http://www.pwc.com/hu/en/crimesurvey

Underestimated threats?

Global and Hungarian Economic Crime Survey 2016

pwc

46%

The most common type of economic crime in Hungary is asset misappropriation.

17%

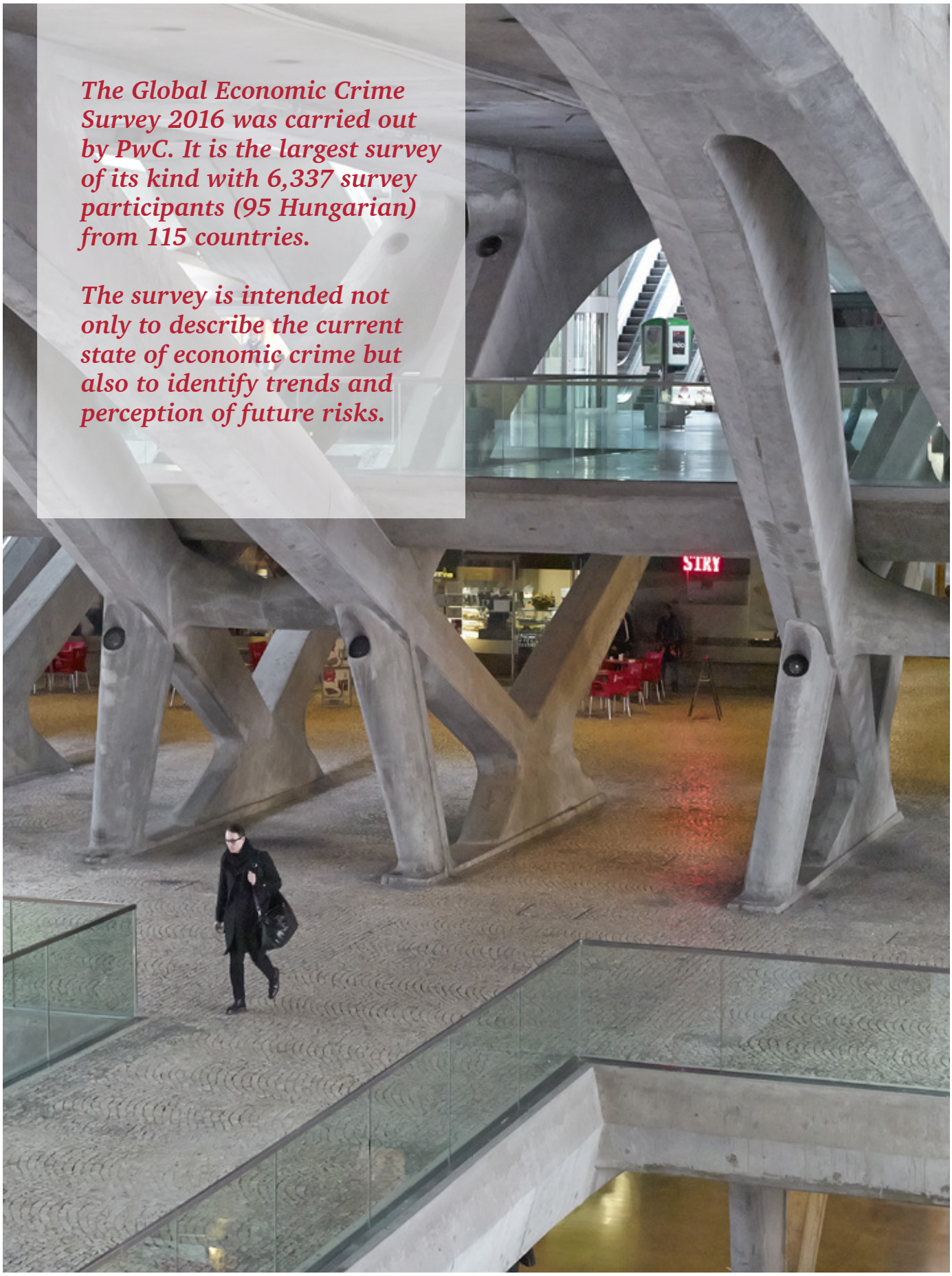
Less than one-fifth of the respondents in Hungary that have suffered an economic crime reported that they were victims of cybercrime. This raises red flags that companies in Hungary might have been compromised without even knowing it.

76%

Three-quarters of the Hungarian companies surveyed said that their Code of Conduct covers key risks and policy areas, and sets out the organisation's values.

