www.pwc.com/sk/forensic-services

Global Economic Crime Survey 2014

Economic Crime is on the rise

Report for Slovakia

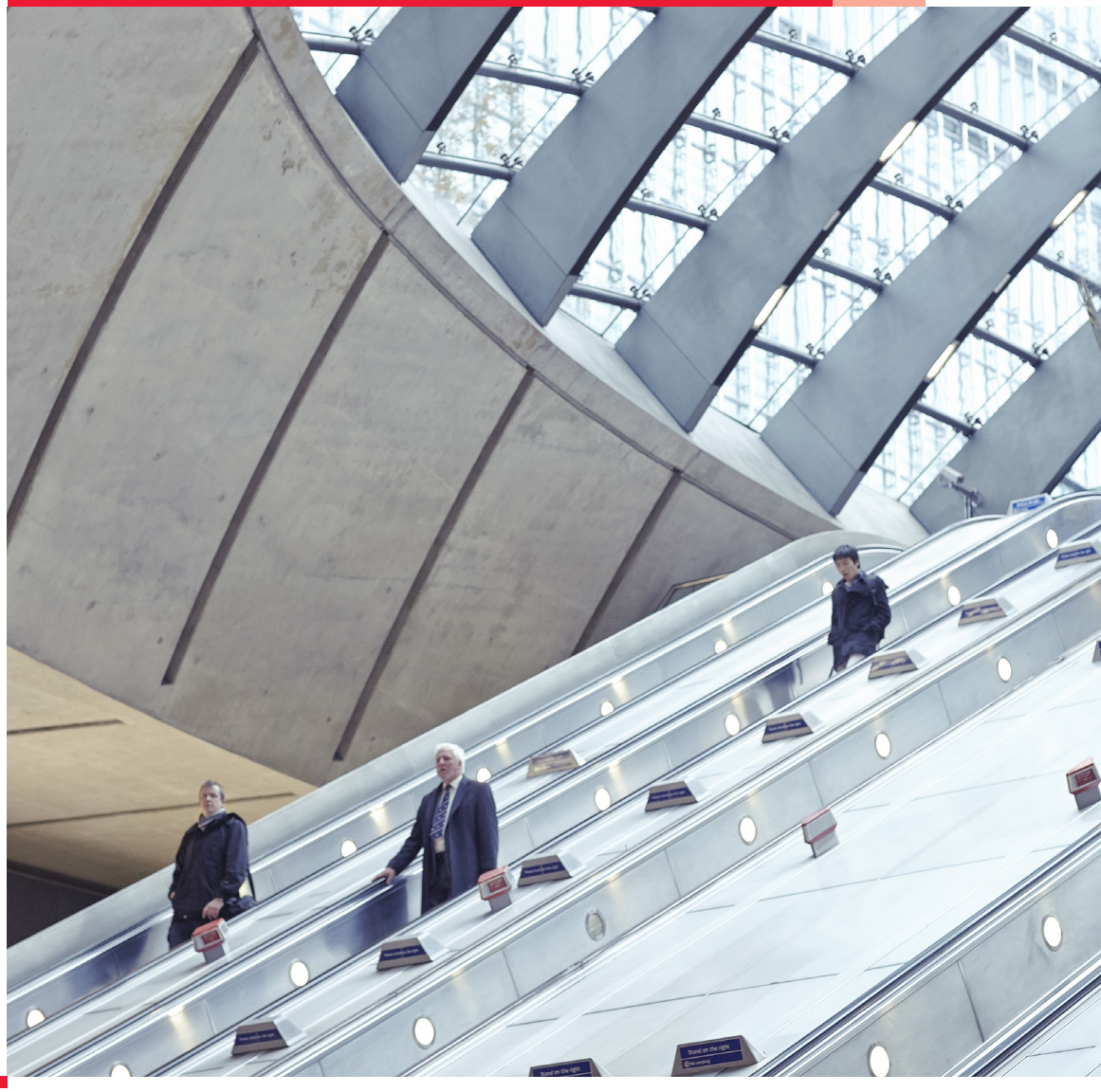
Evolution of Fraud

Dangers of Crime

Cybercrime

Procurement Fraud

Corruption and Bribery



pwc

Contents

The Global Economic Crime Survey 2014 was carried out by PwC. It is the largest survey of its kind with 5,128 survey participants from 99 countries, including 76 respondents from Slovakia.

The survey is intended not only to describe the current state of economic crime but also to identify trends and the perception of future risks.

Preface

In Lewis Carroll's 'Alice Through the Looking Glass', the Red Queen is reported as saying: *"Now, here, you see, it takes all the running you can do, to keep in the same place"*. In modern times, this has been used as an analogy of the theory of evolution.

