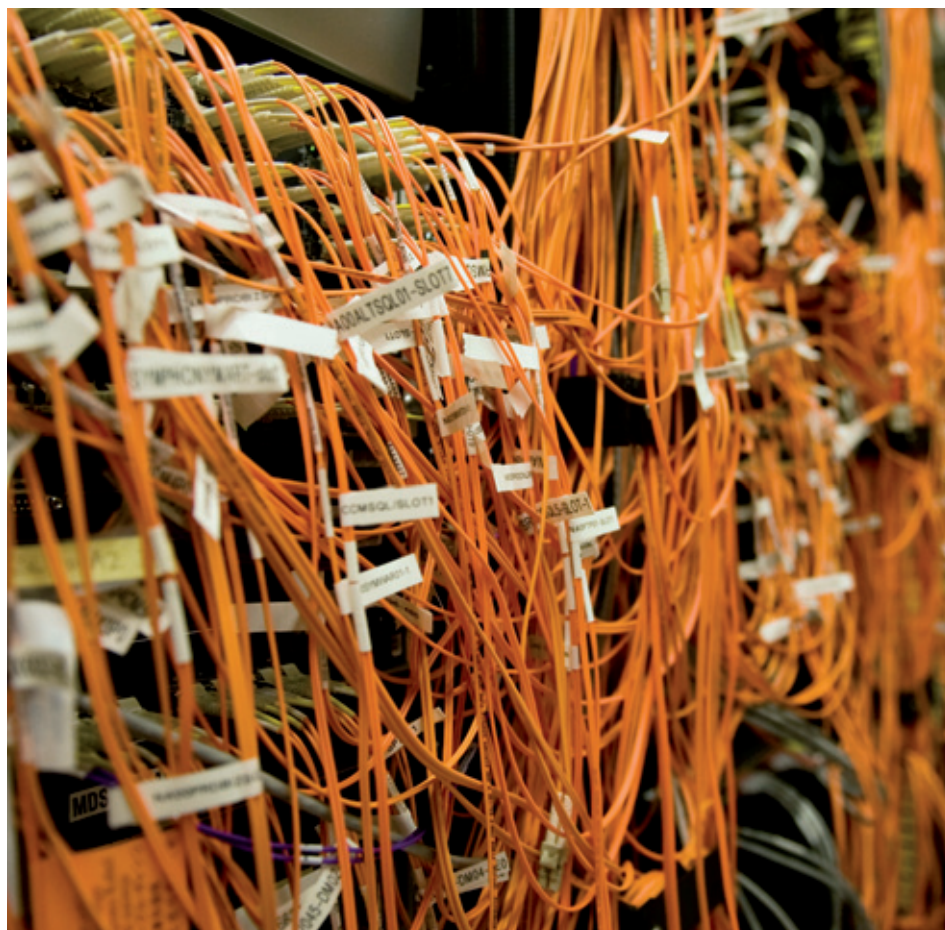
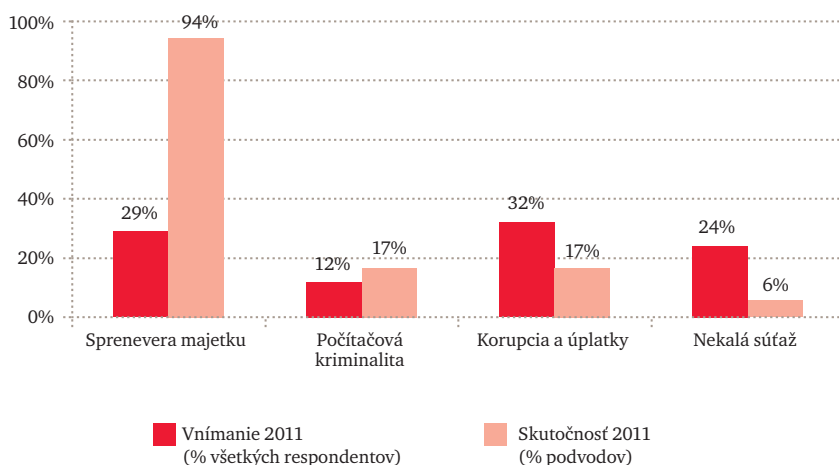
skutočne uvedených prípadov podvodu v roku 2011. Výsledky poukázali na zaujímavý nesúlad: zatiaľ čo iba 29% zo všetkých respondentov si myslí, že ich spoločnosť by sa mohla stať obeťou sprenevery majetku, skutočný výskyt tohto typu podvodu bol oveľa vyšší (94%). Na druhej strane, zatiaľ čo 17% podvodov na Slovensku sa týkalo korupcie a úplatkov, oveľa vyššie percento respondentov (32%) vníma tento typ podvodu ako potenciálny problém pre ich organizáciu.