.

Contents



The Global Economic Crime Survey 2016 was carried out by PwC. It is the largest survey of its kind with 6,337 survey participants (95 Hungarian) from 115 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 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 organisations' awareness about economic crime we collected responses from 6,337 organisations from 115 countries, including 95 leading companies within Hungary.

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

This report also explores the theme of opportunity – not only the opportunities that enable economic crimes to be perpetrated, but more importantly the opportunities available to organisations to proactively counter this trend 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 on fraud and provide their insights. We are especially grateful to the responding entities from Hungary. All respondents share our belief that economic crime is too costly to ignore.

Dr. Csaba Polacsek

Executive Director
Advisory sevices

Tibor Hurton

Manager
Forensic services

The highlights

The current fraud environment in Hungary

- Economic crime continues to be a serious issue affecting organisations worldwide, across Central & Eastern Europe ("CEE") and in Hungary. In the past 24 months 25% of companies in Hungary have experienced one or more incidents of economic crime; which is slightly below the average for CEE (33%) and globally (36%).
- Compared to the previous survey, the reported occurrence of economic crime remained at the same level, however this actually masks a worrying trend - in the context of an evolving risk landscape, organisations might face sophisticated fraud schemes which run undetected for several years. These latent and long-running fraud cases represent the most dangerous and costly threats for the companies than one-off incidents.
- As, traditionally, the most common type of economic crime in Hungary remains asset misappropriation (46%). Asset misappropriation has been traditionally seen as the easiest to detect compared to other types of economic crime, thus its prevalence from year to year is generally predictable.
- Apart from asset misappropriation, the top four types of economic crime reported by our survey participants include bribery and corruption (38%), tax fraud (21%), cybercrime (17%) and procurement fraud (17%).
- Most of the fraud in Hungary is detected by various means of corporate controls (in total 42%). However, still almost one in five fraud cases is detected beyond the influence of management (21%).
- According to the 2016 survey the share fraud is heavily weighted toward of internal perpetrators (46%) compared to external perpetrators (33%).

Cybercrime

- Seventeen percent of the respondents in Hungary that have suffered an economic crime, reported that they were victims of cybercrime. This is slightly below the CEE (22%) and suspiciously lower that the global (32%) average. If there is one take away from this survey it is the change in perception of cybercrime – cybercrime is no longer just an IT problem, it should rather be considered a fundamental business problem.
- Compared to our last issue of the survey the occurrence of cybercrime remained at the same level (17%) in Hungary, whereas globally this figure is sharply higher (32%). This is surprising and raises red flags that companies in Hungary might have been compromised without even knowing it. Increased awareness is needed in a changing business ecosystem in which the vast majority of documents, communication and transactions has gone digital.
- According to the survey, 55% of surveyed organisations think the risk of cybercrime remains the same. This underlines the risk of underestimating cybercrime threats in Hungary.

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

Ethics and Compliance

- According to our survey, corruption and bribery are the second most common type of economic crime in Hungary. At the same time our survey participant reported that 11% 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 the global average (13%). The current number for Hungary represents a significant drop compared to the previous issue of the survey (19%). There is no clear explanation for this decrease. Based on our experience corruption and bribery is a type of economic crime that is rather difficult to detect.
- One positive message is that more than 81% of survey participants have a formal business ethics and compliance programme which is in line with the CEE and global average (identically 82%).
- Seventy-six percent of the organisations surveyed responded that the Code of Conduct in their organisation covers key risks / policy areas and sets out the organisational values. And 88% of respondents report that organisational values are clearly stated and understood. Sixty percent of organisations regularly provide training on their Code of Conduct and supporting policies. As understanding of the employees and firm-wide communication are important features contributing to effective compliance, these relatively high reported numbers appear optimistic.

Economic Crime in Hungary

How many organisations experienced fraud in the last 24 months?