We can take Mr Carroll's words as a very fine description of the development of the area of economic crime. Economic crime is constantly evolving and seeking new ways to thrive. Companies need to find new and more efficient ways to defend their assets or else they will be outpaced by the evolution of fraud.

The Global Economic Crime Survey 2014 supports this observation: economic crime is more common in the Slovak Republic and takes more diverse forms. Above all, procurement fraud has emerged as a standalone major category of fraud. We strongly advise companies to adjust their risk assessments accordingly.

Other interesting observations include a rise in the cost of economic crime, an increase in the share of fraud committed by agents or intermediaries, and generally the strict measures taken by companies against identified fraudsters.

We invite all entrepreneurs and managers to read through the report and to draw conclusions relevant to their undertaking. A global report available on www.pwc.com/crimesurvey and local variants for different countries including Slovakia are available to help companies doing business globally.

Last but not least, we would like to thank the survey participants who were kind enough to share their observations of fraud and provide their insights. We are especially grateful to the 76 responding entities from the Slovak Republic. All respondents share our belief that economic crime is too costly to ignore.

Sirshar Qureshi
Partner responsible for Forensic Services in CEE
PwC

Michal Kohoutek
Head of Forensic Services
PwC

Main Findings

The Dangers of Crime

Econimic crime is on the rise
Economic crime is increasingly common in the Slovak Republic. 34% of respondents indicated that their company has experienced economic crime within the last 24 months in the Slovak Republic; this represents a significant increase compared to GECS 2011 (21%). The current occurrence is in line with regional and global averages (38% and 37% respectively). 58% of organisations who suffered economic crime estimated the resulting total financial loss as USD 100,000 or more.

Types of economic crime are more "creative"
Traditionally, assets' misappropriation is the main type of crime seen (54%). However, fraudsters seek out new avenues from which to defraud their victims. The distribution of various types of economic crime is becoming more even, seeing an increase in the share of other types of crimes: bribery or corruption (31%), procurement fraud (31%), mortgage fraud (19%), cybercrime (12%), and money laundering (12%).

Cybercrime

Occurrence
Globally, companies are more likely to suffer cybercrime than at any time in the past. A decline in the reported instances of cybercrime in the Slovak Republic (12% compared to 17% in GECS 2011) raises doubts regarding the ability of Slovak companies to detect cybercrime. The latency (share of undetected occurrences) of cybercrime may be even higher than in other countries.

Risks of cybercrime
In business practice, more and more reliance is being put on web applications, remote access and clouds. This increases the potential impact of cybercrime.

High frequency of undetected cases
Generally, cybercrime is dangerous as the victim companies might not detect the fraud taking place. We believe the latency is higher than the latency of asset misappropriation. Therefore, the real occurrence is most probably significantly higher than the number reported.

Procurement fraud

Occurrence
Procurement fraud emerged as a standalone category of fraud, having been reported by 31% companies in Slovakia that were a victim of fraud. The top reported risk factor is the process of selecting vendor contracting /maintenance.

Risks of procurement fraud
Procurement fraud usually includes collusion between business parties. Therefore, the detection of this type of fraud is often difficult. However, there are ways to mitigate the risks. For example, companies with a large number of transactions and vendors may take advantage of data analytics to identify potential frauds or inefficiencies in procurement.

Corruption and bribery

Risks of corruption
31% of companies that experienced fraud reported bribery and corruption. In comparison with the last survey, this represents an increase of 14 percentage points. Corruption is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss. This is supported by PwC's 17th Global CEO Survey 2014: 69% of Central and Eastern Europe ("CEE") Chief Executive Officers ("CEO") are concerned about the impact of corruption and bribery on their business. According to the PwC CEO Survey, corruption and bribery was the top threat to growth in the CEE region.

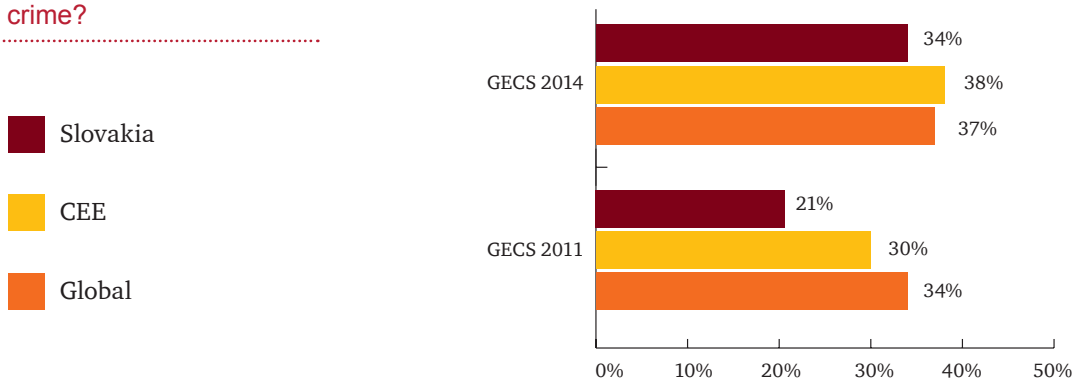
Economic Crime in the Slovak Republic

Central themes

Dangerous territory?

