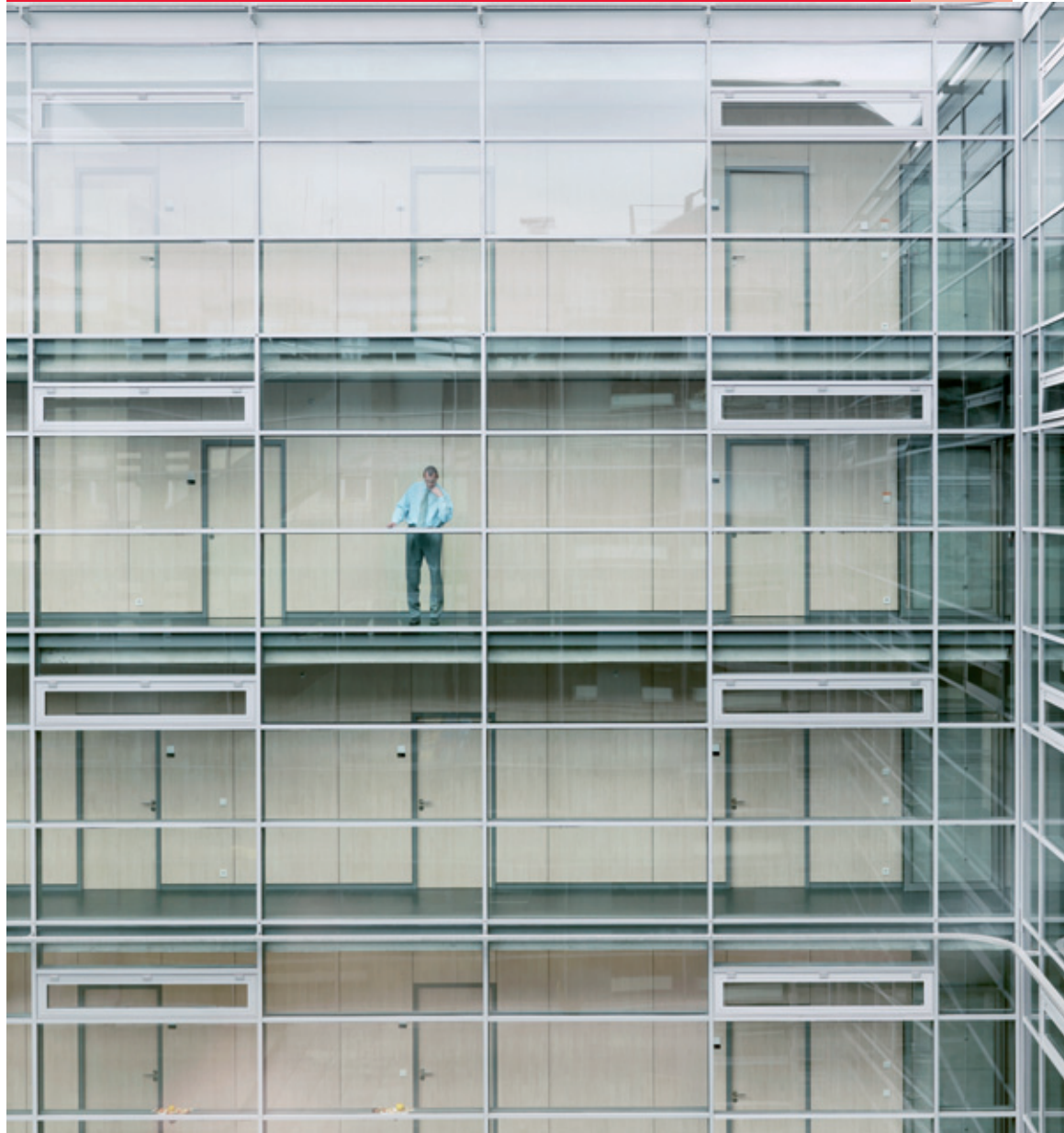


# *The Global Economic Crime Survey 2011 Slovakia*

Cybercrime in the spotlight

*Nearly 4,000 organisations  
in 78 countries help provide  
a global picture of fraud  
and other crimes*

*December 2011*



# Introduction

We are pleased to present the results of the **2011 PwC Global Economic Crime Survey**. With **3,877** respondents from across **78 countries**, including 84 leading organisations within Slovakia, this study continues to be the largest of its kind available worldwide. We trust that our survey will provide Slovak business leaders and corporate executives with an unparalleled insight into the perceptions, awareness and impact of economic crime on businesses around the world. Economic crime doesn't discriminate. It affects organisations all over the world. And no industry or organisation is immune. The fallout isn't just the direct cost; economic crime can seriously damage brands or tarnish a reputation, leading organisations to lose market share. As society becomes less tolerant of unethical behaviour, businesses need to ensure they're building – and keeping – public trust.

Our sixth Global Economic Crime Survey, in which Slovakia participates for the third time, **turns the spotlight on the growing threat of cybercrime**. Today, most people and businesses rely on the internet and other technologies. So they're potentially opening themselves up to attacks from criminals anywhere in the world. Against a backdrop of data losses and theft, computer viruses and hacking, our survey looks at the significance and impact of this new type of economic crime and how it affects businesses worldwide.

We asked a number of questions specifically relating to cybercrime, the threats posed by cybercrime and how organisations try to counter any cybercrime attacks. And, to help us spot long-term trends, we asked several 'core' questions on economic crime in general, so we could compare this year's data with previous surveys.

Accordingly, this year's report is divided into two sections:

- Cybercrime – its impact on organisations, their awareness of the crime and what they are doing to combat the risks; and
- Fraud, the fraudster and the defrauded – focussing on the type of frauds committed, and how they are detected, who is committing them and what the repercussions are.

