Global Economic Crime Survey 2016

Slovakia

34% companies experienced one or more incidents of economic crime

13% of incidents were cybercrime
The Global Economic Crime Survey 2016 was carried out by PwC. It is the largest survey of its kind with 6,337 survey participants from 115 countries, 89 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.
We are pleased to present to you the results of 2016 PwC Global Economic Crime Survey which continues to be the largest study of its kind available worldwide. To get the most updated insight into the current state of economic crime, its perception, impacts and the awareness organisations have about economic crime, we collected responses from 6,337 organisations from 115 countries, including 89 leading companies in Slovakia.

This year’s survey again draws attention to cybercrime, which was considered a completely new form of economic crime a couple of years ago; however, it has recently formed an integral part of any fraud-related discussion. No company is immune – cybercrime affects organisations irrespective of the industry and geography. Apart from cybercrime, the survey turns the spotlight on the ethic and compliance area. In light of the continuously growing globalisation of the business environment and increasing enforcement, compliance has become a prominent topic.

This report also explores the theme of opportunity — not only those opportunities that enable economic crimes to be perpetrated, but, more importantly, the opportunities available to organisations to proactively counter economic crime while balancing their legal responsibilities.

We invite all entrepreneurs and managers to read through the report and to draw conclusions relevant to their undertaking. A global report and local variants for different countries are available to help companies doing business globally.

We believe that the results of our analysis will allow companies to better understand the significant impact that economic crime can have on their business, assess the risks of fraud that they may face, and find ways to mitigate those risks.

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 responding entities from Slovakia. All the respondents share our belief that economic crime is too costly to be ignored.

Sirshar Qureshi,
Partner responsible for Forensic Services in CEE, PwC
The highlights

The current fraud environment in Slovakia

Economic crime continues to be a serious issue affecting organisations worldwide, across Central & Eastern Europe ("CEE") and in Slovakia. In Slovakia more than one third (34%) of respondents has experienced one or more incidents of economic crime in the past 24 months. Occurrence of economic crime in Slovakia is comparable the average for CEE (33%) and globally (36%).

Compared to previous surveys, the occurrence of overall reported economic crime is the same. It does not necessarily mean that the environment is stable. In the context of the evolving risk landscape, organisations might face sophisticated fraud schemes which remained undetected for several years. These latent and long running fraud cases represent more dangerous and costly threats for the companies than one-off incidents.

Traditionally, the most common type of economic crime in the Slovakia is asset misappropriation (67%). Asset misappropriation has been traditionally seen as easier to detect compared to other types of economic crime, thus its prevalence year after year is generally predictable.

Apart from asset misappropriation, the top five types of economic crime reported by our survey participants include cybercrime (13%), procurement fraud (20%), bribery and corruption (23%), insider trading and mortgage fraud (10% each).

Most fraud in Slovakia is detected by various means of corporate control (in total 61%). Around one from every five fraud cases is detected by means that were influenced by corporate culture; 11% of cases are raised by tip offs from external parties.

According to the 2016 survey, the share of crime committed by internal perpetrator (52%) on the committed fraud is prevailing when compared to external perpetrator.

In Slovakia more than one third (34%) of respondents has experienced one or more incidents of economic crime in the past 24 months.
Cybercrime

13% of the respondents in Slovakia that suffered an economic crime reported that they have experienced cybercrime. This is well below the CEE results and global average. If there should be one take away from this survey, it should be the change in perception of cybercrime – cybercrime is no longer just an IT problem, rather, it should be considered a fundamental business problem.

According to our previous surveys, the trend in the occurrence of reported cybercrime is stable. Considering the changing business ecosystem where the vast majority of documents, communication and transactions has gone digital, this is something of a contradiction.

According to the survey, participants from Slovakia consider cybercrime to be the second biggest threat after asset misappropriation and its occurrence in the next 24 months is likely in opinion of 17% of the respondents. This perceived risk is lower in comparison with CEE (25%) and global results (34%). However, 58% of surveyed organisations think that the risk of cybercrime has increased.

Due to rapid technological progress, the traditional perspective of cybercrime has become much wider. Currently, cyber risk encompasses more than just computers. The appliances at risk of cybercrime range from mobile devices, gadgets interconnected in cloud, cars to household devices.

Cybercrime appears to be costly in financial terms. Globally, one fourth of the surveyed organisations has lost EUR 44,000 or more through cybercrime in the last two years.