We have seen a rise in reported economic crimes since the previous survey. In 2011, the number of Slovak companies detecting frauds (21%) was well below the regional and global average (30% and 34% respectively). This year, 34% of respondents indicated their companies had experienced economic crime in the past 24 months, which is in line with the global and regional average (37% and 38% respectively).

How many companies experienced economic crime?

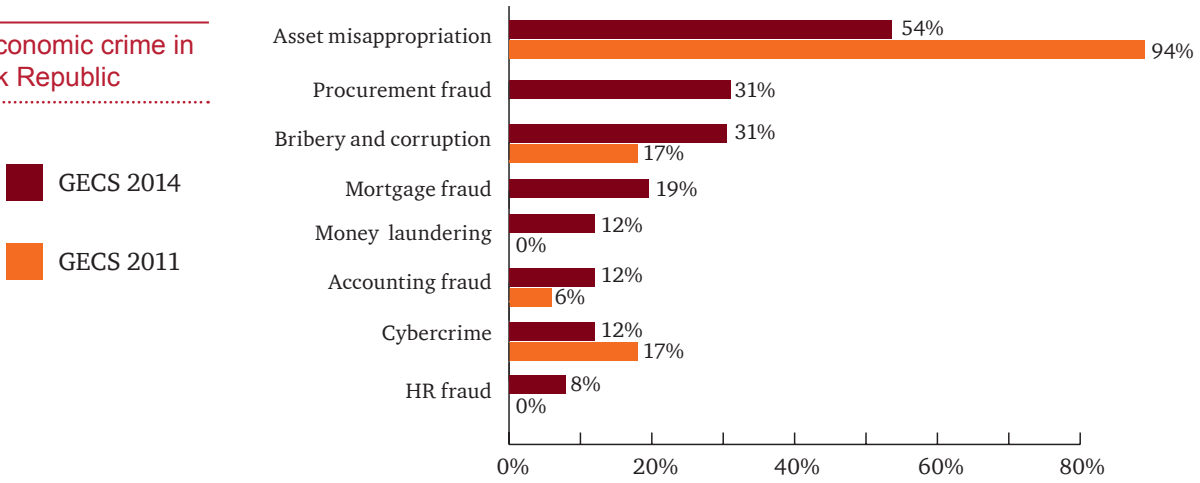


In order to understand the underlying reasons behind the increase, let us have a look at the changes in individual fraud categories.

Greater propensity to types of economic crime

Attacks against corporate assets are more and more ”creative”. The relative share of asset misappropriation as the traditionally most common and simplest type of crime is decreasing in favour of more “creative” types of fraud.

Type of economic crime in the Slovak Republic



Since our first global economic survey in 2001, three types of fraud have consistently registered as leaders among respondents – asset misappropriation (usually by a wide margin), bribery and corruption, and accounting fraud. We added cybercrime as a distinct classification in 2011 and it immediately registered at 17%, alongside bribery and corruption, and accounting fraud.

This year, we added another new category – procurement fraud. Potentially driven by the on-going megatrend of outsourcing and organisational interconnectivity, procurement fraud received a significant response (31%), making it one of the most common types of fraud in the Slovak Republic.

The two other newly added categories of mortgage fraud (19%) and human resources fraud (8%) also reported significant occurrence in the Slovak Republic and it comes as no surprise that the overall number of organisations reporting economic crime in the Slovak Republic has increased so dramatically.

The most significant changes when comparing 2011 and 2014 were reported as the occurrence of money laundering (increase from 0% to 12%) and asset misappropriation (decrease from 94% to 54%). This seems to support the belief that the traditional type of fraud as asset misappropriation is still significant, however is decreasing in favour of “modern” types of fraud, or the schemes used by fraudsters are becoming more sophisticated and thus difficult to detect.