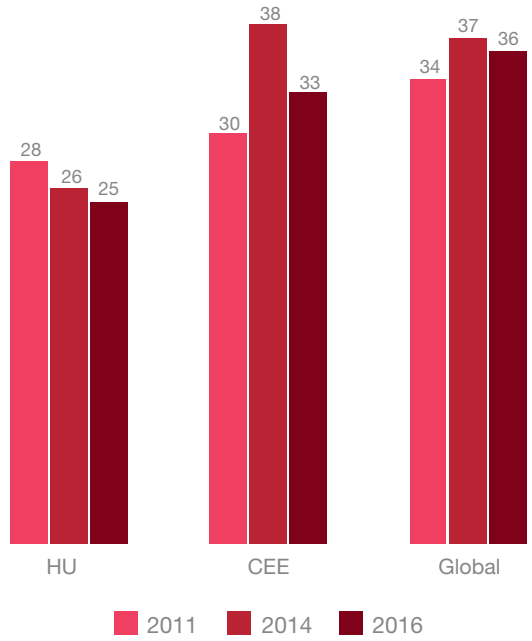
More than a quarter of Hungarian organisations have experienced economic crime in the past 24 months, as reported by the respondents to PwC's Hungarian Economic Crime Survey 2016. This year's results show that there is a decreasing trend of the occurrence of economic crime among Hungarian organisations. In the last seven years, occurrence of crimes in Hungary decreased from 30% to 25%. This year's Hungarian results show that the incidence of economic crime has declined marginally by 1%.

At first glance, this could be evidence of a return on the investments in preventative measures which organisations have been making over the past few years. But as we look at the data more closely, one could suspect this small decrease is actually masking a worrying trend: economic crime is changing significantly, and detection and controls programmes are not keeping up with the pace of change.

"In a rapidly evolving economic and technological environment, with the adoption of new business models, increasingly complex and sophisticated forms of fraud are emerging. The Hungarian results paint a more optimistic picture than global and regional figures about the incidence of fraud. This could be because some companies have been compromised without even knowing it, while others may be overconfident about the robustness of their existing control environment."

Tibor Hurton
PwC Hungary,
Manager
Forensic services

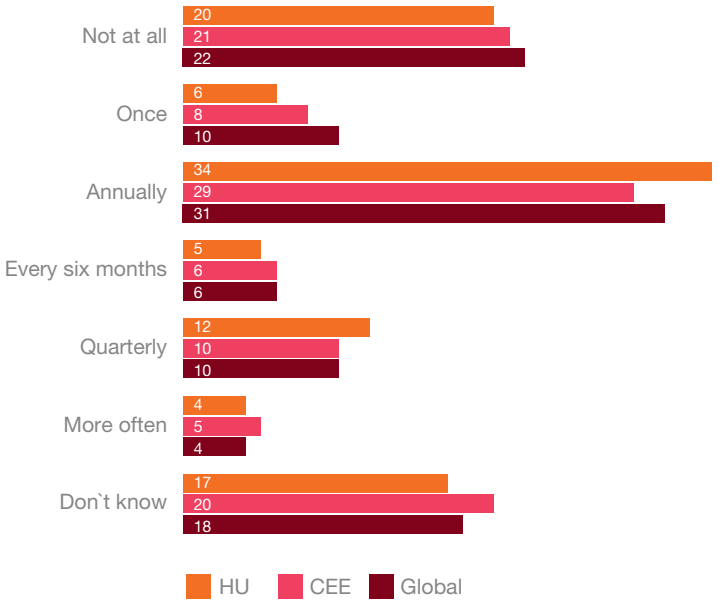
Has your organisation experienced any economic crime within the last 24 months? (marked "yes", %))



In the last seven years, the percentage of respondents in Hungary reporting incidences of economic crime has decreased from **30%** to **25%**

Despite this evolving threat, globally we have seen a decrease in the detection of criminal activity by methods within management's control, with detection through corporate controls down by 7%. What's more, 1 in 5 Hungarian organisations (20%) have not carried out a single fraud risk assessments in the last 24 months.

In the last 24 months, how often has your organisation performed a fraud risk assessment? (%)