**Sirshar Qureshi**  
Forensic Services Partner for the  
Czech Republic and Slovakia

**Michal Kohoutek**  
Forensic Services Director, PwC

# Highlights

## Cybercrime

- While being statistically insignificant in the past, **cybercrime** has emerged as one of the **top three** reported types of economic crime in Slovakia (17%); across Central & Eastern Europe (“CEE”) (18%) and globally (23%). Yet **only 12%** of Slovak organisations believe their organisation **will likely face cybercrime** in the following 12 months, which is considerably less than compared to CEE (22%) and Global (26%).
- Slovak organisations are increasingly aware of the risk of cybercrime. **95% of respondents** stated that their perception of the risk of cybercrime has either increased or remained the same over the last year. This is despite the fact that **more than half** of the respondents in Slovakia **hadn’t had any cyber security training** in the past 12 months.
- **Theft or loss of personal identifiable information**, together with **intellectual property theft (including theft of data)** and **reputational damage** causes the biggest concerns to Slovak organisations when it comes to the effects of cybercrime.
- The cybercrime threat is no longer seen primarily as an external one: **43%** of respondents now see cybercrime as both an external and internal threat, or even just an internal one. The **Information Technology department** is perceived as the most likely source of cybercrime threat internally; this is consistent in Slovakia, and in CEE as well as globally.
- **Nearly 70%** of all respondents reported that they have **in-house capabilities to prevent and detect** cybercrime and **44%** also believe they have the capabilities to investigate cybercrime internally. Presumably, these capabilities often reside with Information Technology Departments – the department seen as the biggest internal threat for cybercrime. It is, therefore, alarming that only **13%** of respondents said they had access to forensic technology investigators.

- **Only 20%** of Slovak organisations **review cybercrime threats regularly on a more frequent than annual basis**. While this is consistent with their CEE and global counterparts, it might not be frequent enough to keep up with the fast speed of the development of technology and IT threats.

## Fraud, the fraudster and the defrauded

- Economic crime continues to be a serious issue affecting organisations worldwide, across CEE and also in Slovakia. **21%** of organisations in Slovakia experienced one or more economic crimes in the past 12 months; less than the average for CEE (30%) and globally (34%).
- The results of our survey indicate, however, that it is possible that mechanisms implemented by Slovak organisations to detect fraud may either be insufficient or ineffective and, therefore, a large part of incidents of economic crime could remain undetected:
  - There is a correlation between how often fraud risk assessments are performed and how many frauds are reported. **49%** of all Slovak respondents said they did not perform a fraud risk assessment, or did not know if their organisation had performed one. Since this is higher than globally (41%), it may explain the low number of reported fraud incidents in Slovakia. It is troubling that **70%** of those respondents not performing fraud risk assessment do not know what a fraud risk assessment involves, or why their organisation does not perform it.
  - We have also noted that **61%** of Slovak organisations **do not employ a whistle-blowing mechanism**. Moreover, from those respondents whose organisation uses a whistle-blowing system, over a **half** of respondents consider this system to be only slightly effective or not effective at all. In our experience an effective whistle-blowing mechanism helps to discover fraud in many cases in which other means of fraud detection might be ineffective.

- The top three economic crimes were **asset misappropriation, cybercrime and bribery and corruption**. Asset misappropriation remains the crime reported by most respondents of those who experienced fraud in Slovakia (**94%**), and it also prevails in CEE (69%) and globally (72%). Compared to the 2009 Survey results, this represents a significant **increase by 49% points** in Slovakia.
- **Bribery and corruption** reported in Slovakia **increased by 7% points** since 2009 to **17%** and was at the same level as cybercrime. Comparison to the CEE average of 36% indicates, however, that the actual incidence of bribery and corruption in Slovakia might be even higher, but that it went undetected.
- The main threat of economic crime in the last 12 months **came internally from employees (2011: 61%; 2009: 30%)**. Junior staff members in Slovakia perpetrated **73%** of internal frauds, which is considerably higher than across CEE (36%) and globally (39%). In the case of internal perpetrators, dismissal was the most frequent action taken in Slovakia, in **82%** of cases.
- External parties to the organisation played a role in a third of fraud cases in Slovakia – with **customers (67%) and agents/intermediaries (33%) being the external perpetrators**. In Slovakia, the business relationship was terminated with external perpetrators in **67%** of cases, which not only represents an increase from **45%** in 2009, but is also above the CEE (53%) and the global (39%) average.
- These results indicate a relatively low level of tolerance to both internal as well as external fraudsters in Slovak organisations. Whilst this is definitely a positive sign, we would recommend that organisations also step-up their efforts on a prevention front: **knowing your employees and your business partners** prior to engaging with them is less costly than dealing with the consequences of fraud.

# Cybercrime in the spotlight

## What is cybercrime?

GECS 2011 focussed on the financial crime and fraud aspect of cybercrime and for the purposes of our survey questionnaire, cybercrime was formally defined as follows:

*“Cybercrime, also known as computer crime, is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one”.<sup>1</sup>*

The above definition may be considered a fairly common definition of cybercrime, yet it would appear that many perceive this as a wider phenomenon which makes the definition open to different interpretations. There is no standard globally accepted definition of cybercrime available, and the implications of not having a clear-cut definition could be that if organisations are not aware of what the dangers are, where the dangers come from and how cybercrime can impact on their business, then it is the harder to detect and combat cybercrime.

<sup>1</sup> As defined in GECS 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer.

## Cybercrime enters the frame

In our previous economic crime surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. Hence, we combined the results with ‘other types of fraud’ in our past survey reports.

Given the increasing concerns around cybercrime, we focussed on it this year. Of those respondents who indicated that they had experienced economic crime, **every sixth** stated that they were subject to **one or more cybercrime incidents** in the past 12 months. As such, cybercrime has emerged as one of the top types of economic crime in Slovakia (17%); CEE (18%) and globally (23%).

*“In today's technology world, more and more organisations are using web, mobile and social media platforms to improve their performance and serve customers more effectively. There is a dark side as well. As usage of new technologies increases, so do the scale and sophistication of cyber attacks. We clearly observe cybercrime to be on the increase in the current marketplace, in the multiple cases we helped organisations to investigate how sensitive information leaked and who was responsible for that. “*

Pavel Jankech  
Senior Manager  
Forensic Technology Solutions

## Is it really an external threat to organisations?

Since the rise of the internet, cybercrime has generally been perceived as an external threat. In Slovakia, **43%** of respondents now see cybercrime as both an external and internal threat, or even just an internal one. This suggests that the perception of cybercrime is changing from being an exclusively external threat to an internal one, and organisations are now recognising the **internal risks of cybercrime**.