Ethics and compliance

According to our survey, corruption and bribery rank as the fourth most common types of economic crime in Slovakia. At the same time our survey participants reported that 8% of organisations were asked to pay a bribe in the past 24 months. This number is considerably lower when compared to the CEE (17%) and global (13%) average.

The positive message is that more than 80% of the survey participants have a formal business ethics and compliance programme which is slightly below the CEE and global average (both 82%).

90% of the organisations surveyed responded that the Code of Conduct in their organisation covers key risks/policy areas and sets out the organisational values. According to 92% of respondents, their organisational values are clearly stated and understood and 57% of organisations provide regular training on the Code of Conduct and supporting policies. These relatively high reported numbers suggest that Slovak companies have adequate Codes of Conduct. Having an understanding of the employees and firm-wide communication are two of the key features contributing to the effective compliance function. In addition, regular trainings are advised for all participants.

Approximately 8% of organisations were asked to pay a bribe in the past 24 months.
Economic Crime in the Slovak Republic

Economic crime is an obstinate threat
How many organisations experienced fraud in the last 24 months?

Economic crime continues to be a major concern for organisations of all sizes, industries and different ownership structures. In Slovakia, more than one third (34%) of respondents has experienced economic crime in the past 24 months. When compared to the relevant region, CEE, which indicates 33%, the occurrence of economic crime in Slovakia is slightly higher. The positive outcome of this result is that it demonstrates a stable trend with the results of the previous survey from 2014 but it still shows a growing trend considering the results since 2011.

Occurrence of crime

More than 10 incidences per company were reported by 17% of companies who experienced economic crime in comparison to 31% in 2014 survey. This result is significantly lower when compared to the CEE (30%) and global (31%) occurrence.
What types of economic crime are companies facing?

Among the most common types of economic crime are asset misappropriation (being the first with 67% of organisations who have suffered this form of economic crime), followed by bribery and corruption (23%), procurement fraud (20%), cybercrime (13%) and insider trading and mortgage fraud (both 10%).

Most of the economic crime types have decreased compared to the results from previous surveys (except for cybercrime and accounting fraud).

Asset misappropriation has been first place in our survey for a number of years. This fact is generally predictable, because asset misappropriation is regarded as the easiest of frauds to detect.

Generally speaking, the Slovak results are more or less in line with economic crime as shown in the CEE and global statistics. Slovak surveyed companies had a lower occurrence of cybercrime than those in CEE and globally. Bribery and corruption appear to be more significant issues on the CEE level than in Slovakia.

Types of fraud

- Asset misappropriation
- Cybercrime
- Bribery and corruption
- Procurement Fraud
- Accounting Fraud
- Human resources fraud
- Money laundering
- Intellectual Property (IP) Infringement
- Insider Trading
- Tax Fraud
- Mortgage Fraud
- Competition/Anti-Trust Law Infringement
- Espionage
- Other
Cybercrime

Cybercrime in Slovakia has risen since 2014, but all the values are below both CEE and Global levels.

It has risen globally as well as regionally, but, in Slovakia, it is well below those levels (13% in Slovakia compared to 22% in CEE and 32% globally). Cybercrime is also perceived as the second biggest threat in terms of economic crime among the respondents in Slovakia.
Bribery and corruption

In spite of the fact that our surveys report a decrease in bribery and corruption in Slovakia (from 31% in 2014 to 23% in 2016), in the CEE and globally as well, this type of economic crime has been significant since 2011.

Surveyed participants also reported that in the last 24 months their organisation was asked to pay a bribe (8% in Slovakia) and also lost an opportunity to a competitor who paid a bribe (22% in Slovakia). The current numbers for Slovakia represent a significant drop (by 12 and 19 percentage points respectively) compared to the previous issue of the survey.

This decreasing trend appears optimistic; however, we should be careful when drawing conclusions as the actual state of corruption and bribery can be much worse. Based on our experience, corruption and bribery are types of economic crime that are rather difficult to detect. The perception of bribery and corruption also might be subjective across the organisations – behaviour that one considers to be part of normal business practices, another might see it as already crossing the borders of corruption and bribery.