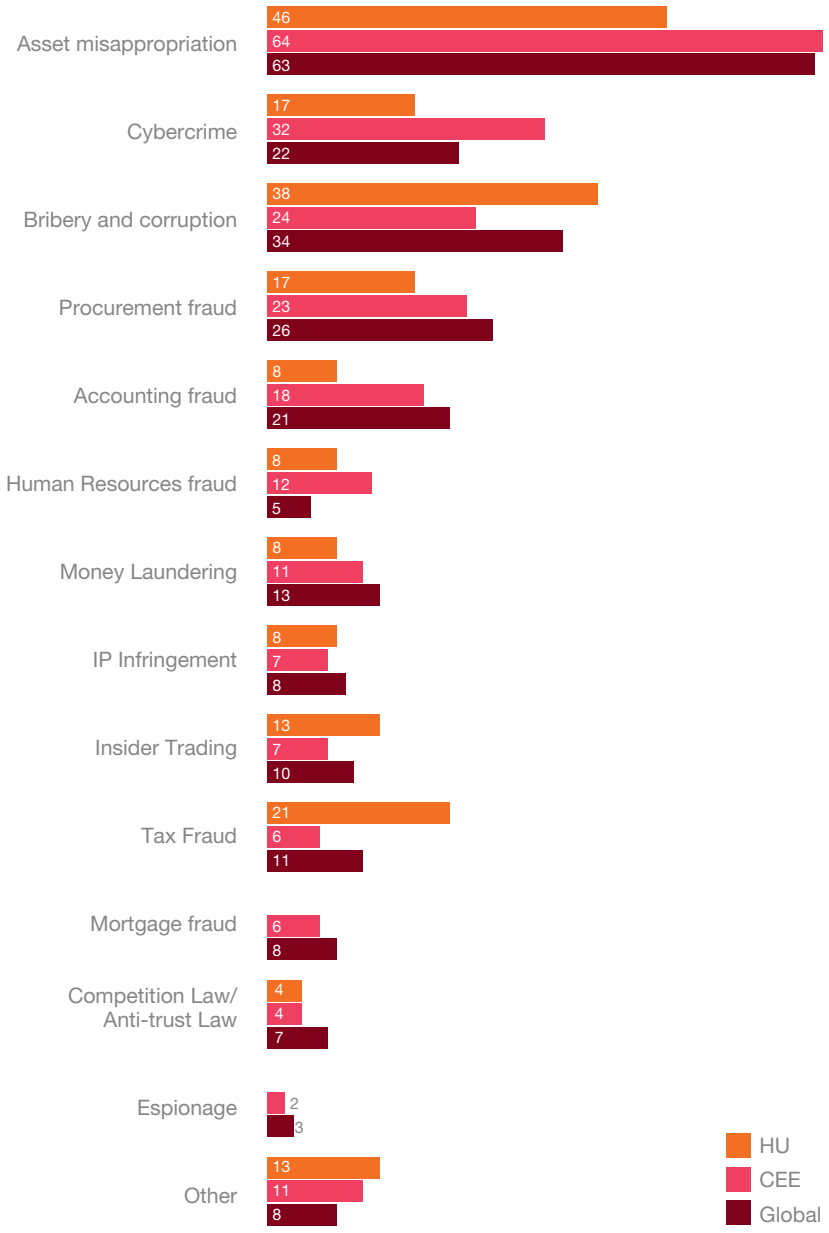


Types of economic crime in the region and Hungary

The results show that 64% of organisations who suffered economic crime have lost approximately USD 50,000 or more in the CEE region. Among the most frequent types of economic crime are asset misappropriation (63%), bribery and corruption (34%), procurement fraud (26%) and cybercrime (22%).

In Hungary asset misappropriation (46%), bribery and corruption (38%), tax fraud (21%) and procurement fraud (17%) are the traditional leaders in this category. Asset misappropriation showed a decrease this year over 2014's statistics, however it is still in first place in our survey year to year. This fact is generally predictable, because asset misappropriation is regarded as the easiest of frauds to detect.

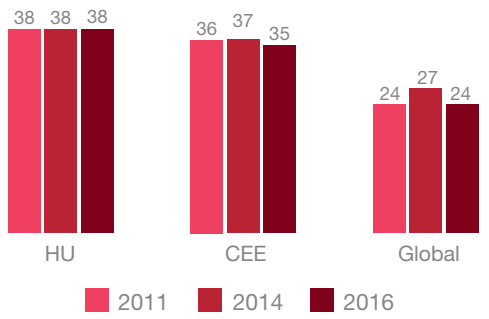
What types of economic crime has your organisation experienced within the last 24 months? (%)



Bribery and Corruption

Bribery and corruption (38%) is the second most common economic crime experienced not only in Hungary, but in the CEE region as well. In spite of a decrease in bribery and corruption in the CEE region and also globally, this type of economic crime has been significant and above CEE and global levels since 2009 in Hungary.