## Cybercrime is “attractive”:

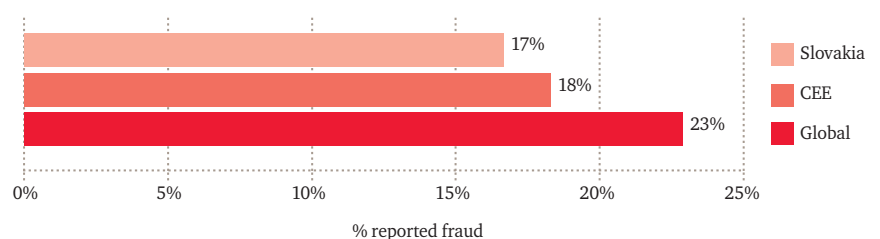
The fraudster is usually not present at the location of the crime, so there is less chance of getting caught.

The fraudster may be located in a different country/jurisdiction, there is then less chance of law enforcement identifying the perpetrator and punishing him.

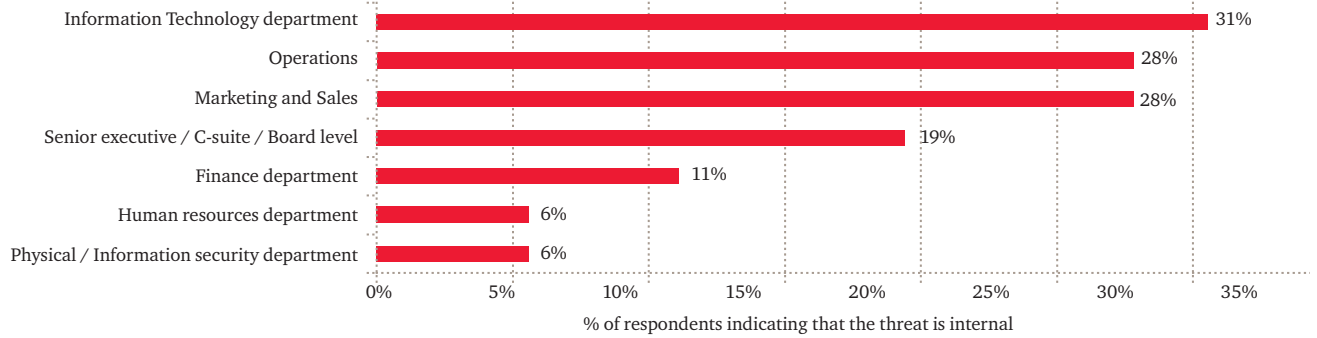
Due to lack of geographic control, law enforcement, political obstacles the perpetrator can return to the “scene of crime” with minimal fear of detection.

Rapid change in technology makes it difficult for organisations to keep up with the prevention of cybercrime.

Chart 1: Percentage of respondents having experienced cybercrime within the last 12 months



**Chart 2: Perception of most likely sources of internal cybercrime threat**



## Is your organisation's data safe?

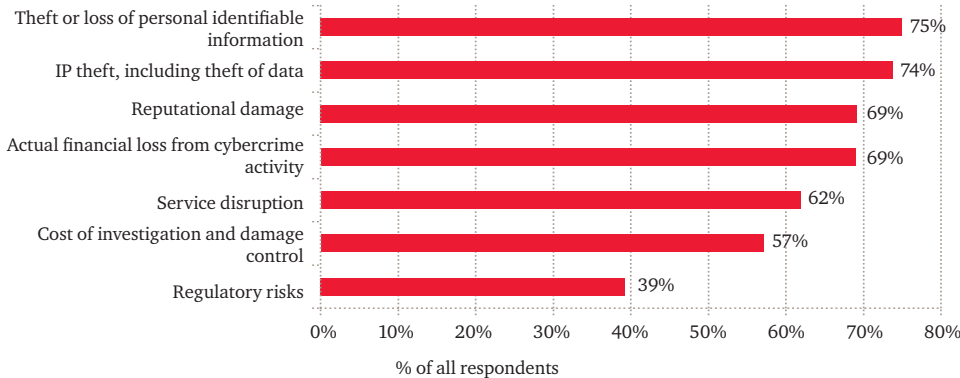
Our survey investigated the concerns respondents have about the effects of cybercrime activity on their organisation, and 75% of respondents see theft or loss of personal data as having a significant impact. Other high-ranking risks were Intellectual Property theft, reputational damage and actual financial loss.

Due to the great concerns organisations have, particularly around reputational damage, it is very important for them to demonstrate that the security is important to them and that they are a secure business. It becomes critical for organisations to market a safe and secure operational environment.

*“The way to get the business thinking about cybercrime is to talk about risk and not about encryption, penetration testing or firewall setting. Let them think about what can happen to the reputation of the firm if some critical business data is lost.”*

