www.pwc.com/crimesurvey

Economic Crime:

A Threat to Business Globally

Hungarian country report
February 2014

pwc

www.pwc.com/hu/crimesurvey

Contents

Global Economic Crime Survey 2014 was carried out by PricewaterhouseCoopers. It is the largest survey of its kind with over 5,000 survey participants from over 100 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.

Preface

We are pleased to present to you the Hungarian results of the 2014 PwC Global Economic Crime Survey.

This is the seventh time we have prepared the global survey and the sixth time we have published a Hungarian country edition. This survey describes the current state of economic crime and also identifies trends and perception of future risks. To provide a more comprehensive overview of these topics, we also included global and regional data.

With over 5,000 responses from senior executives from around the world, including 91 Hungarian companies, this is the most comprehensive global survey of economic crime available to businesses.

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.

Our survey supports this observation: economic crime is common in Hungary and is taking 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.

The results have also shown that the costs of economic crime and asset misappropriation are rising, and bribery and corruption remain the two most widely experienced types of economic crime in Hungary.

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 organisations do 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 91 respondents from Hungary. All respondents share our belief: economic crime is too costly to ignore.

Miklós Fekete
Partner,
PwC Hungary

George Surguladze
Senior Manager,
PwC Hungary

Main Findings

The Dangers of Crime

Crime around us

Economic crime continues to be a serious issue affecting organizations in Hungary, and no industry is immune.
Our survey indicates that approximately 1 in 4 Hungarian organisations (26%) reported having experienced one or more instances of economic crime in the last two years.

In our experience, many cases remain undetected, and it would be extremely difficult for organisations to uncover all instances of fraud, especially if the organization does not make available anonymous ways to report economic crime and/or does not perform fraud risk assessments regularly.
Fifty-eight percent of respondents reporting fraud estimated the total financial loss of their company due to economic crime as being between USD 100,000 and USD 5 million.

Crime evolves

Traditionally, asset misappropriation is the most frequently observed type of crime (63% of companies). However, fraudsters are seeking out new avenues for defrauding victim companies. The distribution of various types of economic crime is becoming more diverse, companies are seeing an increase in the share of other types of crimes: cybercrime (17% of companies), procurement fraud (25%), money laundering (25%), bribery and corruption (38%).

Cybercrime

Occurrence

Companies are more likely to suffer from cybercrime now than at any time in the past. In the previous survey, there were approximately 12 companies reporting asset misappropriation (the most common economic crime) for each company reporting cybercrime. This year the ratio is four to one.

Risks of cybercrime

Business operations are relying more and more on network applications. This increases the potential impact of cybercrime.

High latency

Moreover, cybercrime is dangerous as the victims may not be aware it is happening. The latency (share of undetected occurrences) of, for example, IP theft must clearly be many times higher than the latency of cash theft.

Therefore, the real occurrence is most probably significantly higher than reported.

Procurement fraud

Occurrence

Procurement fraud emerged as a standalone category of fraud, having been reported by 25% of respondents. The top reported risk factor is the process of inviting and selecting vendors.

Risks of procurement fraud

Procurement fraud usually includes collusion between parties. Therefore, the detection of this type of fraud is often difficult. However, there are ways to mitigate the risks.

Corruption and bribery

Risks of corruption

Corruption is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss. This finding is also in line with PwC 's Global CEO Survey, according to which corruption and bribery is the highest scoring threat to business growth.

What Hungarian companies do and do not do

Remedial actions

The picture is somewhat ambiguous with respect to measures taken against fraudsters. In the case of internal perpetrators, quite often, the law enforcement authorities are notified (70%); civil action is also often taken (60%) – these results exceed both CEE and global averages. But at the same time, internal perpetrators were dismissed in only half of the cases (50%) reported in Hungary which is below regional (78%) and global averages (79%).

When fraud by an external subject is discovered, the law enforcement authorities are notified only in the half of the cases (50%); civil action is also sought (57%). But business relations are discontinued in only approximately a third of all instances.

Prevention and detection

There does not seem to be a clear pattern in terms of how fraud is detected in Hungary. Methods such as data analytics and suspicious transaction reporting do not play a dominant role in fraud detection.

It is also evident that there is room for improvement in terms of crime detection methods.
Hungarian companies should definitely start thinking of increasing the efficiency of detection methods based on computer analysis.