In the last 24 months, has your organisation meet with bribery and corruption? (%)



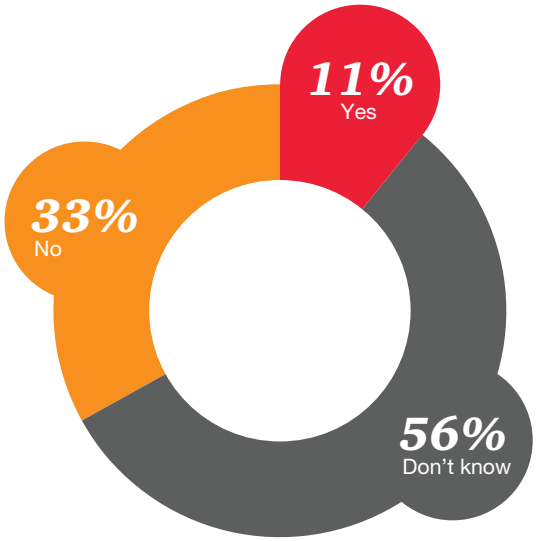
A contributing factor to an above-average level of bribery and corruption in Hungary might be that local management often has to deal with issues such as how to ensure that all their people are doing the right thing all the time.

How do organisations respond to this risk? Having a recognised Code of Conduct is a starting point, but if employees do not know how to use it in their day-to-day decision-making this does little to mitigate compliance risks. The code and other polices need to be embedded through training, regular communications, reward and recognition of where good decisions are made, and disciplinary procedures where bad decisions are made.

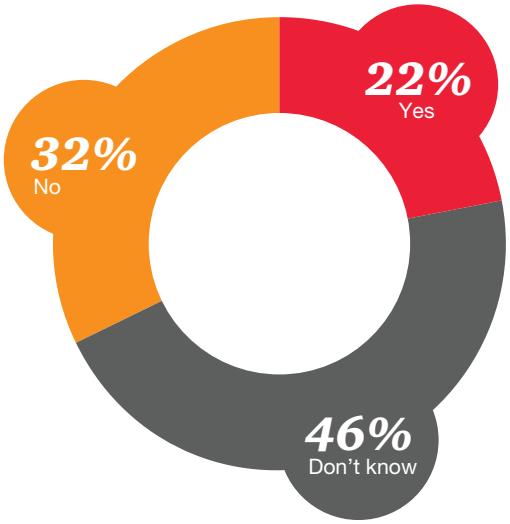
Although 81% of organisations in Hungary stated that their organisation had a Code of Conduct in place, only 60% said that training was provided regularly and supported by regular communication and advice.

Surveyed participants also reported that in the last 24 months their organisation was asked to pay a bribe (11% in Hungary) and also lost an opportunity to a competitor who paid a bribe (22% in Hungary).

In the last 24 months, has your organisation been asked to pay a bribe?



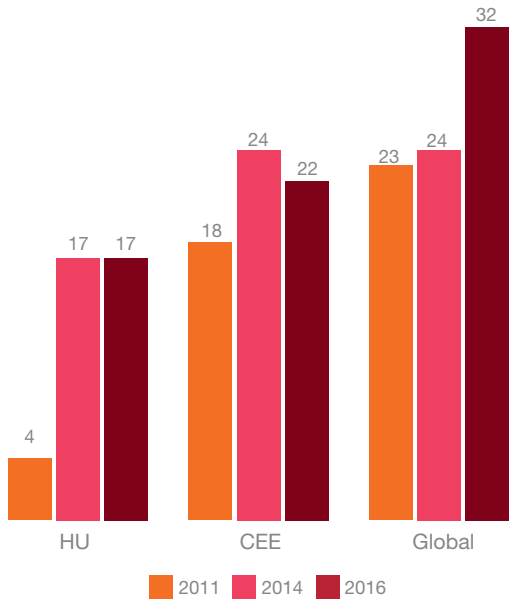
In the last 24 months, has your organisation lost an opportunity to a competitor which you believe paid a bribe?



Cybercrime

Cybercrime (17%) in Hungary shows the same level compared to our last survey in 2014. However the level of cybercrime globally has increased steadily since its debut in our survey back in 2011.

Cybercrime perception in the last 24 months. (%)



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 are, of course, not always quantifiable, and can over time dwarf the relatively shorter-term impact of financial losses.

How much does the fraud cost?

When considering the financial losses due to economic crime, the survey shows that 50% of Hungarian organisations that suffered economic crime have lost approximately USD 50,000 or more.