Filip Volavka  
Senior Manager  
Forensic Technology Solutions

**Chart 3: Concerns around effects of cybercrime in Slovakia**

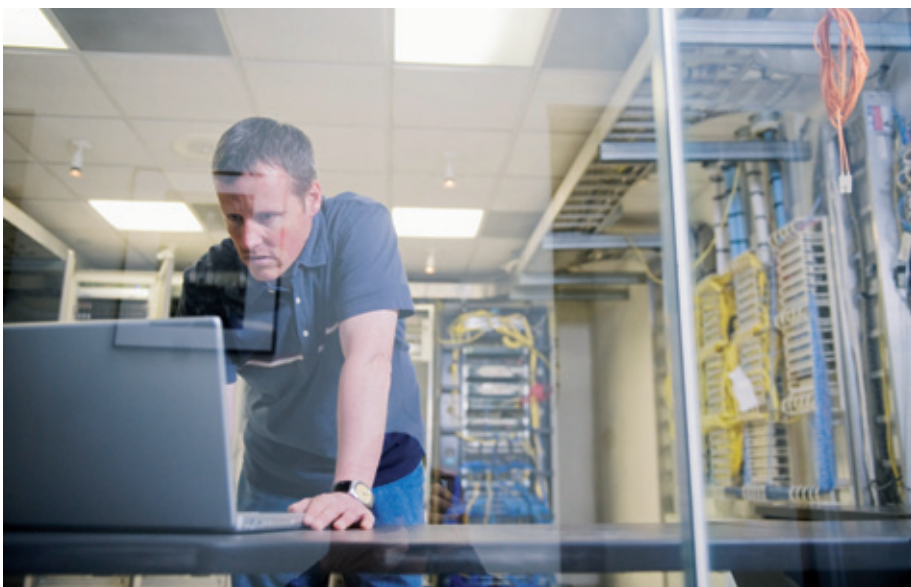


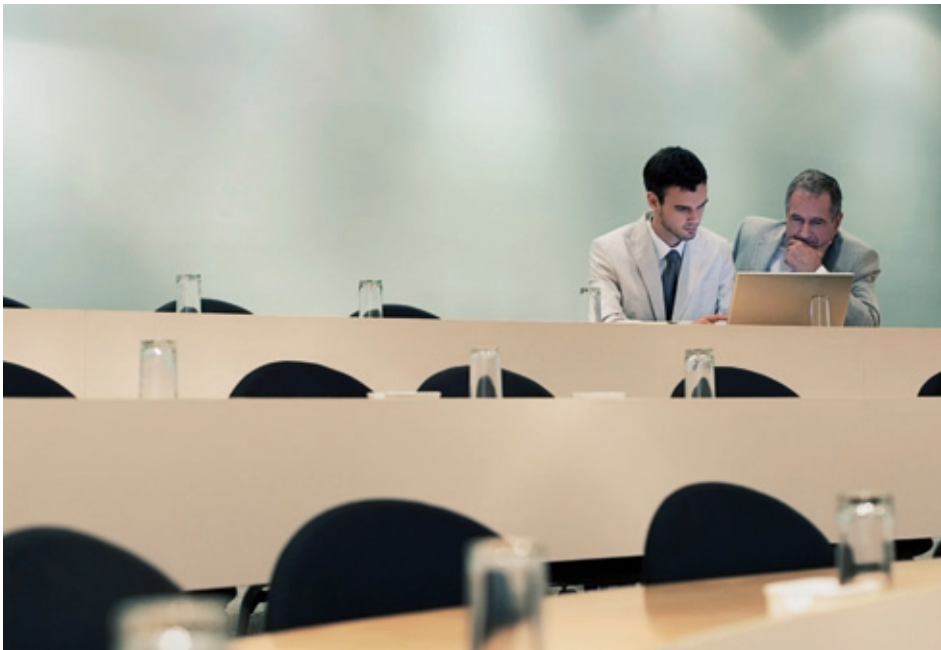
## Is your organisation like a deer in the headlights?

Every sixth of those respondents who experienced economic crime in the past 12 months, reported to have suffered cybercrime. A fourth of all respondents said they perceive the risk of cybercrime to be growing, and 69% of all respondents are very or quite concerned about the reputational damage caused by this type of economic crime. However, whilst being aware of the risks, organisations are doing little about it and seem to be reactive rather than proactive in fighting cybercrime.

Our survey shows that in Slovakia:

- 56% said their organisation does not have the in-house capability to investigate cybercrime, or they are not aware of it;
- 87% said their organisation does not have access to forensic technology investigators, or they are not aware of it;
- 52% of Slovak respondents have received no cyber security training in the past 12 months; and
- 69% said their organisation does not have a media and public relations plan in place, or they are not aware whether their organisation has.





## Who is ultimately responsible for dealing with cybercrime inside an organisation?

We asked organisations who should ultimately be responsible for dealing with cybercrime risks within their organisation. According to the results, 51% of Slovak respondents named the Chief Information Officer (“CIO”), with 32% stating that the ultimate responsibility resides with the Chief Executive Officer (“CEO”) and the board. Whilst we understand that the Information Technology security risk is usually the responsibility of the CIO, we would expect the CEO and the board to understand and probe into cybercrime risk related matters on a regular basis.

It is, therefore, not surprising that, according to our survey, the CEO and the board do not perform routine reviews of the risks that cybercrime presents to their organisations: **only 20%** of them review cybercrime threats regularly on a more frequent than annual basis and **14%** do not review cybercrime threats at all.

The statistics indicate that the most senior people within organisations are not placing enough emphasis on the importance of managing the real threats that cybercrime present to their organisation. In the future, we believe that leadership by a CEO who truly understands the risks and opportunities of the cyber world will be a defining characteristic of those organisations – whether public or private sector – that realise the real threats and manage the risks most effectively.

*“CEOs and boards are still regarding information security as a technology issue. This is a perception that needs to be changed. The scale of the financial and reputational risks to a business means that information security should be one of the key board-level risk issues.”*

Tomáš Kuča  
Risk Assurance Partner for the  
Czech Republic and Slovakia

## What actions should organisations take to defend themselves against cyber security attacks?

1. **Get the CEO involved** – the CEO and the board needs to be aware of cyber threats. They need to understand the risks and opportunities of the cyber world.
2. **Reassess the security function and preparedness** of the organisation should a cybercrime occur – unlike traditional ‘economic crimes’, cybercrime is fast paced with new risks emerging which means an organisation needs to adapt its procedures continually in order to reflect this.
3. **Awareness** – organisations need to have a clear awareness of their current and emerging cyber environment. If this is in place, well informed and prioritised decisions and actions can be taken.
4. **Create a cyber incident response team** – which needs to act with speed and agility. A well functioning cyber response team means that an incident spotted anywhere in the business will be tracked, risk assessed and escalated.
5. **Educating all employees** – an organisation needs to embed a ‘cyber awareness’ culture, through recruiting those with the relevant skills so that this knowledge can be shared with all employees creating a cyber aware organisation which is better able to protect itself.
6. **Take a more active and transparent stance towards cybercrime** – take action by pursuing cybercrime perpetrators through legal means, and communicate more publicly regarding the actions the organisation is taking regarding the threats, incidents and responses.

# Fraud, the fraudster and the defrauded

## Fraud – what are we facing?

Globally, of the 3,877 respondents to our survey, 34% (1,303 respondents) reported having been a victim to one or more economic crimes in the past 12 months, a **4% point increase** on the results in 2009.