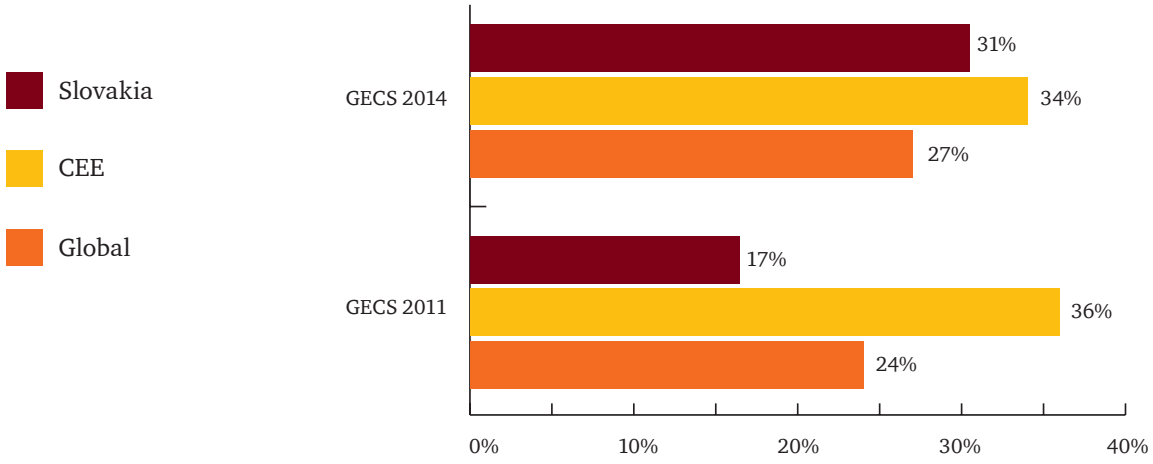
It is also quite likely that the relative occurrence of crimes such as bribery, cybercrime or procurement fraud is even higher. These types of crimes are difficult to detect. During our own forensic engagements, we encountered numerous instances of long-term schemes which were accidentally detected by the victim company.

Therefore, companies should pay adequate attention to the different fraud schemes they may be facing. Control over cash and other physical assets might not be enough.

Corruption and bribery

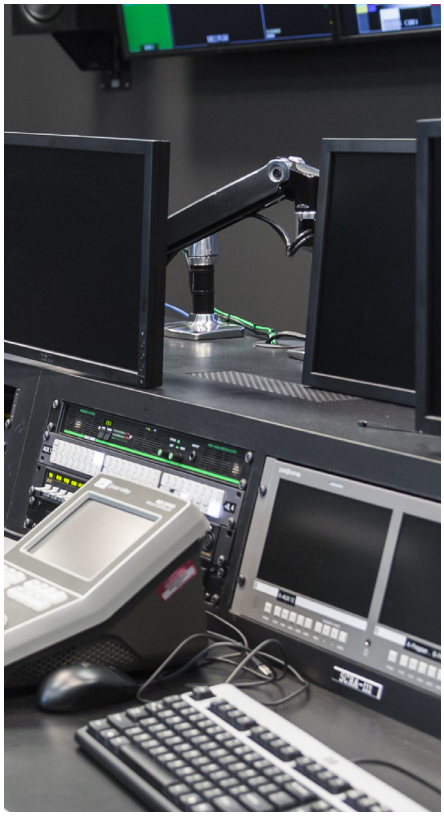
In recent years, corruption has become a topic of public discussion in the Slovak Republic, and for good reason. Corruption is among the most serious economic crimes and is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss. In terms of occurrence, it is the second most recorded type of economic crime in the Slovak Republic (31%) and the third globally in GECS 2014 (27%). CEE is, along with Africa, the region with the largest prevalence of corruption.

Share of corruption and bribery on fraud reported



PwC's 17th Global CEO Survey 2014 indicated that corruption awareness is on the rise, more than half of CEE CEOs considered corruption and bribery to be a threat.

According to GECS 2014, 20% of Slovak respondents indicated their company has been asked to pay a bribe in the last 24 months. 41% of respondents believe their company has lost an opportunity to a competitor which they believe had paid a bribe in the same period.



Procurement fraud

For the first time, 2014 GECS included procurement fraud as a separate category within the economic crime category. 31% of Slovak companies which reported economic crime indicated that their companies experienced at least one instance of procurement fraud.

The reported high occurrence of procurement fraud exceeded even our expectations. As the detection of procurement fraud is difficult, it is probable that the actual occurrence is even higher.

This ranks procurement fraud as the second-to-third (together with bribery and corruption) most common reported type of fraud in the Slovak Republic. The most vulnerable point is vendor contracting and maintenance.