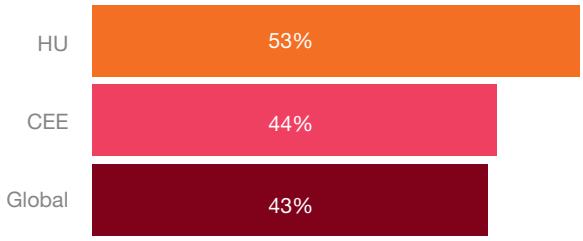
There may be various impacts of economic crime. The survey shows that in Hungary the biggest risk is the impact on employee morale, followed by damaged reputation (or brand strength) of an organisation. Negative impact on employees might serve as a trigger to other criminal acts.

Technology – an economic crime blessing or curse?

Digital technology continues to transform and disrupt the world of business, exposing organisations to both opportunities and threats. The reality in 2016 is that, like every other aspect of commerce, economic crime has, to some extent, gone digital. Here's the digital paradox: Companies today are able to cover more ground, more quickly, than ever before – thanks to new digital connections, tools and platforms which can connect them in real time with customers, suppliers and partners. Yet at the same time cybercrime has become a powerful countervailing force that's limiting that potential.

Nearly half of our survey respondents (43%, up 12% since 2014) see an increased risk of cyber threats, perhaps due to intensifying media coverage. But our survey suggests that companies are nonetheless inadequately prepared to face current cyber threats.

Perception that the risk of cybercrime has increased in the last 24 months.



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 USD 50,000 or more through cybercrime in the last two years.

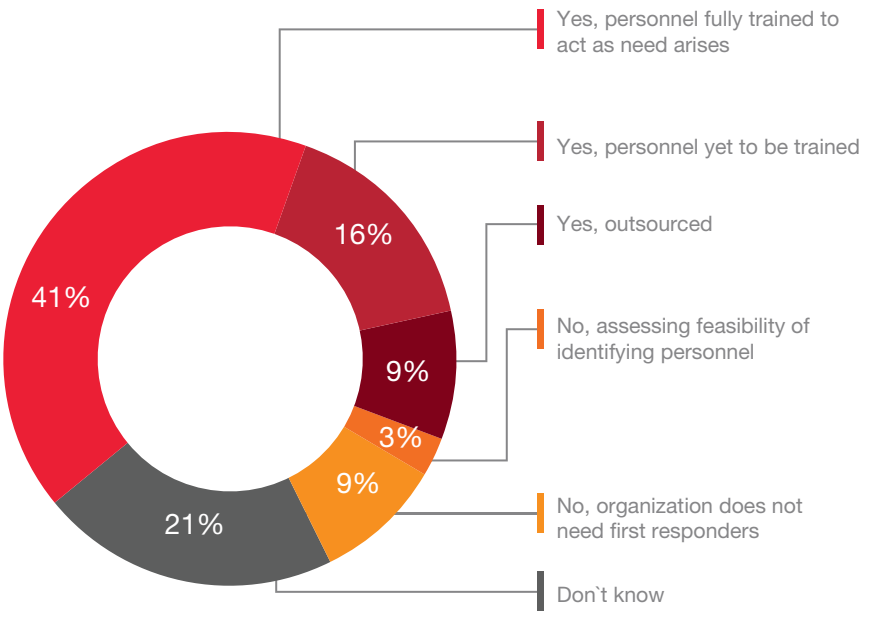
The survey revealed that 55% of Hungarian organisations see the greatest cybercrime threat coming from external perpetrators, 18% of them thinks it comes from both internal and external perpetrators and just 8% believe it comes from internal perpetrators only. This is perceived similarly globally and regionally.

Responsibility for redressing cyber vulnerabilities starts at the top. Yet our survey suggests that many boards are not sufficiently proactive regarding cyber threats, and generally do not understand their organisation's digital footprint well enough to properly assess the risks. Thirty-one percent of the respondents' organisations do not produce any information regarding the readiness of the organisation to deal with cyber incidents, 23% do not even know.

The same problem occurs with the incident response plan to deal with cyber-attacks. Only 42% of the surveyed organisations has such a plan fully in operation.

Should a cyber crisis arise, only four in ten companies have personnel that are "fully trained" to act as first responders – of which the overwhelming majority are IT staff .

Has your organization identified first responders who can mobilise within a short space of time should a technology breach occur?