Bribery and corruption

<table>
<thead>
<tr>
<th>Region</th>
<th>GECS 2011</th>
<th>GECS 2014</th>
<th>GECS 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>SK</td>
<td>17%</td>
<td>23%</td>
<td>24%</td>
</tr>
<tr>
<td>CEE</td>
<td>31%</td>
<td>36%</td>
<td>34%</td>
</tr>
<tr>
<td>Global</td>
<td>39%</td>
<td>24%</td>
<td>27%</td>
</tr>
</tbody>
</table>
How much does fraud cost?

When considering the financial losses due to economic crime, the survey shows that 47% of Slovak organisations who suffered economic crime have lost EUR 44,000 or more.

Our survey respondents consistently note wider collateral damage from business disruptions, remedial measures, investigative and preventative interventions, regulatory fines, legal fees — and, critically, damage to morale and reputation — as having a significant impact on long-term business performance. These kinds of losses, of course not always quantifiable, can over time dwarf the relatively shorter-term impact of financial losses.

However, the consequences of economic crime for companies are much wider than just financial losses. Of those who had experienced damage as a result of fraud, 73% of companies state that their employees' morale was negatively affected. One half of the organisations reported damage to employee morale and 31% consider that their business relationships have been impacted by fraud.
Technology – an economic crime: blessing or curse?

Cybercrime is a threat to all aspects of business

It is no surprise that, in the current digital business environment, there is an increasing trend in the occurrence of cybercrime globally. Its frequency has changed since it was first introduced in our survey (17% in 2011 compared to 12% in 2014 and 13% in 2016 of companies which experienced economic crime did experience cybercrime). Furthermore, in Slovakia, 17% of all respondents’ organisations reported that they were affected by cybercrime. This result is slightly below the CEE and global average (22% and 26%, respectively).

The increase in cybercrime incidents as mentioned above is also supported by the perception of the related risk – 58% of surveyed organisations think that the risk of cybercrime has increased.

Damage to the reputation of an organisation, theft or loss of personal identity information and service disruption are globally the greatest concerns when it comes to cybercrime. Cybercrime appears to also be costly in financial terms. Globally, one fourth of the surveyed organisations has lost EUR 44,000 or more through cybercrime in the last two years.

Survey revealed that Slovak companies’ biggest cybercrime threat is perceived to be coming from the external environment (47%) in next 24 months. Despite cybercrime being considered a threat to the companies, board members of almost half of Slovak companies do not request any information regarding readiness to deal with cybercrime. With regards to the readiness to deal with cyber incidents, there are:

- 23% of the respondents’ organisations that do not produce any information regarding the readiness of the organisation to deal with cyber incidents.
- 22% respondents that do not even know about such requests.
The results show that 51% of surveyed organisations have an incident response plan to deal with cyber-attacks - both above the CEE (36%) and global rates (37%). On the other hand, some companies are still not adequately prepared, with 17% of organisations not having any similar plan. This figure compared to 13% of Slovak companies affected by cybercrime and more than a quarter of companies currently does not have any response plan in place is quite high.

More than half of the organisations surveyed in Slovakia (60%) have response teams who are fully trained and able to deal with technology breaches. This figure might seem quite high; however, considering the context of an ever-changing digital environment and the fact that no company is immune to the attacks, companies still have work to do to mitigate the risk of the negative impact of potential attacks.
Response team usually consists of IT security, IT staff, senior level management and an attorney. Only a limited number of incident response teams include a specialist digital forensic investigator (7% in Slovakia and CEE and 11% globally). Inadequate team composition and understandable haste to solve the problem after an incident could lead to a higher risk of crucial evidence being potentially overlooked. This could hamper a company’s ability to fully understand the impact of the breach and ability to prosecute perpetrators.
How did Cyber Fraud evolve in the recent past?
The whole world is currently operating almost everything through ICT (information and communication technologies) and the complexity of solutions, amount of data and hardware performance is increasing significantly every year. Cyber Fraud is evolving as well. For example, due to the price decrease in computation power, the various approaches, which were not possible before, are currently quite common. Therefore, more complex scenarios could happen. It’s important to realise that subjects, which are committing fraud, could use exactly the same technologies as you do and, in many cases, they use them better. It is quite common for them to be able to use advanced analytics like machine learning algorithms e.g. just to simulate the behaviour of a regular customer.

What are the main critical areas where Cyber Fraud is involved?
The most critical area lies in services related to money transfers. Most cyber fraud incidents are related to money theft. The way how is it done differs depending on the type of business (it could be a shortage in a warehouse through the manipulation of warehouse records, changing banking accounts in the procurement or payroll system, layering transactions, identity theft to gain access to banking accounts, etc.). The second critical area is corporate espionage and reputation damage. For example, there are groups which aim to cause significant reputation damage to you because your competitor "hired" them to do it. In general, even this usually has one goal - to gain a better position on the market, which leads to increased profit. Corporate espionage nowadays relies heavily on cyber intelligence.