Tens of thousands or more of records, hundreds of disconnected worksheets, many different systems... Where should a 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, it is often difficult to gain insights within the data using traditional analytical 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.
Many companies are now using the power of visualisation to detect fraud and abuse; from detecting fictitious employees and conflicts of interest, to detecting inappropriate travel expense expenditure.

Digital footprints

We asked Pavel Jankech, Senior Manager in Forensic Technology Services, for his thoughts on prevention and detection techniques

- Do you think that the measures that companies use against fraud are sufficient?

Currently, companies use primarily preventative measures to combat fraud. This, however, increases the risk of fraud remaining undetected for longer. The impact of such fraud can be really serious, and it's not just a pure financial loss. Also at risk is reputation, employee morale, or business relationships with suppliers.

- What would you recommend to companies?

Robust control environment is an absolute necessity. Nevertheless, it is never 100% bullet proof, so we recommend that companies also implement detection mechanisms, such as regular data analytical tests or implementation of a continuous fraud detection system. Using detection measures will help identify fraud earlier and thus reduce losses.

- What data test do you have in mind?

Traditional methods seek to identify suspicious transactions (red-flags) through rules-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 high cost of manual investigation. Moreover, these rules are already well known, so the fraudster can easily avoid them.

- How can a company avoid those limitations?

In our experience, each of the different types of fraud leaves a "footprint" in the data. Using advanced analytical techniques and visualization can identify different patterns of behavior 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 available?

These are advanced statistical methods or data mining techniques. These can help identify hidden patterns in the data behavior. Each of the patterns indicates the behavior of the supplier or user, and is compared with standard behavior in the dataset. Unusual or anomalous patterns indicating fraud are subsequently investigated. Using a combination of techniques for the visualization of data and detailed knowledge of the company, the investigation should focus just on unusual or anomalous behavior. 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 specifics of the company and its business and its existing control environment to identify key risk areas for fraud.
Based on those we would define 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.

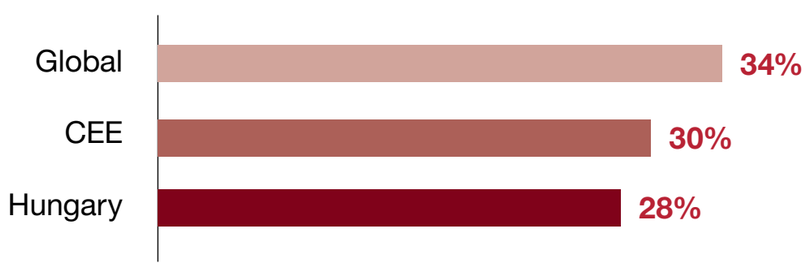
Economic Crime in Hungary

Central themes

Safer than CEE?

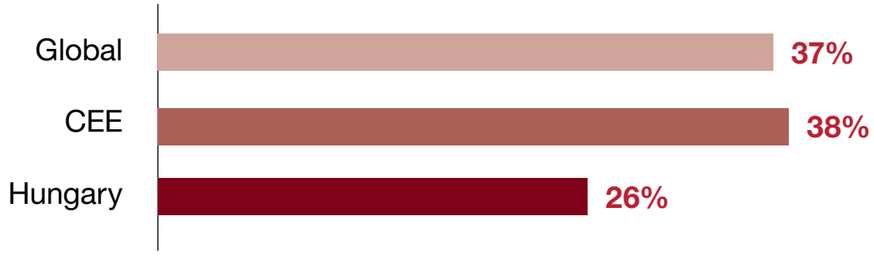
We have not seen a material change in the reported economic crimes since the previous survey. In 2011, the number of Hungarian companies detecting fraud was somewhat below the regional and global average.

Shares of companies experiencing economic crime: GECS 2011



This year, similar to 2011, approximately a quarter of respondents indicated their companies detected economic crime in the past 24 months, more than 10 percentage points below the global and regional average (37% and 38% respectively).

Shares of companies experiencing economic crime: GECS 2014



Note:

GECS 2014 asked participants to describe their experience with economic crime in the previous 24 months whereas GECS 2011 asked about the 12-month experience of the survey participants.

