Global Economic Crime Survey 2014
The Evolution of Fraud

Czech Republic
Contents

Preface

Main Findings

The Dangers of Crime

What companies do and do not

Economic Crime in the Czech Republic

Central themes

Managing fraud

Expectations

Contacts

Preface 5

Main Findings 6

The Dangers of Crime 6

What companies do and do not 7

Economic Crime in the Czech Republic 9

Central themes 9

Managing fraud 14

Expectations 19

Contacts 20
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.

The survey is intended not only to describe the current state of economic crime but also to identify trends and perception of future risks.
In Lewis Carroll’s Alice Through the Looking-Glass, the Red Queen is reported to say: “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 for the theory of evolution.

We can take Mr Carroll’s words as a very fine description of the development in 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 protect 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 Czech Republic and takes more diverse forms. Procurement fraud and cybercrime have gradually emerged as standalone major categories 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 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 and local variants for different countries 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 thankful to the 94 responding entities from the Czech Republic. All respondents share our belief that economic crime is too costly to ignore.
Main Findings

The Dangers of Crime

Crime around us. Economic crime is more common in the Czech Republic than we would like to think. 48% of respondents indicated their company experienced economic crime within the last 24 months. This is clearly above the regional and global average (38% and 37%, respectively). For the Czech Republic, this represents an increase by more than two thirds compared to the results of our previous survey from 2011. 44% of organisations who suffered economic crime estimated the resulting total financial loss to be USD 100,000 or more.

Crime evolves. Traditionally, asset misappropriation is the main observed type of crime (80%). However, fraudsters seek out new avenues from which to defraud their victims. The distribution of various types of economic crime is becoming more diverse, seeing an increase in the share of other types of crimes: cybercrime (31%), procurement fraud (29%), money laundering (27%), bribery and corruption (27%), mortgage fraud (24%).

Cybercrime Occurrence. Companies are more likely to suffer cybercrime than at any time in the past. Compared to the previous survey, cybercrime occurrence has more than doubled. In the previous survey, there were 6 companies reporting asset misappropriation (the most common economic crime) for each company reporting cybercrime. This year the ratio is 2.5:1.

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. Moreover, 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 29% of respondents that became a victim of economic crime. The top reported risk factor is the process of selecting a supplier.

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 complex data analytics to identify potential frauds or inefficiencies in procurement.

Corruption and bribery Risks of corruption. 27% of companies that experienced fraud reported bribery and corruption. In comparison with the last survey, this represents an increase by 6 percentage points. Corruption is seen as the greatest risk in doing business globally, both in terms of loss of reputation 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.
What companies do and not do

Remedial actions. Companies take strict measures against fraudsters. They usually do not hesitate to terminate the rogue employee when identified (91%). Quite often, law enforcement authorities are notified (46%) or a civil action is sought (36%). When fraud by an external subject is discovered, law enforcement authorities are usually notified (83%), the business relation is ceased (70%) or civil action is sought (65%).

Prevention and detection. Czech companies seem to rely on specific traditional methods of fraud detection while methods such as data analytics and reporting suspicious transactions play a less significant role. In addition, there is a relatively large number of crimes detected without active involvement on the part of the company. In total 42% of serious frauds were detected outside the corporate controls.

It would seem that there is room for improvement in terms of crime detection. Czech companies should definitely start thinking of increasing the efficiency of detection methods.

Methods of fraud detection usually fall into one of three categories: corporate controls, corporate culture, or actions beyond the influence of management.

GECS 2014 shows that the significant share of fraud in Czech companies (30%) was detected by fraud risk management which is significantly above the regional and global average (9% and 4%, respectively). However, the survey shows that other methods such as rotation of personnel, whistleblowing system or data analytics are not fully utilised in the Czech environment.

Literally, hundreds of thousands of records, scores of disconnected worksheets, many different systems... Where should the company begin? All the information one could possibly want is available but how to analyse it?