In Slovakia, the level of reported economic crime was lower with **21%** of all Slovak respondents reporting that their organisation faced economic crime within the last 12 months; **8% point decrease** compared to the results in 2009. Although this result looks like a positive development at first sight, indicating that economic crime is on the retreat in Slovakia, we found it necessary to understand the context of fraud occurrences and the effectiveness of the systems organisations use to detect fraud.

## Fraud – are organisations detecting fraud and how?

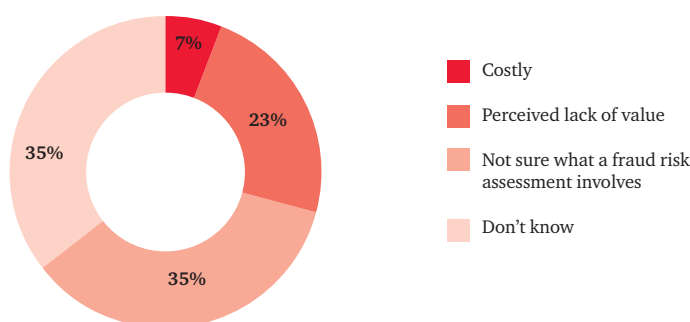
The best way to fight fraud is to know how to assess and identify the risks. Organisations can establish this by doing regular fraud risk assessments. Global results show a clear correlation between how often these assessments are done and how many incidents of fraud are reported.

The global results demonstrate that the fewer fraud risk assessments organisations carry out, the less fraud they are likely to detect. For example, globally, more than three-quarters of those organisations that said they do not perform any assessments reported less than ten incidents of fraud. These figures, then, confirm the dictum of “**seek and you shall find**”.

49% of respondents in Slovakia said they **do not perform fraud risk assessments or did not know if their organisation does**. This is higher compared to global results (41%) and so may partly explain the lower number of reported fraud incidents in Slovakia.

It is troubling, as illustrated in Chart 4, that **70%** of Slovak respondents not performing fraud risk assessments do not know what a fraud risk assessment involves or why it was not being performed. Interestingly, cost was listed as a reason in only 7% of responses.

Chart 4: Reasons for not performing fraud risk assessments in Slovakia



*“Organisations need to understand the benefits of doing regular fraud risk assessments and how important they are in the fight against fraud. As fraud from its essence entails intentional misconduct, it is designed to evade its detection. Conducting a fraud risk assessment might seem to be an activity of low importance to busy managers, who must deal with many urgent and critical business issues. However, a well designed and properly conducted fraud risk assessment is an effective tool for combating fraud. It should identify where fraud may occur and if the internal controls are set up properly to prevent fraudulent behaviour.”*

Kateřina Halásek Dosedřlová  
Senior Manager  
Forensic Services



So how were the incidents of economic crime actually detected in Slovakia? As illustrated in Chart 5, Slovak results confirmed the increasing importance of corporate control tools such as **internal audit (17%)**, **electronic/automated suspicious transaction reporting (17%)** and **corporate security (17%)** in detecting fraud.

## What is Electronic and automated suspicious transaction reporting?

Electronic and automated suspicious transaction reporting is normally used to detect, investigate and fight fraud in the financial services sector where highly sophisticated tools are used to identify triggers within the system to help enable the organisation to investigate suspicious transactions. This detection method is based on an electronic automated system without human intervention. Perhaps the most effective tool for the future.

Significantly less fraud was detected via external or internal tip-offs compared to our 2009 Slovak results. Surprisingly, no incident of fraud was reported to be detected by a whistle-blowing system in Slovakia in 2011. This indicates that Slovak organisations either do not employ a whistle-blowing mechanism or, if they do, the mechanism may not be working effectively:

- Slovak organisations do not perceive the benefits of a whistle-blowing system: **61%** of all respondents in Slovakia did not employ a whistle-blowing mechanism.
- Although **48%** of respondents using a whistle-blowing system recognised its benefits for their organisation, still more than **half** of respondents considered this system to be **only slightly or not effective at all**.

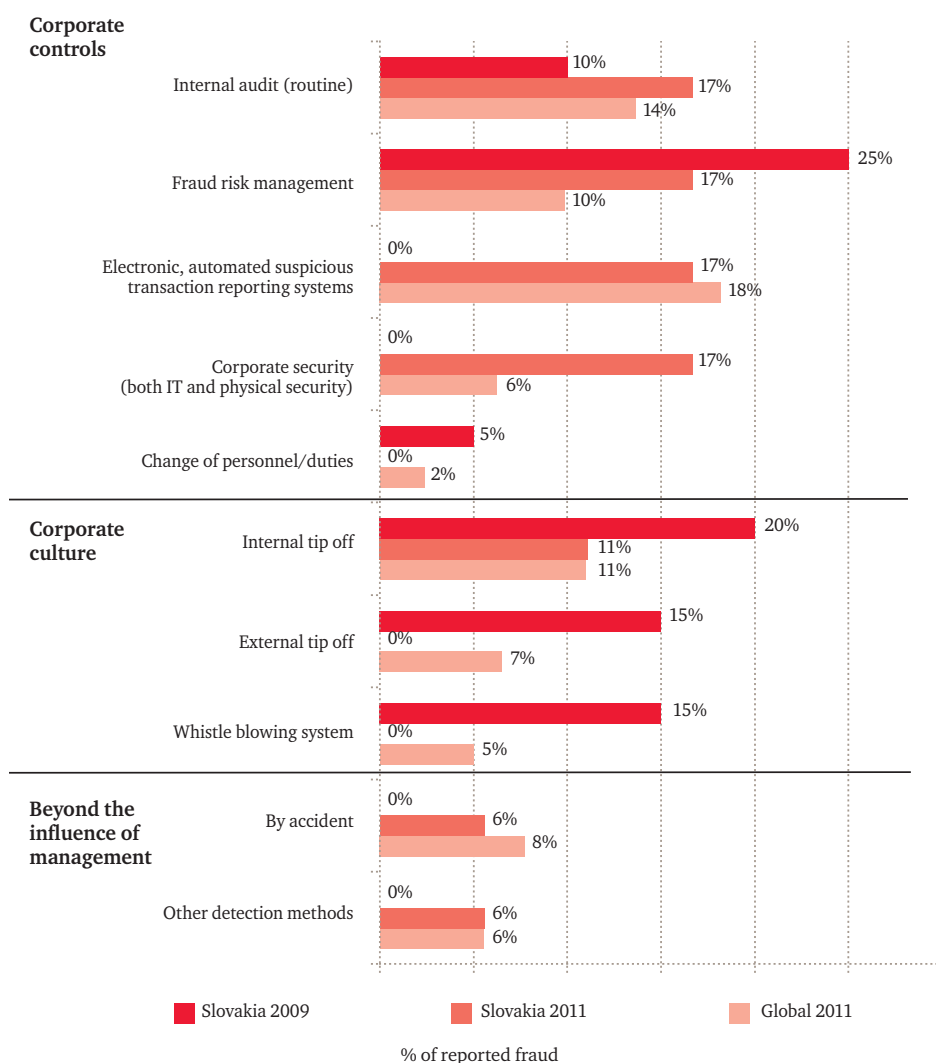
This is surprising as organisations in CEE seem to recognise the **importance of a well designed whistle-blowing system** which provides the organisation with a more structured approach to the prevention of fraud and corruption. In our experience, an effective whistle-blowing mechanism helps to discover fraud in many cases when other means of fraud detection prove ineffective.