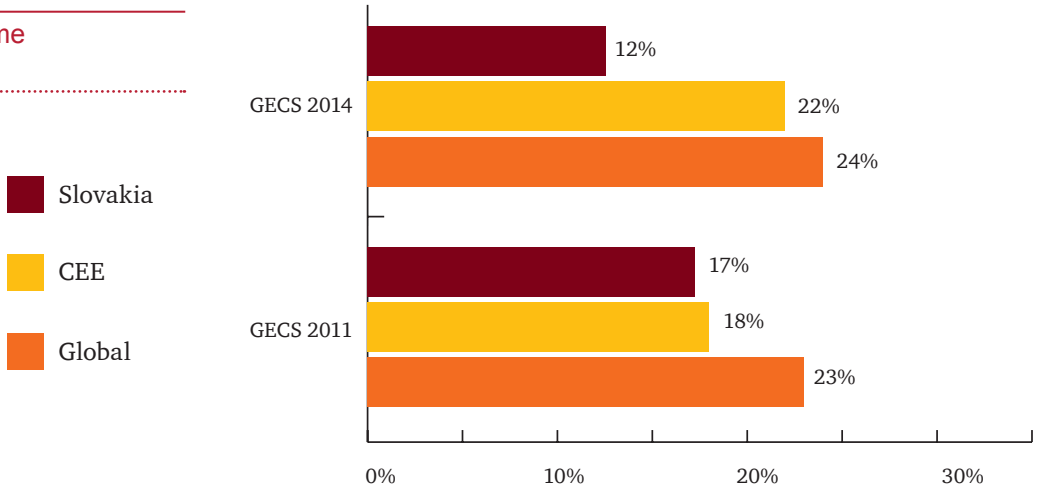
Generally speaking, when an organisation goes outside its own walls for services, goods or assets, the potential for procurement fraud exists. An increasing interconnectedness of business entities, together with more common outsourcing, makes companies more vulnerable to procurement fraud than ever before. Moreover, there are numerous ways procurement fraud can be committed. As a result, procurement fraud is one of the more difficult frauds to be detected and investigated.

Cybercrime

Interestingly, the share of cybercrime as reported by Slovak companies is well below regional and global averages. The last share of 12% is even lower than the corresponding number from the previous pool (17%).

Cybercrime

Share of cybercrime on fraud reported



Contrary to the low number of reported actual instances of cybercrime, 24% of respondents expect they will experience at least one occurrence of cybercrime in the next 24 months (see graph on page 14).

This raises certain doubts as to a possible gap between detection of cybercrime and its true occurrence. It is not clear why cybercrime's share in Slovakia, which is definitely a well-developed and computerised country, would amount to only half of its share in other countries. Therefore, we believe there is a risk that Slovak companies do not have the necessary abilities for detection (and prevention) of cybercrime. However, we have to bear in mind that almost one fourth of Slovak respondents thinks they are at risk of cybercrime and perceive a cybercrime occurrence likely in the forthcoming 24 months.

Modern companies are following trends in utilising technology to its full potential and to give their employees more freedom. People work from home using their own smart devices connected to cloud, respond to emails from internet cafes while on vacation, and review reports at airports. This is basically enlarging the perimeter that needs to be protected and deal with environments that are not fully under company control.

This is also a reason for a shift in security paradigm:
- 90s - respond after the breach;
- 00s - get ready for the breach; and
- 10s - assume the breach has happened or is underway.

It is not a question of whether the company will be subject to cyberthreat, but when and how it will happen. Successful companies are prioritising what matters most - guarding their crucial data against organised targeted attackers in the global business ecosystem covering fluid data moving around internally as well as to/ from business partners and other stakeholders. More than one half of respondents indicated that their perception of cybercrime risks has increased over the last 24 months. Theft of intellectual property, personal data or damage to reputation is of the greatest concern when it comes to cybercrime.

We can describe one of the cases we have worked on in the past. IT personnel in a large energy company found a computer in their server room, which they did not have in their books and they could not access it. At the same time they started to experience drop outs in internet connectivity, which was a significant issue due to online banking.

Through the investigation we have established the function of the unknown computer - one of the IT administrators was running a side internet business and he was misusing company resources for that. His cyber activity actually affected the whole business because they were not able to reconcile client payments as the online banking was not functioning.

Tomáš Kuča, Risk Assurance Partner leading our cyber security practice

Aren't cybercrime and cybersecurity just more buzzwords?
These are labels for the current phenomena in the information technology world. The rise of cybercrime is evident and supported by thousands of cases happening around us all the time. Cybersecurity is a preventative measure used to respond to this situation.

What has changed in this field in the last couple years?
In the past, companies responded after an incident occurred. In better cases they were building their protection in anticipation of a future incident. It would seem the current best approach for development of a cybersecurity policy is to assume a security breach has already happened.

The attackers have changed, which means they use sophisticated and persistent methods, they target specific information for strategic gains, they work across the globe, they are structured and organised and some of them act on behalf of states.

What can be done to improve our situation?
- Employ a chief information security officer and get him involved at the board level "the top of the house".
- Clarify roles and responsibilities in this area.
- Create a cyberincident response team.
- Invest in cyberskills of your employees.
- Set up cooperation with cybercrime experts.

Impact of economic crimes

No discussion of economic crimes would be complete without trying to quantify the impact of fraud. After all, the anti-fraud effort is just another function of the company which should pay off to justify its existence.