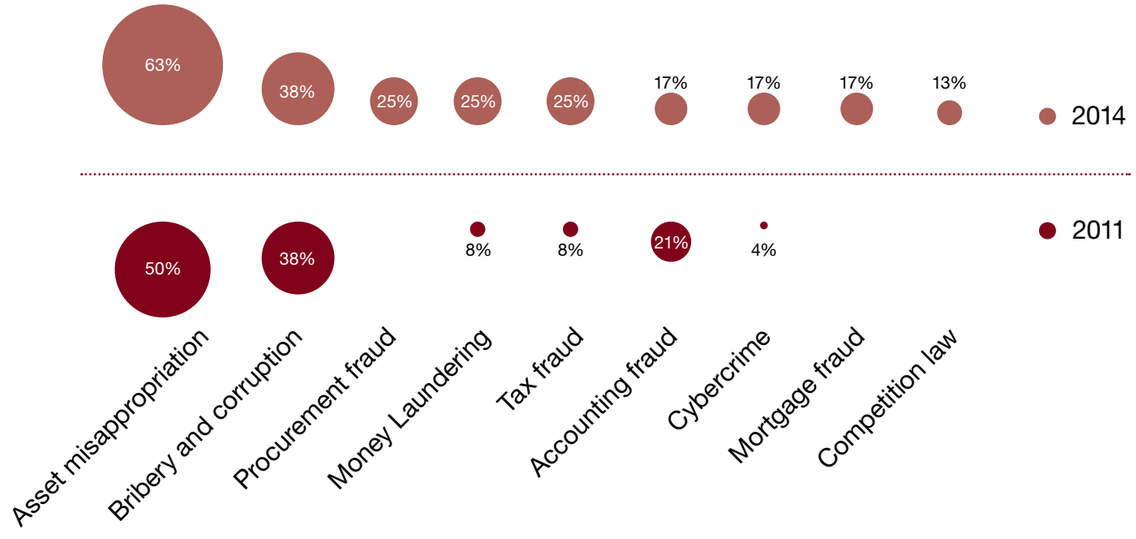
High diversity in economic crimes

Asset misappropriation remains the traditionally most common and most simple type of crime. Yet it is clear that attacks against corporate assets can take diverse forms.

It is 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-going schemes which were detected by the victim company by accident.

Therefore, companies should consider different fraud schemes they may be facing. Control over cash and other physical assets might not be enough.

Economic crimes as reported by companies



Note:

procurement fraud, mortgage fraud and competition law abuses were not included in GECS 2011 as separate categories. Less frequent types of crime omitted for clarity.

Cybercrime

Compared to the previous survey, the share of respondents experiencing cybercrime increased to 17% from about 4%.

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

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

Cybercrime might take completely new forms, previously unheard of, or find room for old types of fraud in the network environment, e.g. theft of working time and bandwidth (malware used for distributed denials of service; there was no equivalent in pre-computer times) and now Bitcoin scams using fake marketplaces (an old fraud in a new environment, where the users may not always recognize the hazards). This increases the general risks of cybercrime.

About a third of respondents indicated that their perception of cybercrime risks has increased over the last 24 months. This is a significant increase compared to our 2011 survey, according to which only 14% of Hungarian respondents commented that their perception of cybercrime risk had increased.

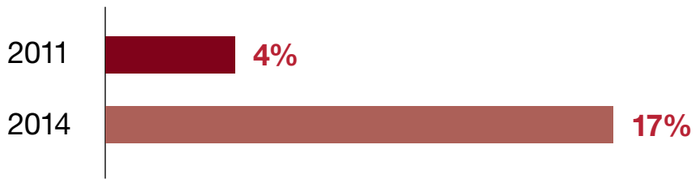
Our survey suggests that theft of intellectual property, personal data, reputational damage and service disruption are of the greatest concern when it comes to cybercrime.

While globally 30%, and in the CEE 26% of respondents believe that their organisations will likely face cybercrime in the following 12 months, in Hungary only 16% of respondents believe so.

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

This is also a reason for a shift in the security paradigm: 90s - respond after the breach, 00s - get ready for the breach, 10s - assume the breach has happened or is underway. It is not a question whether the company will be subject to cyber-threat, but when and how it will happen.
Successful companies are prioritizing in what matters most - guarding their crucial data against organized attackers who target intelligently in a global business ecosystem consisting of fluid data moving around internally as well as to/from business partners and other stakeholders.

Hungarian companies experiencing cybercrime



Procurement fraud

For the first time, GECS 2014 included procurement fraud as a separate category of economic crime. 25% of respondents indicated that their companies experienced at least one instance of procurement fraud. This was globally the second most frequently indicated economic crime. The most vulnerable point, both in Hungary and globally, is the vendor selection process.