Which technologies are currently used within Cyber Fraud?
Cyber fraud can incorporate any technology currently available. It is a matter of usage and the perpetrator’s intent on how to use it. Technology choices can range from the usage of special phrases in public search engines to highly sophisticated hacking techniques, which usually involve a social engineering component. The important fact is that the amount of technologies is increasing and, as stated before, the complexity and number of functions in available devices is improved year by year. Therefore, Cyber Fraud is not a case for computers only as we know it. Almost everyone has a smart phone today with access to online/mobile banking. There are smart wearables, which will allow you to interact with some applications as well. The operating systems are part of TVs and Home Cinemas as well. You even have operating systems on gaming consoles or cars and, as we are more and more approaching the era of smart homes, the number of devices, which could be used for Cyber Fraud and Crime, will increase again as well.

What to do if something happened in my organisation?
This is something that depends on the maturity of internal procedures, controls, systems and readiness for such an incident within your organisation. Based on our experience, each type of fraud has a specific fingerprint, which could be detected within enterprise data regardless of whether it is a recurring or one-time-only fraud. We are able to analyse the data (both structured and unstructured), detect these fingerprints and investigate them. We help customers with prevention and also in providing complete support during this unpleasant situation and supporting them with further steps.

Is it possible to do something better to avoid Cyber Fraud or at least to be ready when it happens?
There is always a way to do things better, it mainly depends on your type of business. Typically, the majority of fraudulent cases start because the process settings in an organisation are wrong, the discipline of application users is low and the risk of potential fraud is ignored before it happens. Users must regularly use information systems and comply with internal and external policies and procedures. If you do regular risk assessments within your organisation, you are able to identify weak spots and focus on them. If you are an international company, it is visible how these risks, threats are moving from continent to continent, and from country to country; therefore, you are able to react prior to any incident. On top of this, you can add advanced systems for pattern recognition, suspicious activities detection, incident prediction and others, which are able to utilise and process all your enterprise data (both structured and unstructured data) and increase your level of protection and readiness. Here in PwC we are providing such support based on our long-term experience and proven quality.

Interview

Pavol Adamec
Director, Risk Management and Information Technology
Detection methods

It is a positive finding that an increasing number of fraud incidents is detected via systematic mechanisms (55% of cases in 2014 comparing to 61% in 2016). 61% of the Slovak respondents reported that fraud was detected by corporate controls (compared to 54% in CEE and 47% globally).

In particular, we would like to highlight the increasing share of data analytics (increase from 5% in 2014 to 14% in 2016) and suspicious transaction monitoring (increase from 8% to 25%) . In a changing business landscape, when different fraud incidents leave a different specific footprints in the data, these automated electronic detection mechanisms can be very powerful tools. Moreover, when fully automated, these tools can run in real time without or with very limited human intervention. On the other hand, “traditional” means of detection such as fraud risk management (4%) and internal audit (7%) are reported lower in Slovakia as compared to CEE (10% and 12%) and global (8% and 11%), respectively.

However, despite this encouraging result, this is no time to rest on our laurels. According to the organisations surveyed in Slovakia, 18% of economic crime was still detected by means beyond the influence of management; the most frequent simply by external tip-off (11%). We also see room for improvement in detection methods which can be classified as corporate culture.

A whistleblowing hotline was the detection method in 7% of cases of reported crime with only 34% of companies preparing reports from the whistleblowing hotline. An effective whistleblowing system is not only a powerful tool for combating economic crime, but it is also part of a sound and ethical business environment.
64% of companies questioned performs a fraud risk assessment at least on an annual basis. This figure is in line with the detection methods described above. This figure is higher than the respective results for CEE and global (50% and 51%). An additional 7% of Slovak companies (8% and 10% in CEE and globally respectively) performed a fraud risk assessment at least once in the last 24 months.

Approximately three quarters of the companies, in Slovakia, CEE and globally, utilise internal resources to investigate identified cases of economic crime, while one third contacts legal advisors. Other actions that companies tend to do are contacting an external auditor or engaging a special forensic investigator.