In Slovakia 58% of respondents who experienced economic crime reported a total loss of at least USD 100,000. This is a reported loss by companies that usually care and try to prevent and detect fraud. How greater would the actual loss be if the company did not care and there were no counter fraud measurements?

There are also other negative impacts on the company besides purely financial losses. Companies report a clear impact on the company's reputation and employee morale as the greatest non-financial impact.

In this respect, we would like to point out that a negative impact on employee morale might serve as a trigger to secondary actions (fraud being perpetrated by frustrated or demotivated employees). "Everybody does it" or "they deserved it" has been observed many times as a handy rationalisation of first-time fraudsters!

Managing fraud

Who commits fraud

We tried to make a profile of the perpetrator of the most serious economic crime that the respondent companies had experienced.
There is an imbalance of internal and external perpetrators of the most serious fraud detected (31% against 58%).

It should come as no surprise that middle to senior managerial persons are much more likely to commit the most serious internal fraud than junior staff members. The most typical fraudster is male, 31 to 40 years old and has spent 6 to 10 years in the company.

The person most likely to commit the most serious external fraud is a customer, both in the Slovak Republic (53%) and globally (32%). As already indicated in GECS 2011, we would recommend that organisations continue their efforts on the prevention front: knowing your employees and your business partners prior to engaging with them is less costly than dealing with the consequences of fraud.

Prevention of fraud

Why would someone decide to commit a fraud? Our survey indicates that by far the most significant contributing factor for internal fraudsters is simply opportunity.

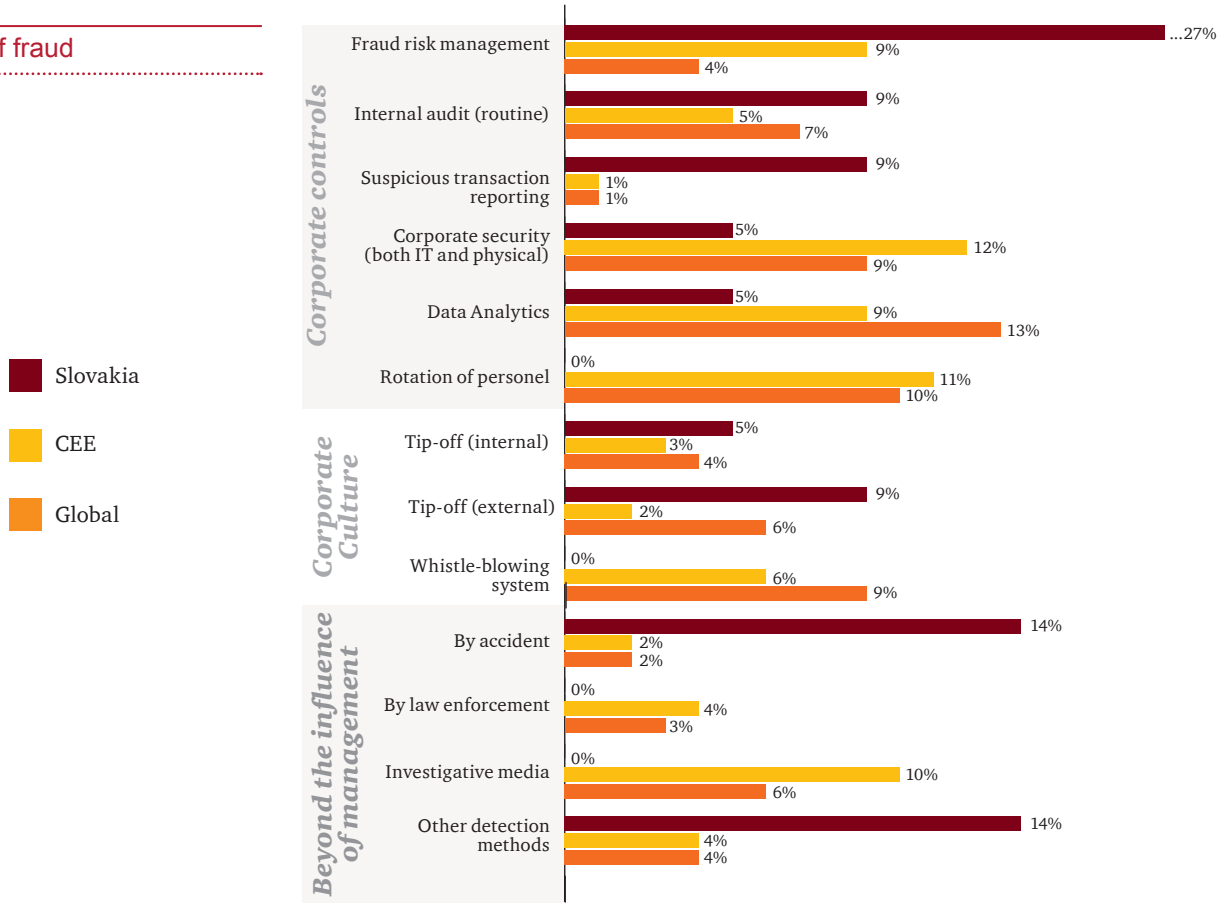
At the same time, out of the possible contributing factors, opportunity is the one most within a company's control. Therefore, a review of procedures in the areas most vulnerable to fraud may be an effective way to reduce the risk of falling victim to fraud.