The reported high occurrence of procurement fraud exceeded even our expectations. There are numerous ways how procurement fraud can be committed. As a result, procurement fraud is one of the more complex fraud to be detected and investigated. As the detection of procurement fraud is difficult, it is possible that the actual occurrence is even higher. The impact of such fraud can be severe, and financial loss is often not the most damaging aspect. Employee morale, relationships with business partners or company's reputation are all at risk.

With only preventative measures in place, there is a higher risk that a determined fraudster can operate undetected for longer. Employing additional detective measures can help identify fraud earlier, resulting in reduced loss.

Corruption and bribery

Corruption is seen as the greatest risk in doing business globally, both in terms of reputation loss and monetary loss.

According to this survey, in terms of occurrence, corruption and bribery is the second and third most frequently indicated type of economic crime in Hungary and globally respectively. Central and Eastern Europe is, along with Africa, the region with the largest prevalence of corruption.

This is also in line with the findings of PwC's CEO Survey, which indicated that corruption awareness is on the rise; more than half of the CEO's surveyed say they are concerned or very concerned about corruption as a threat to their organisations.

Almost one in five Hungarian respondents indicated that their company was asked to pay a bribe in the last two years. One in three Hungarian respondents believe that their company lost an opportunity to a competitor which they believe had paid a bribe during the same period.

Share of corruption and bribery in total fraud reported

Impact of economic crimes

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

It is very difficult to accurately estimate the financial impact of economic crime. However, we asked our respondents to estimate, to the best extent possible, the cost of fraud and economic crime, they have suffered. 58% of respondents reporting fraud estimated the total financial loss of their company due to economic crime as being between USD 100,000 and USD 5 million.

This is an increase compared to 42% per our 2011 survey and exceeds both the regional and global results (43% and 38%, respectively).

There are also other negative impacts on the company besides purely financial losses. Consistent with both the previous Hungary results and the global results, the companies report an impact on employee morale as the greatest non-financial impact.

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

Managing fraud

Who commits fraud

We tried to make a profile of the perpetrator of the most serious economic crime the respondents' companies had experienced.

The responses indicate that in the majority of Hungarian cases, parties external to the organisation are the main perpetrators of economic crime (58%). Vendors and customers represent the bulk of external perpetrators. Fraud committed by vendors (21%) is nearly double the regional (11%) and global (10%) average. This is also consistent with the fact that procurement fraud was the third (together with money laundering and tax fraud) most frequently experienced type of economic crime in Hungary.

Our view has not changed since our last survey. Namely, based on our experience, due to a lack of resources, some organisations tend to neglect the importance of background checks on their business partners. This can lead to, in many cases, organisations not having a clear picture of the past business history and reputation of their business partners. If corporate intelligence/background checks of external parties (vendors, agents, intermediaries, etc.) are not performed, questionable business ethics cannot be identified in time, and the organisation can become a victim of economic crime.

We recommend that organisations step-up their efforts in this area. As a key prevention measure, knowing your business partners prior to engaging with them is less costly than dealing with the unpleasant consequences.

According to the surveyed companies, the share of fraud performed by internal perpetrators is 42% which is in line with 46% for CEE. The responses indicate that middle and senior managers are more likely to commit fraud than junior staff members, which is also in line with the findings for the CEE and globally. The most typical internal fraudster is a male, 31-40 years old, who has spent three to five years in the company.