10% of Slovak companies which experienced crime had contacted a forensic investigator, while this percentage reaches 20% globally. Quite surprisingly, 7% of Slovak companies (10% and 11% in CEE and globally, respectively) choses to wait to see if further indicators of potential fraud in the same area might arise.
Fraud risk assessment performed

**Features of an effective whistleblowing hotline**

- Integral part of the organisation’s ethics and compliance programme
- Multiple means (for example: dedicated phone line, email box, contact point) to make the mechanism accessible and easy to use for all employees and whistleblowers from the environment outside the organisation
- Anonymity and confidentiality
- Protection of whistleblower against any retaliation
- Communication and education
- Positive tone at the top
- Analysis of the alerts received through this channel and produce statistics
- Publication of “wins”
- Possibility of an external provider
Perpetrators of economic crime

What is the typical profile of the fraudster?

Historically the split between the internal and external fraudster was usually equal. This year’s survey shows that, in Slovakia, 52% of fraud was committed internally, while 38% was committed externally. For the remainder of the perpetrators, the respondents did not know whether the company was attacked from inside the company or from the outside environment.

If it is an external perpetrator, the global results show it would very likely be a customer (25%). Customer held a higher share than agents/intermediaries (which were at the top in the last survey from 2014) or vendors (17% and 10%, respectively).

How can companies defend themselves from attacks committed by external actors? One of the key recommendations is simply to know who you are doing business with. Before entering business relationships, organisations should employ corporate intelligence and due diligence techniques. These procedures assist organisations to fully identify their business partners and verify the partner’s integrity and probity. Any adverse history should trigger a red flag for the organisation. These procedures should be conducted to determine if there have been changes over time. Moreover, nowadays in light of sanctions and increasing requirements by regulators, these transparency methods have become increasingly important.
What are the drivers of economic crime?

When we asked our respondents what factor they feel has contributed the most to economic crime committed by internal actors, the majority unsurprisingly answered opportunity or ability to do it.

However, the presence of the opportunity only is not sufficient to commit fraud. The perpetrator of the fraud needs to have an incentive or pressure to commit fraud and has to be able to justify the crime. The results of this question indicates that companies consider opportunity to be the most important while they could omit the importance of the other two necessary motivators.

A crucial factor that contributes to the committing of economic crime is simply the opportunity to do it (globally 69%). So the best way to prevent this opportunity is to strengthen controls.
Ethics & Compliance:
Aligning Risks and Responsibilities with Values and Strategy of the Organisations

Four fundamental areas of focus for enhancing the effectiveness of compliance programmes

- **People and culture**
  Clear processes and principles, culture where compliance is hard-wired to values, measuring and rewarding desired behaviours.

- **Roles and responsibilities**
  Formal compliance structure ensuring they are correctly aligned with current risks.

- **High-risk areas**
  Better implementing and testing in high-risk markets and divisions.

- **Technology**
  Better use of detection and prevention tools, including big data analytics.

Our survey shows that formal business ethics and a compliance programme are established in 80% of organisations. Even though this number is quite high, there is still room for improvement. In line with regional and global results, the companies most frequently have a Chief Compliance Officer who takes care of the business ethics and compliance programme (51% in Slovakia, 38% in CEE and globally).

The crucial factor that contributes to economic crime being commit is simply the opportunity to do it (globally 69%). So the best way to prevent this opportunity is to strengthen the controls. To ensure that the company’s compliance and business ethics programme is effective, 84% of companies pursues internal audit, 49% pursues management reporting and 34% monitors whistleblowing hotline reports. Such reports actually include not only fraud suspicions, but also incidents on management compliance and/or other staff matters.
Companies expect spending for compliance programmes to be at the same level as in the previous 24 months. One fifth of Slovak companies expects some increase in spending.

When looking closer at how ethics and compliance are in-built in the corporate environment, 90% of the organisations surveyed responded that the Code of Conduct in their organisation covers key risks/policy areas and sets out the organisational values.

Understanding the employees’ needs and firm-wide communication are two of the essential features contributing to the effective compliance function. Our survey shows a positive highlight that, according to 92% of respondents, organisational values are clearly stated and understood and 57% of organisations provide regular training on the Code of Conduct and supporting policies.

81% of respondents are of the view that the leadership of their organisation conveys the importance of ethical business conduct and sets a positive example. This is what we call “the tone at the top setting the ethical climate of the organisation” and is a vital element of effective internal control.