Detection of fraud

The survey results indicate a different distribution than the global results. In total 27% of Slovak organisations that reported economic crime have detected fraud via Fraud risk management which significantly above the regional and global results (9% and 4% respectively).

Detection by accident reached 14%, while globally the crime survey reported only 2%. This might indicate a potential link to the overall lower occurrence of fraud in Slovakia compared to CEE and global – the number fraud cases could remain undetected by the companies.

Detection of fraud



Numbers are rounded to the nearest whole number

And what's the first reaction of a company when a potential fraud is detected? Most companies resort to internal investigation. Interestingly, almost one fifth waits to see if further indications of potential fraud occur before they react.

Pavel Jankech,
Senior Manager in Forensic Technology Services

Do you think that the measures that companies use to combat fraud are sufficient?
Currently, companies primarily use preventative measures to combat fraud. This, however, increases the risk that fraud will remain undetected longer. Our experience shows that fraud is usually identified, on average, only after it has already been taking place for two years. The impact of such fraud can be really serious, and it's not just a pure financial loss. A company's reputation, employee morale, or business relationships with business partners are also at risk.

What would you recommend to companies?
A robust control environment is an absolute necessity. Nevertheless, it is never 100% bulletproof so we recommend the companies also implement detection mechanisms, such as regular data analytical tests or a continuous fraud detection system. Using detection measures will help a company to identify fraud sooner and thus reduce losses.

What data test do you have in mind?
Traditional methods seek to identify suspicious transactions (red-flags) through rule-based testing. Classic examples include round-sum invoices and late-night postings. The challenge is that red-flags are typically not unusual events, and therefore the outputs from the tests are long lists of exceptions with many false-positives, leading to a costly manual investigation. Moreover, these rules are already well known, so the fraudster can easily avoid them.

How to proceed in these cases?
Based on our experience, each fraud scheme can be classified into one of several categories. Each of the different types of fraud leaves a specific "footprint" in the data. Using advanced analytical techniques and visualisation, we can identify different patterns of behaviour that correspond to these tracks. This approach can be used proactively to identify potential weak areas of control in the company, or reactively in the investigation of a specific incident.

What kind of advanced analytical techniques are they?
These are advanced statistical methods or data mining techniques. These can help identify hidden patterns in the data behaviour. Each of the patterns indicates the behaviour of the supplier or user, and is compared with standard behaviour in the dataset. Unusual or anomalous patterns indicating fraud are subsequently investigated. Using a combination of techniques to visualise the data and detailed knowledge of the company, the investigation should just focus on unusual or anomalous behaviour. The results of detailed investigations shall apply retroactively to increase the accuracy of the search algorithm.

What data is required for this type of testing?
During the initial phase of the project we would seek to understand the specifics of the company and its business and its existing control environment to identify key risk areas for fraud. Based on those we would decide where to start looking for fraud. The main sources are typically data from ERP and accounting systems, or actual cash flows gathered directly from bank statements, but also other, less usual sources of data like car GPS records, physical entry access records, or call or network traffic logs can be utilised for analysis.