Prevention of fraud

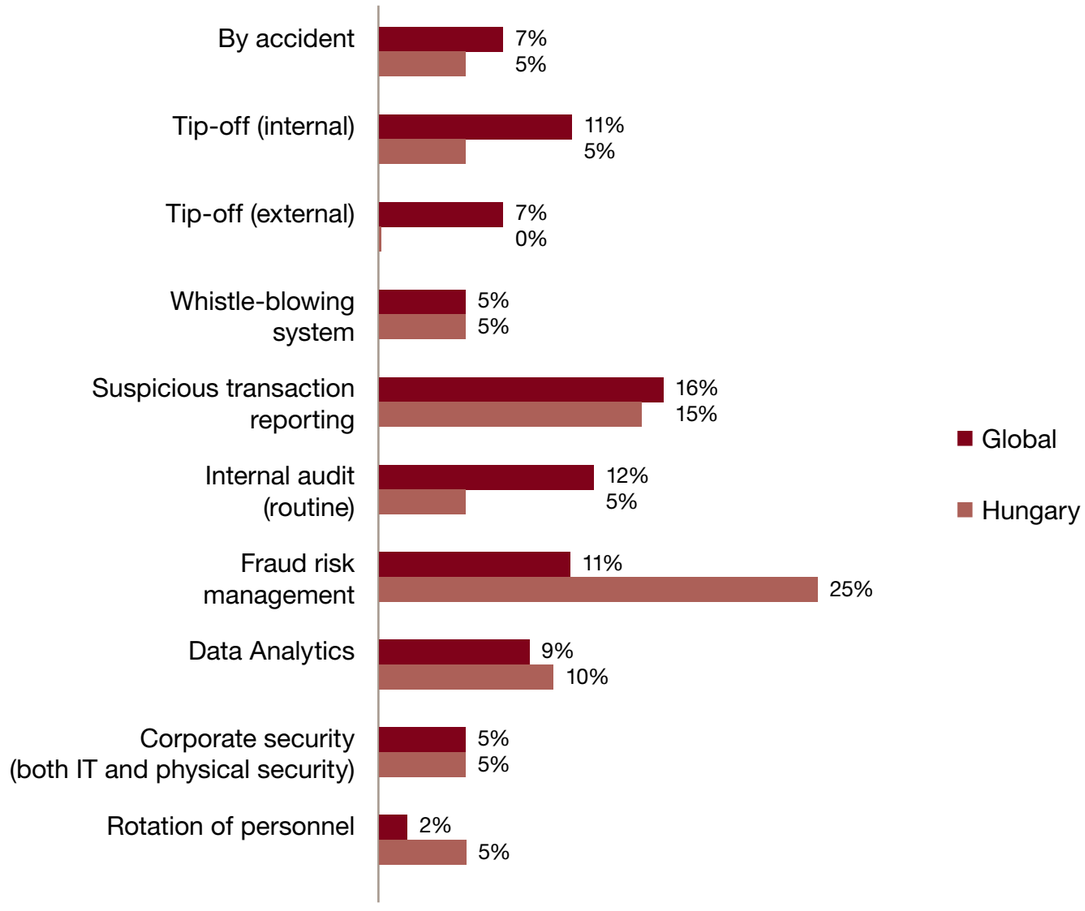
Why would someone decide to commit fraud? Our survey indicates that, by far, the most significant contributing factor for internal fraudsters is simply opportunity.

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

Companies do not take economic crime lightly. It is encouraging to see that there are responsible corporate executives who are not leaving the detection of economic crime to chance. They use proactive methods such as fraud risk management (25%) and suspicious transactions reporting (15%). Proactive identification and detection of economic crime are the most powerful tools in the fight against fraud.

Method of detection of the most serious economic crime



On the other hand, there is still room for proactive actions. Data analytical methods could be used more often as these techniques can be a very cost-effective supplement of traditional methods, when employed correctly.

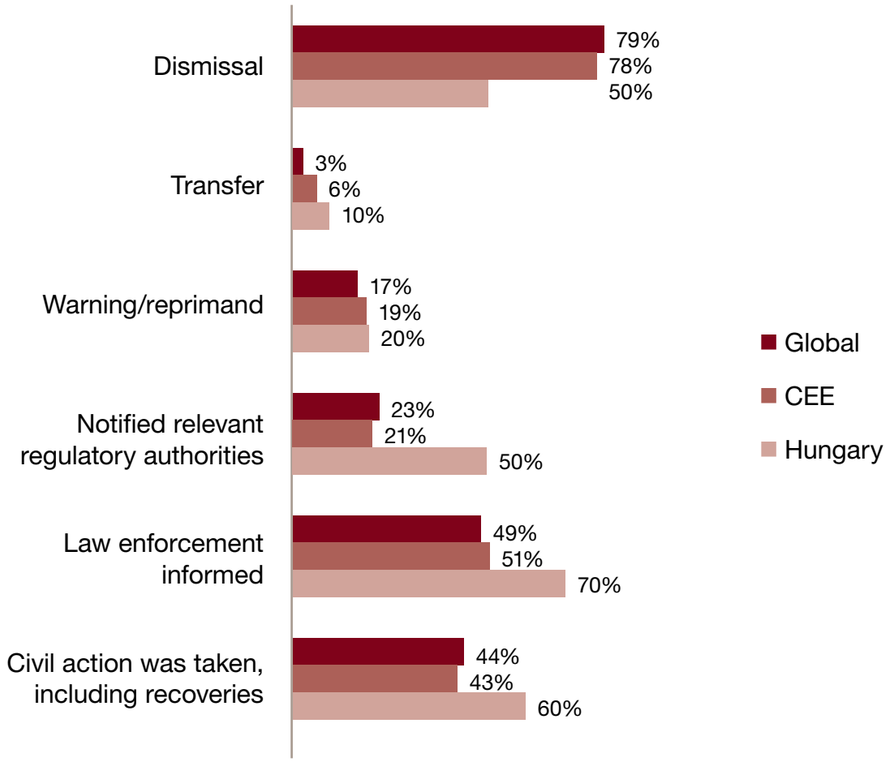
And what's the first reaction of a company when potential fraud is detected? Most companies resort to internal investigation.