## What types of fraud are we facing?

Economic crime can take on many different forms, with some being more common and persistent than others. Chart 6 shows the different types of economic crime as experienced by Slovak respondents who reported to have been subject to economic crimes over the past 12 months.

The 3 types of economic crimes reported by the most respondents in the past 12 months were asset misappropriation, cybercrime and bribery and corruption. Asset misappropriation continues to be reported by the most respondents in Slovakia (**94%**), CEE (**69%**) and globally (**72%**).

Chart 5: Detection methods

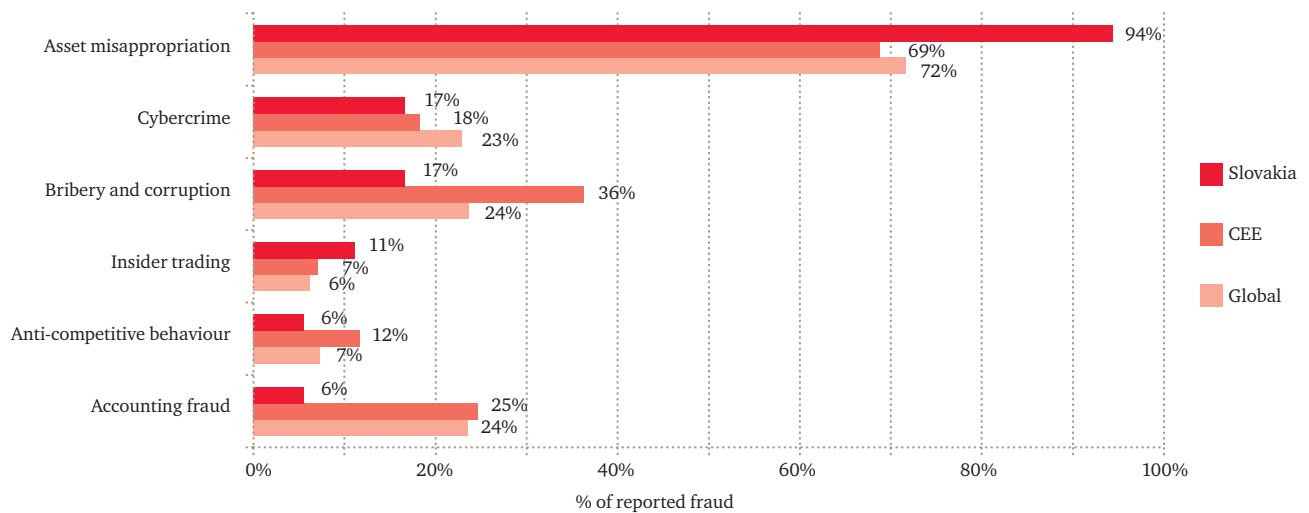


*“In order to increase the effectiveness of a whistle-blowing system, there are a couple of critical steps to be done preceding its implementation such as understanding and correctly evaluating corporate culture, setting the targets and their communication, selecting appropriate instruments to be used. It is also important to have a clear plan of how the announced incidents will be solved and what messages will be sent to the other employees.”*

*An effective whistle-blowing system not only increases the likelihood of preventing wrongdoing and criminal behaviour, it also sends a positive signal towards business partners and the public at large and reduces the risk of a negative reputation.”*

Jiří Urban  
Senior manager  
Forensic Services

Chart 6: Types of economic crimes



When compared to the results of the 2009 survey, asset misappropriation has significantly **increased by 49% points to 94%**, whereas accounting fraud has dropped **from 45% to 6%** and in the 3 most reported crimes was replaced by a **'new kid on the block': cybercrime<sup>2</sup> (17%)**.

Bribery and Corruption **increased from 10% to 17%** and was reported by Slovak respondents at the same level as cybercrime. The increase comes as no surprise. In our 2009 Slovak supplement we did point out that 10% appeared to be unrealistically low and that we expected actual incidents to be higher. A comparison with the 2011 CEE average of **36%** indicates that the actual incidence of bribery and corruption in Slovakia might be even higher.

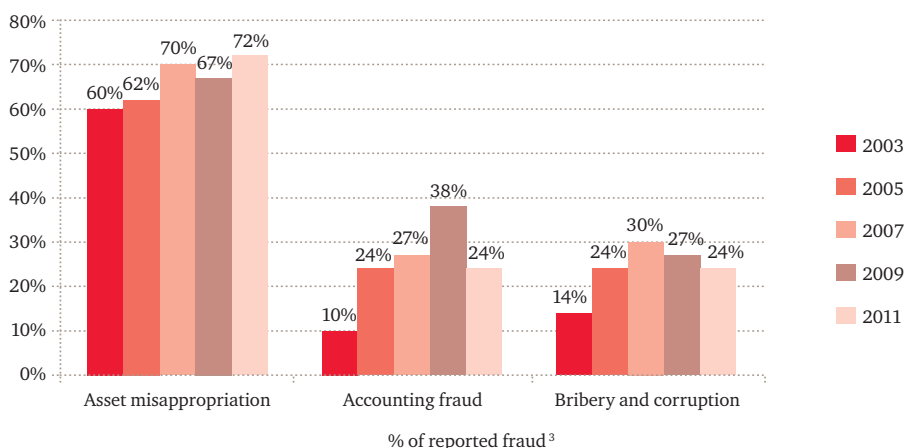
Global trends in reported fraud are illustrated in Chart 7. One of the facts that stands out is that asset misappropriation has not only been the most common type of economic crime, it has also shown an increase over the years; globally a rise of **20%** since 2003.