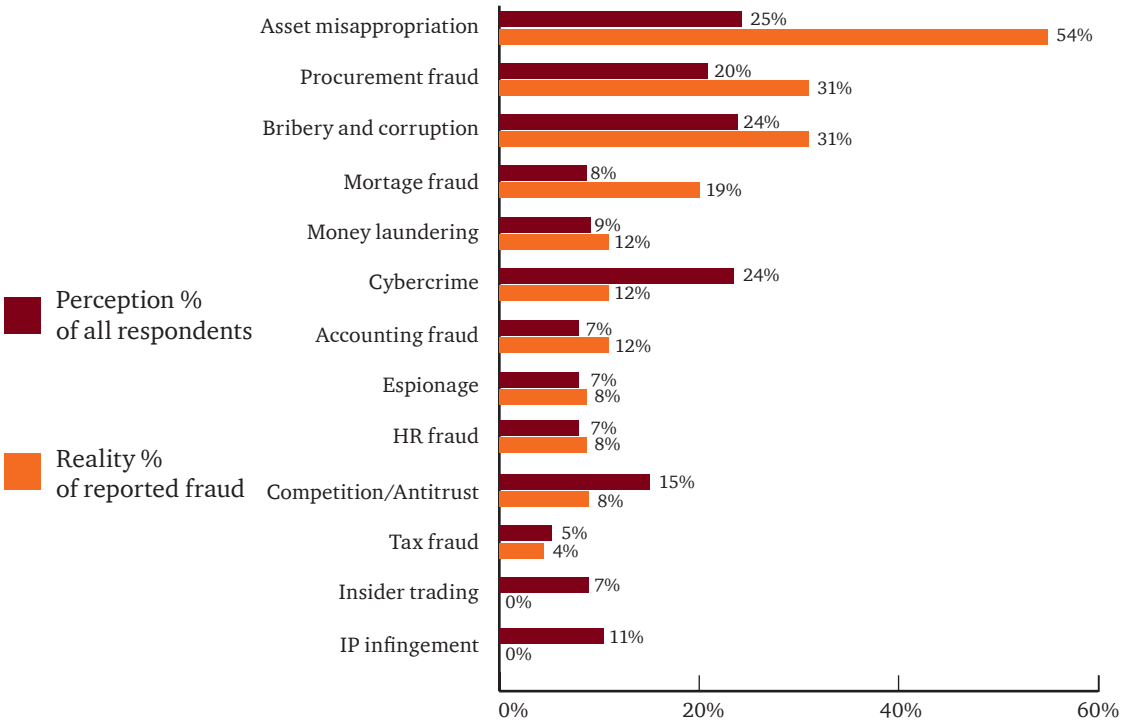
Remedial actions

The survey indicated a clear stance of most companies against fraudsters, both internal as well as external. The occurrence of dismissals of internal perpetrators (100%) is even higher than in the previous survey (82%). This would suggest a high awareness of companies that fraud is costly. Especially in times of economic turmoil, there are few reasons to take fraud lightly. Civil action (38%) is preferred to law enforcement action (25%).

With an external perpetrator, dismissal is obviously not an option. The most preferred option is the termination of the business relationship (67%), with the notification of law enforcement authorities as the second most common action (60%).

Expectations

We also asked which types of crime companies expect to face in the next 24 months. Please note that the following data depend on the perception of risks by the companies. This is not the same as the real extend of risk. Still, it is interesting to compare the perception of risks with the real occurrence. It would seem that companies underestimate the risk of asset misappropriations in spite of its reported occurrence.



Are you a member of our Fraud Forum?

The Fraud Forum is a platform for sharing the knowledge and experience of managers and professionals dealing with fraud prevention, detection, and forensic investigation in companies. Membership in the Fraud Forum is extended to financial directors and specialists, internal auditors, risk and compliance managers, security and forensic investigation specialists, and company lawyers.

The Fraud Forum offers

- professional updates and the latest information about trends in fraud prevention, detection and forensic investigation;
- participation in seminars and discussion forums on various topics relating to fraud in companies;
- opportunities to participate in surveys focused on fraud and obtain detailed conclusions and reports from the surveys; and
- opportunities to share knowledge and exchange experience and opinions with other.

Membership in the Fraud Forum platform is free and absolutely flexible – each member can participate in any and all activities that are of interest to him/her. By becoming a member of the Fraud Forum, you will have the opportunity to meet regularly with other members and share your knowledge, experience and ideas with them. We will send you updates, analyses and invitations to events organised by the Fraud Forum.

For registration form please follow the link www.pwc.com/sk/fraud-forum. If you have any questions relating to Fraud Forum platform, please contact **Jana Grošeková at: jana.grosekova@sk.pwc.com**.

Contact

Sirshar Qureshi
Partner, CEE Forensic Leader
+420 251 151 235
sirshar.qureshi@cz.pwc.com

Michal Kohoutek
Head of Forensic Services
+420 251 151 231
michal.kohoutek@cz.pwc.com

Pavel Jankech
Senior Manager
Forensic Technology Solution
+420 251 151 336
pavel.jankech@cz.pwc.com

Radoslav Ratkovsky
Manager
Advisory Services
+421 259 350 585
radoslav.ratkovsky@sk.pwc.com

Bratislava

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

Košice

PwC, Aupark Tower, Protifašistických bojovníkov 11, 040 01 Košice
tel.: +421 (0)55 32153 11, fax: +421 (0)55 32153 22

www.pwc.com/sk

About the Survey

The 2014 Global Economic Crime Survey was completed during September and October 2013. There were 5,128 respondents from 99 countries, including 76 respondents from Slovakia. Of the total number of respondents, 50% were senior executives from their respective organisations, 35% represented listed companies and 54% represented organisations with more than 1,000 employees. www.pwc.com/crimesurvey

pwc