Although companies store and analyse more data than ever before, finding insights within the data are often difficult to achieve using traditional analytic methods. While spreadsheets are easy to prepare and understand, the ability to draw conclusions from the data diminishes as the volume and complexity of data grows.

Visualisation, or visual analytics, is the concept of using pictures, charts, diagrams and maps to reveal key relationships, communications, trends and patterns within large amounts of data. Some companies are starting to appreciate the power of visualisation to detect fraud and abuse; from detecting fictitious employees and conflicts of interest, to detecting inappropriate travel expense expenditures.
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.

Pavel Jankech
Senior Manager in Forensic Technology Services
Economic Crime in the Czech Republic

Central themes

Dangerous territory?
Since the previous survey, we have seen a steep rise in the number of reported economic crimes. In 2011, the number of Czech companies detecting frauds (29%) was below the regional and global average (30%, respectively 34%). This year, 48% of respondents indicated their companies had experienced economic crime in the past 24 months, well above the regional and global average (38% and 37%, respectively).

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.
Since our first global economic crime 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 13%. In line with our expectation (and predictions), the number of companies reporting cybercrime has increased significantly (reaching 31%) in the Czech Republic, even above the global average (24%).

This year, we added another new category – mortgage fraud, human resources fraud and procurement fraud. Potentially driven by the ongoing megatrend of outsourcing and organisational interconnectivity, procurement fraud received a significant response (29%), becoming the third most-reported type of fraud in the Czech Republic.

With an increase observed in each single reported fraud category, including the two other newly added categories of mortgage fraud and human resources fraud, it comes as no surprise that the overall number of organisations reporting economic crime in the Czech Republic has increased so dramatically.

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.
Cybercrime can be described as the most dangerous crime of this century. This is supported by:

- survey results on actual occurrence;
- survey results on perception of future threats; and
- the very nature of today’s business transactions and the increasing dependence on computer applications.

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.

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.

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.

Tomáš Kuča, Risk Assurance Partner leading our cyber security

**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.
Modern communication methods and new technologies are enlarging the perimeter that needs to be protected. Companies are dealing with environments that are not fully under company control.
**Procurement fraud**

For the first time, GECS 2014 included procurement fraud as a separate economic crime category. 29% of Czech companies which suffered fraud indicated that their companies experienced at least one instance of procurement fraud. This ranks procurement fraud as the third most common reported type of fraud in the Czech Republic. The reported high occurrence of procurement frauds exceeded even our expectations.

The most vulnerable point, both in the Czech Republic and globally, is the vendor selection process. This underscores even more the importance of knowing your business partners, a point we have emphasised in our last survey.

Generally speaking, when an organisation goes outside its walls for services, goods or assets, the potential for procurement fraud exists.

An increasing interconnectedness of business entities together with more common outsourcing make companies more vulnerable to procurement frauds than before. Moreover, there are numerous ways a procurement fraud can be committed. As a result, procurement fraud is one of the more difficult frauds to be detected and investigated.

**Corruption and bribery**

In recent years, corruption has become a topic of public discussion in the Czech 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 loss of reputation and monetary loss. In terms of occurrence, it is the fourth most noted type of economic crime in the Czech Republic (27%) and the third globally in GECS 2014 (27%). CEE are, along with Africa, the regions with the largest prevalence of corruption.

---

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, 16% respondents indicated their company has been asked to pay a bribe in the last 24 months. 35% of respondents believe their company has lost an opportunity to a competitor which they believe had paid a bribe in the same period.
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.

44% of respondents that experienced economic crime reported a total loss of at least USD 100,000. This represents a 6 percentage point increase compared with GECS 2011. 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 ways that a company could suffer besides losses that are purely financial. Consistent with the global results, companies would report a negative impact on corporate reputation as the greatest non-financial issue. However, the impact on employee morale shall be also considered.

In this respect, we would like to point out that a negative impact on employee morale might serve as a trigger to secondary actions (frauds 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 respondents’ companies had experienced.

There is an almost perfect balance between internal and external perpetrators (49% against 51%).