Chart 7 also indicates that the **decrease in accounting fraud** in Slovakia is in line with global development, as since 2009 this type of economic crime has fallen globally by **14% points** and has returned to the levels experienced in 2005.

There could be various reasons for this change but some of the factors that we think could have had an impact on this change are:

1. Organisations may have put tighter controls in place, which deter the perpetrator;
2. There is a possibility that the senior management in organisations no longer feels similar pressures to two years ago when organisations struggled to survive in difficult times and, therefore, management felt the pressure to commit financial statement manipulations;
3. Another possible reason for the drop in accounting frauds since 2009 could be due to the fact that economic crime is not being detected accurately due to the reductions in headcount within organisations globally over the past couple of years, causing fewer resources available within departments responsible for detecting and preventing economic crime; or
4. Given the focus of our survey on cybercrime this year, it is possible that some of the respondents who used to classify accounting frauds involving use of computers, electronic devices, systems, and internet may have reclassified it as cybercrime this year.

Chart 7: Trends in reported fraud globally



<sup>3</sup> % respondents who experienced economic crimes in the past 12 months for 2011 and 2009; and in the last 2 years for 2007 and 2005

<sup>2</sup> In our previous economic crime surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. Hence, we combined the results with 'other types of fraud' in our past survey reports. Given the increasing concerns around cybercrime, we focussed on cybercrime this year.



*“As a confident choice goes hand in hand with precise information, it is recommended that organisations implement background checks into their normal business procedures. Background checks cannot only help organisations to assess potential risks coming from external parties such as vendors and intermediaries, but also to assess the risks coming internally. Background checks can be implemented into the organisation’s hiring process thus providing valuable information prior to the individual being hired, and can also be performed regularly in order to assess any potential conflicts of interest that current employees could have.”*

Eva Krištofová  
 Manager  
 Forensic Services

## Fraud – where does the risk come from?

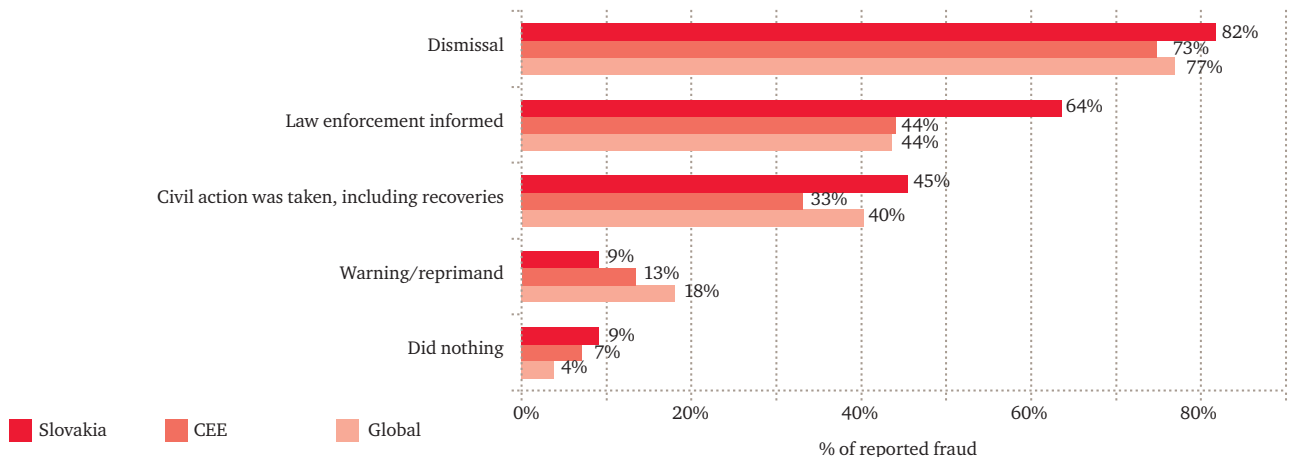
The results of our survey support our experience that the main threat of economic crime is perpetrated by the employees, as 61% of reported perpetrators were identified as **internal perpetrators**. In terms of the seniority of the internal perpetrators, 73% of respondents in Slovakia answered that the crime was committed by junior staff members, which is well above the CEE (36%) and global (39%) averages. This may explain the higher percentage of asset misappropriation in Slovakia as this type of fraud is often committed by junior employees.

In respect of internal perpetrators, in 82% of reported internal fraud cases the perpetrator was **dismissed** by the organisation which not only shows a steep increase since 2009 (35%) but also exceeds CEE (75%) and global (77%) results. We perceive this as a positive trend as it implies that organisations in Slovakia actively deal with the identified fraud and are increasingly less willing to tolerate it.

**External parties to the organisation** played a role in a **third of fraud cases** in Slovakia – with **customers (67%)** and **agents/intermediaries (33%)** being the perpetrators.

Similarly as with internal fraudsters, Slovak organisations showed a low level of tolerance: the business relationship was terminated in 67% of cases of external perpetrators which not only represents an increase from 45% in 2009, but is also well above CEE (53%) and global average (39%). While this surely is a positive sign, we would recommend that organisations step-up their efforts on the prevention front also: knowing your employees and your business partners prior to engaging with them is less costly than dealing with the consequences of fraud.

Chart 8: Overview of most frequent actions taken against the internal perpetrator in Slovakia



## Fraud in the Future

As in our previous surveys, we asked respondents to provide their perception regarding the likelihood that their organisation will be subject to various types of fraud within next 12 months, and our survey shows that the majority of them still think it is unlikely.