Despite the growing emphasis on ethical values in corporate communications and the widespread adoption of business ethics and compliance programmes, companies may experience a disconnect between the tone at the top and the reality on the ground (both behavioural and budgetary), leaving organisations vulnerable to compliance breakdowns.

### Five steps on the way to a more effective compliance programme

- Ensure your programme is in line with corporate strategy; and communicate this alignment
- Evaluate and potentially reimagine the identity of your compliance function so it may adapt to an environment where risk and threats are ever-changing.
- Ensure that all owners of compliance obligations fully understand the compliance “big picture” across the organisation, and the scope of their own responsibilities within it.
- Remember that policies and training on values are not enough: credible, consistent engagement across the organisation is essential.
- Don’t downsize when risks are going up.
What are the most common compliance- and/or ethics-related challenges companies currently face?

The regulatory environment, particularly in the financial services industry, is becoming more and more complex due to new regulatory requirements, but also newly established regulatory bodies. Corporations are thus subject to almost on-going changes, for instance in the global sanctions area. Considering the risk of evolving landscape companies need to follow, they face increasing vulnerability to risk of non-compliance, should an effective compliance programme not be in place.

How has the companies’ compliance function changed in reaction to the evolving risks and challenges?

Nowadays we can find compliance officers not only in financial institutions and the Czech and Slovak subsidiaries of multinational companies, but also in purely Czech and Slovak companies or state-owned entities. This is really a good sign. Unfortunately, there is still a number of companies that consider the compliance function to be pure cost and burden, and try to limit it to a minimum. On the other hand it is not sufficient to tick “we set up the compliance function”. Yet primarily companies need to ensure that the compliance function has appropriate authorisation and it is a partner to the top management, whose responsibility is to provide full support to compliance matters.

Last but not least, it is critical that the compliance function works effectively. And what does this mean? It means you address evolving risks using a risk-based approach, set up a compliance programme across the organisation to mitigate the non-compliance risk; and have an escalation and reporting mechanism in place, for cases where attempt or case of non-compliance is identified.

How should an effective compliance programme work?

An effective compliance programme should take a risk-based approach based on a holistic understanding of the financial crime risk across the whole company and its weaknesses. On one side, you should mitigate the relevant risks and, on the other side, position the company to reach its business goals. The key prerequisite of an effective compliance programme is having the appropriate communication across the whole organisation and link it to the day-to-day operations in all locations. The compliance officer should ensure that the programme is practical and that the compliance team keeps its door open to any employees, at any organisational level, to provide clarification and respond to ad-hoc questions.

You, as compliance officers, should be aware that employees are mostly overloaded with information and employee turnover is, in certain industries, quite high. Consider embedding compliance topics in regular communication to your employees – firm wide, department wide, etc. As mentioned above, top management support is key. However, the most important is the middle management buy-in of the compliance programme. Middle management is in daily contact with your staff and thus they are the messengers and role models. If your staff sees that his/her boss is living and breathing compliance, they will follow him.

To conclude, can you give the typical reasons why the compliance- and/or ethics-related function fails?

As I mentioned earlier, it should not be a tick-the-box exercise. Even if compliance is a non-profit making function, it should not have a low priority. Rather, the other way round. Even if your firm needs to cut costs including headcount and training, you should not automatically cut the compliance function and its activities. This might be a strategic miscalculation. While risk and threats are ever-changing, the substance of a successful compliance programme is that it can foresee and address an evolving risk landscape. Please do not forget, your client-facing and back-office staff are your so-called first line of defence against financial crime risks. Thus, you should try to involve them in the compliance programme already in the preparation stage. Considering also regular communication with them and give them the feeling that you have your door open so they can express their concerns or pose questions feeling comfortable.
Future of economic crime – real state of economic crime versus perception of the risk

We also asked our respondents which types of crime companies expect to face in the next 24 months. We find it interesting to compare the perception of economic crime risks with the real occurrence. It seems that companies underestimate the risk of asset misappropriation in spite of its reported occurrence, perception of cybercrime affecting the company is higher than its actual occurrence.
About the Survey

The 2016 Global Economic Crime Survey was completed during August and September 2015. There were 6,337 respondents from 115 countries, including 89 respondents from Slovakia. Of the total number of respondents, 63% were senior executives from their respective organisations, 27% represented listed companies and 43% represented organisations with more than 1,000 employees. www.pwc.com/crimesurvey