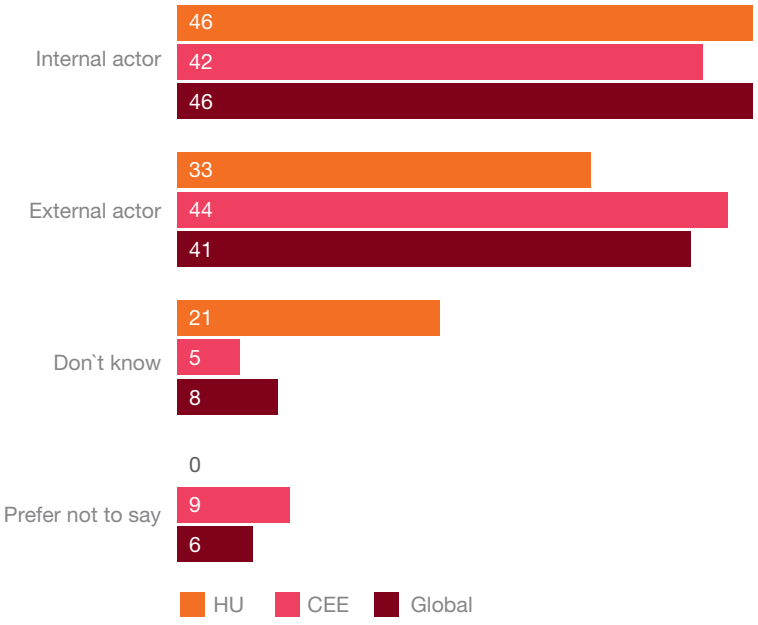
Profile of the fraudster

The typical fraudster could be internal or external. The survey shows that the perpetrator is more likely to be internal. The crucial factor contributing to internal fraudster committing economic crime is simply the opportunity or ability to do it (64%).

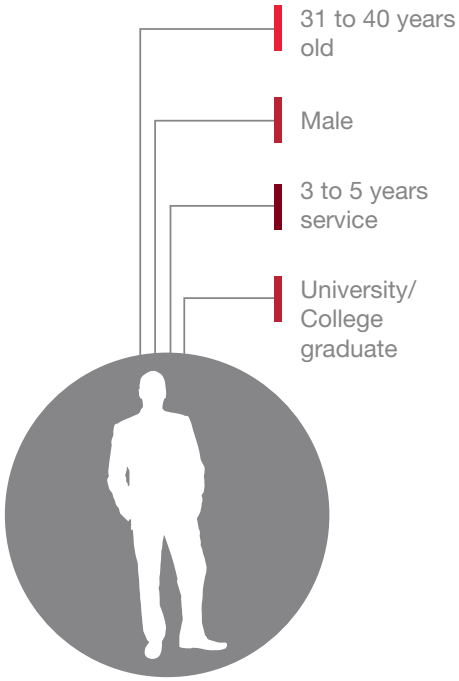
According to the CEE results from 2016, the internal perpetrator is mostly part of junior or middle management. The complete profile of an internal perpetrator obtained from all surveyed companies within the CEE gives us a male (72%) between 31 to 40 years (46%) old, working for the organisation for 3 to 5 years (40%, which is in line with the statement that the perpetrator would be from junior/middle management) and holds a university degree (47%).

If it is an external perpetrator, the CEE results show it would be very likely a consumer (34%). Consumers rank higher than agents/intermediaries (which increased form 12% in 2014 to 28% this year).

Thinking about the most serious (in terms of monetary loss) economic crime your organization experienced in the last 24 months, who was the main perpetrator of the fraud? (%)



Most likely characteristics of internal fraudster



Detection methods

It is a positive finding that an increasing number of fraud incidents is detected via systematic mechanisms: 42% of the Hungarian respondents reported that the fraud was detected by corporate controls (compared to 54% in the CEE and 47% globally).