We further compared the respondents' perception of development in the next 12 months with the type of actually reported fraud in 2011. The results show an

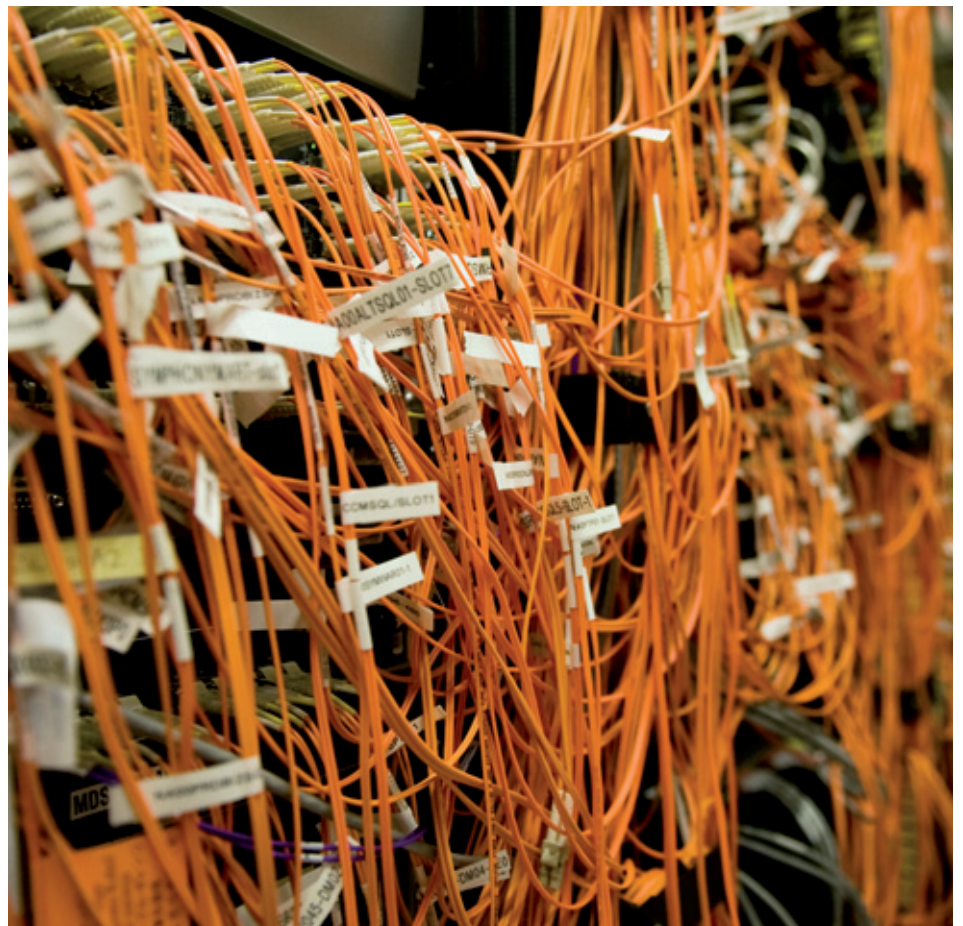
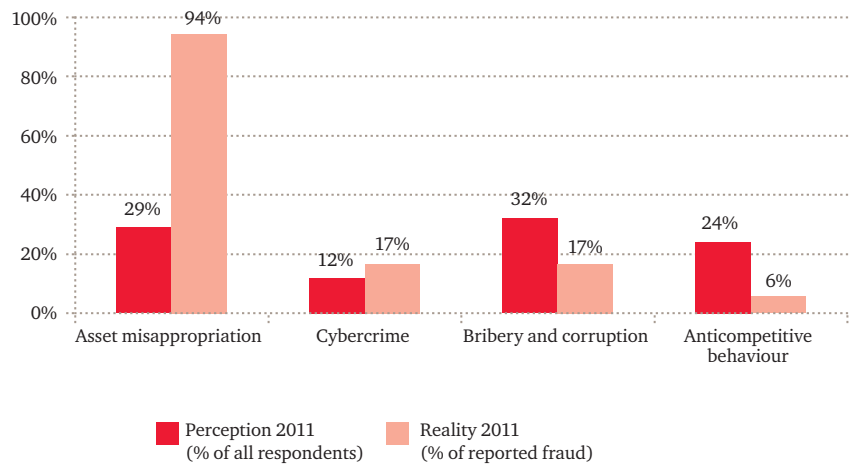
interesting disparity: while only 29% of all respondents think that their organisation will experience asset misappropriation the actual number of respondents who experienced this type of fraud is much higher (94%). On the other hand, while only 17% of fraud reported in Slovakia relates to bribery and corruption, a much higher percentage (32%) perceive this type of crime as a potential problem for their organisation.

Interestingly, for 13% of all Slovak respondents consultation with the auditor is the most likely first step they take when a potential fraud is identified, being higher than CEE (9%).

*“As auditors we have a duty to assess and address the risk of fraud. To do so we look at the controls and procedures that the business put in place starting with the setting of the appropriate tone at the top through the effective codes of ethics and compliance programmes all the way down to operational controls over the transactions and proper segregation of duties. The most pervasive cases of fraud tend to be those that involve senior management. When there is a serious suspicion of management fraud it is important to act promptly in order to increase the chance of a successful investigation. The investigation needs to be set up and the investigators need to report to a sufficiently high level in the organisation that is beyond any suspicion – I recall a case where the Chairman of the Audit Committee of the ultimate shareholder was very successfully put in charge. Well set up and properly conducted investigations usually end up not only with the necessary corrective actions but the specific lessons learned are used to raise awareness around these sorts of issues and strengthen the internal controls and compliance procedures.”*

Alexander Šrank  
Partner  
Assurance

Chart 9: Perception versus reality in Slovakia



# Contacts



---

**Sirshar Qureshi**

Forensic Services Partner for the  
Czech Republic and Slovakia

+420 251 151 235

---



---

**Alexander Šrank**

Partner  
Assurance

+421 259 350 587

---



---

**Michal Kohoutek**

Director  
Forensic Services

+420 251 151 231

---



---

**Pavel Jankech**

Senior Manager  
Forensic Technology Solutions

+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: [name.surname@sk.pwc.com](mailto:name.surname@sk.pwc.com)  
[www.pwc.com/sk](http://www.pwc.com/sk)

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at [www.pwc.com/sk](http://www.pwc.com/sk).

© 2011 PricewaterhouseCoopers Slovensko. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Slovensko, s.r.o., which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.