Initial measures taken

Remedial actions

Compared to our 2011 survey, we see that companies are taking a tougher stance against fraudsters. Namely, this time we did not have any companies indicating that no action was taken against internal perpetrators of fraud, whereas in 2011 almost a quarter of companies reported that no action was taken. Also, it appears that Hungarian companies are more prone to start civil action and turn to law enforcement agencies or regulatory authorities than their peers in the region or globally. 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.

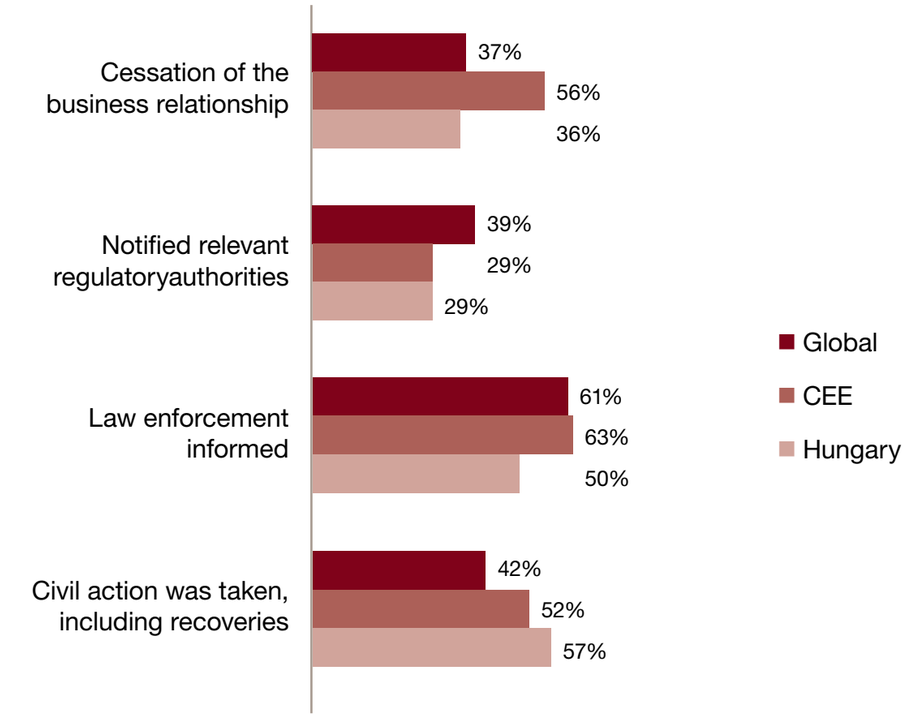
Actions against main internal perpetrator



But at the same time (in line with our 2011 survey results) only about half of the companies reported that internal perpetrators were dismissed; this is lower compared to almost 80% reported regionally and globally.

With an external perpetrator, dismissal is obviously not an option. It appears that Hungarian companies prefer to take civil action including claiming damage compensation more than their regional or global peers. Terminating business relationships or involving law enforcement agencies is not as popular among Hungarian companies as in the case of regional companies.

Actions against main external perpetrator



Who responded

Our survey was conducted in fall 2013, with the participation of 91 companies from Hungary.

The study was not focused on a specific type of organization. The respondents were from all sizes and types of companies, ranging from purely local companies (38%) to truly global ones (26%).

Among the respondents there were CEO's (34%), CFO's (21%), heads of departments (20%) and general managers (13%). Their principal functions included mainly executive management (34%), finance (31%) and compliance (10%).

We would like to once again thank our respondents for all the information they volunteered and all the thoughts they shared.

Contacts

Miklós Fekete
Partner
E-mail: miklos.fekete@hu.pwc.com
Tel.: +36 1 461 9242

George Surguladze
Senior Manager
E-mail: george.surguladze@hu.pwc.com
Tel.: +36 1 461 9127

pwc

www.pwc.com/hu/crimesurvey