Je zaujímavé, že 13% slovenských respondentov uviedlo konzultáciu s externým audítorom ako najpravdepodobnejší prvý krok v prípade odhalenia potenciálneho podvodu, čím Slovensko presiahlo priemer krajín strednej a východnej Európy (9%).

*„Ako audítori sme povinní posúdiť riziko podvodu a reagovať naň. Za týmto účelom hodnotíme kontrolné mechanizmy a postupy zavedené v organizáciách, počnúc nastavením vhodného prístupu na najvyššom stupni, cez efektívny etický kódex a programy pre zabezpečenie súladu s požiadavkami legislatívy až po prevádzkové kontroly a vhodné rozdelenie povinností. Najzávažnejšie prípady podvodu bývajú tie, ktorých sa dopustilo vrcholové vedenie. Ak existuje závažné podozrenie, že podvod bol spáchaný vedením, je nutné konať rýchlo, aby sa zvýšila šanca pre úspešné vyšetrovanie. Vyšetrovanie sa musí správne zorganizovať a vyšetrovatelia musia podliehať orgánom, ktoré sú v hierarchii spoločnosti na takej vysokej úrovni, o ktorej nezávislosti nie sú žiadne pochybnosti – spomínam si na prípad, kedy bol zodpovednosťou úspešne poverený predseda Komisie pre audit. Správne naplánované a vedené vyšetrovanie sa zvyčajne končí nielen potrebnými nápravnými opatreniami ale získané znalosti sa uplatňujú pri zvyšovaní informovanosti o takýchto prípadoch, posilnení kontrolných mechanizmov a postupov dodržiavania požiadaviek legislatívy.“*

Alexander Šrank  
Partner  
Audit

Graf 9: Vnímanie a skutočnosť jednotlivých typov podvodov na Slovensku



# Kontakty



---

**Sirshar Qureshi**

---

Partner  
Forenzné služby  
+420 251 151 235

---



---

**Alexander Šrank**

---

Partner  
Audit  
+421 259 350 587

---



---

**Michal Kohoutek**

---

Direktor  
Forenzné služby  
+420 251 151 231

---



---

**Pavel Jankech**

---

Senior manažér  
Forenzné technológie  
+420 251 151 336

---



---

PwC, Námestie 1. mája 18, 815 32 Bratislava  
tel.: +421 (0)2 59350 111, fax: +421 (0)2 59350 222

PwC, Hlavná 108, 040 01 Košice  
tel.: +421 (0)55 3215 311, fax: +421 (0)55 3215 322

e-mail: [meno.priezvisko@sk.pwc.com](mailto:meno.priezvisko@sk.pwc.com)  
[www.pwc.com/sk](http://www.pwc.com/sk)

Firmy PwC pomáhajú organizáciám i jednotlivcom vytvárať tú hodnotu, ktorú hľadajú. Sme sieťou firiem v 158 krajinách s takmer 169 000 pracovníkmi, ktorí robia všetko pre to, aby poskytovali kvalitné auditorské, daňové a poradenské služby. Viac sa dozviete na našej webovej stránke [www.pwc.com/sk](http://www.pwc.com/sk).

© 2011 PricewaterhouseCoopers Slovensko. Všetky práva vyhradené. Názov "PwC" v tomto dokumente označuje spoločnosť PricewaterhouseCoopers Slovensko, s.r.o., ktorá je členom siete firiem PricewaterhouseCoopers International Limited, z ktorých každá je samostatným a nezávislým právnym subjektom.