It should come as no surprise that middle to senior managerial persons are 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 who has spent 3 to 5 years in the company.

In the case of external perpetrators, the share of agents or intermediaries (22%) is higher than that of customers (17%) or that of vendors (9%).

Generally speaking, agents and intermediaries are entrusted by the victim company, they may have a detailed knowledge of the victim company’s procedures, and they work more or less independently so it is more difficult to oversee their work.

Therefore, we advise companies to think about procedures that can be used to prevent fraud from being committed by agents or to identify such fraud as soon as possible. One notorious example would be fraud orchestrated by agents of insurance or loan companies, sometimes being perpetrated by organised rings of fraudsters who infiltrated the company’s pool of agents. Background checks in justified cases might be a worthy option.

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 (86%).

At the same time, out of 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 results show that companies do not take economic crime lightly. It is encouraging that 40% of Czech organisations that reported economic crime have detected fraud via Fraud risk management or routine internal audit procedures. Similarly as with the 2011 results, this is significantly above the global average (11%).

On the other hand, there is still room for more directed actions. The share of data analytical methods (5%) is below the global average (13%). This suggests understated importance of IT detection systems within Czech organisations, although these systems can be a very cost-effective supplement to traditional methods, when employed correctly.

Numbers are rounded to the nearest whole number.
The first reaction of most companies in the Czech Republic when a potential fraud is detected is to resort to internal investigations (80%). In many cases companies are also seeking specialised advice from external legal advisors (22%). The survey indicated that Czech companies are more relying on their internal sources or legal counsel than engaging specialist forensic investigators (only 11% compared to 20% globally) or consulting the case with their auditor (9% Czech Republic, 21% CEE region, 28% globally).
**Remedial actions**

The survey indicated a clear stance by most companies against fraudsters, both internal as well as external. The occurrence of dismissals of internal perpetrators (91%) is even higher than in the previous survey (81%) and in the 2009 survey (65%).

This would suggest a better awareness of companies that fraud is costly. Especially in times of economic turmoil, there are few reasons to take fraud lightly.

With an external perpetrator, dismissal is obviously not an option. However, 70% of Czech organisations did cease a business relationship in response to an external fraud perpetrator. It is also encouraging that the occurrence of law enforcement notifications is rather high (83%), well above the global average of 61%.

---

**Remedial actions against internal perpetrator**

---

<table>
<thead>
<tr>
<th>Action</th>
<th>CZ</th>
<th>CEE</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal</td>
<td>73%</td>
<td>79%</td>
<td>91%</td>
</tr>
<tr>
<td>Law enforcement notified</td>
<td>46%</td>
<td>51%</td>
<td>49%</td>
</tr>
<tr>
<td>Civil action was taken, including recoveries</td>
<td>36%</td>
<td>43%</td>
<td>44%</td>
</tr>
<tr>
<td>Nothing</td>
<td>9%</td>
<td>14%</td>
<td>5%</td>
</tr>
<tr>
<td>Notified relevant regulatory authorities</td>
<td>5%</td>
<td>21%</td>
<td>25%</td>
</tr>
<tr>
<td>Warning/reprimand</td>
<td>5%</td>
<td>19%</td>
<td>17%</td>
</tr>
<tr>
<td>Transfer</td>
<td>0%</td>
<td>7%</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
<td>6%</td>
<td>4%</td>
</tr>
</tbody>
</table>
Expectations
We also asked which types of crime companies expect to face in the next 24 months. The following data depend on the perception of risks by the companies. This is not the same as the real extent of the 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.
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.kohoute@cz.pwc.com

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

Kateřina Halásek Dosedělová  
Senior Manager, Forensic Services  
+420 251 151 293  
katerina.halasek-dosedelova@cz.pwc.com

Jiří Urban  
Senior Manager, Forensic Services  
+420 251 151 627  
jiri.urban@cz.pwc.com

Filip Volavka  
Senior Manager  
Forensic Technology Solution  
+420 251 151 269  
filip.volavka@cz.pwc.com