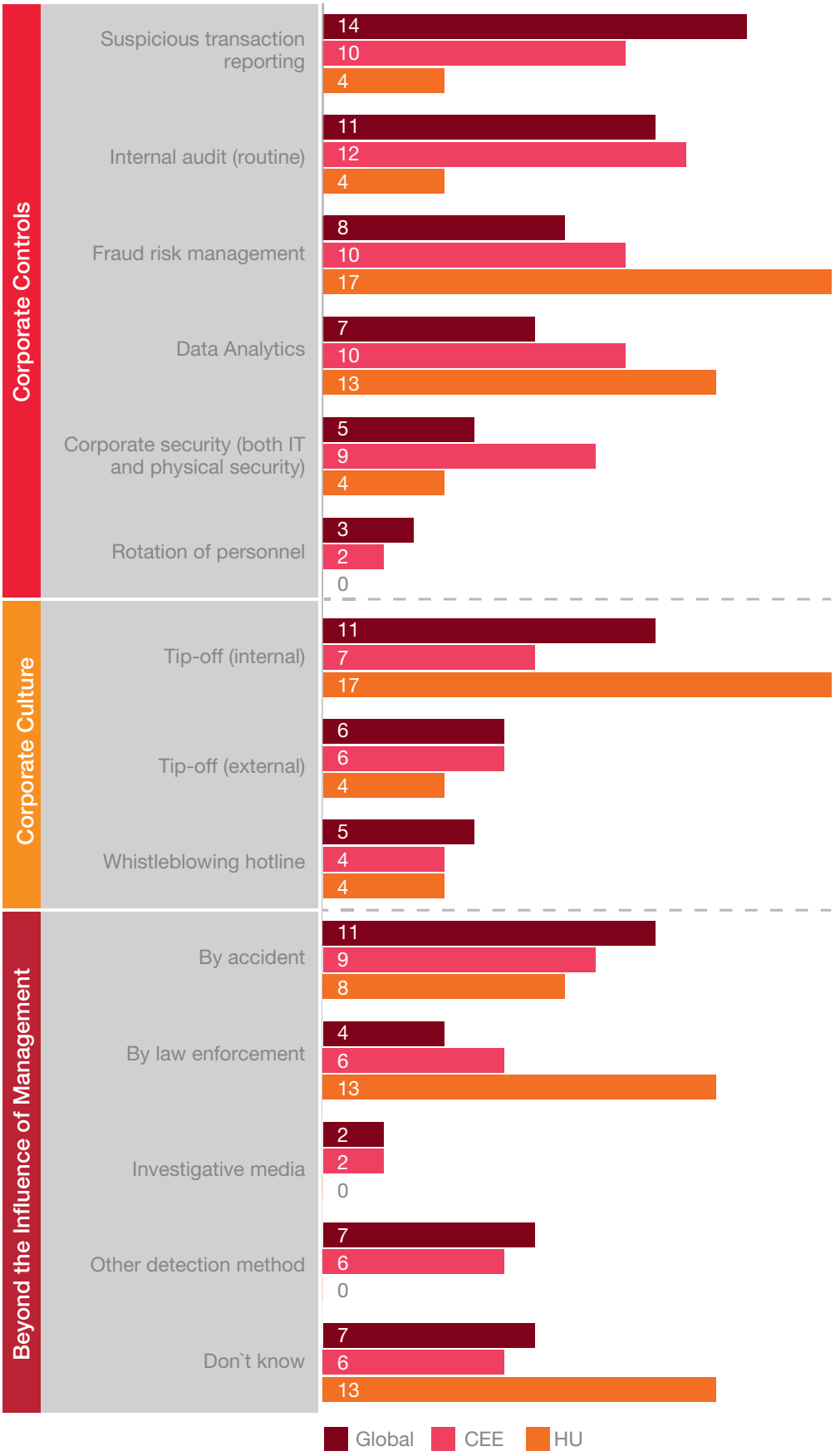
In particular, apart from "traditional" means of detection such as fraud risk management (17%) and internal audit (4%) we would like to highlight the increasing share of data analytics (increase from 10% in 2014 to 13% in 2016). Suspicious transaction monitoring (decrease from 15% to 4%) showing an alarming trend in Hungary. In a changing business landscape in which different fraud incidents make 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.

However, despite this encouraging result, this is no time to rest on our laurels. According to the organisations surveyed in Hungary, 21% of economic crime was still detected beyond the influence of management.

"Rapid detection of fraud is critical for companies to minimize potential losses. Technological advances offer new techniques to detect fraud and mitigate risks. These techniques include risk-based due diligence, focused fraud and corruption risk management, intelligent fraud monitoring, anonymous ways to report economic crime, and comprehensive fraud prevention measures."

Dr. Csaba Polacsek
PwC Hungary,
Executive Director
Advisory sevices

Thinking about the most serious economic crime your organization experienced in the last 24 months, how was the crime initially detected? (%)



Detecting a breach: Crisis management

What happens when you learn of a breach? It's critical to shrink the interval between effective detection and response — and interrupt damaging business impacts as quickly as possible. After calling up your crisis and cyber first responders, here are some steps you can take:

- Get the essential facts about the breach, and find out if it is still ongoing. With the increasing complexity of networks, it can be difficult to identify how a hostile actor might have entered the network. Sophisticated forensic and data analytical tools — some of which are available from outside experts, and others from law enforcement — are critical to this phase.
- Consider that a detected attack can sometimes mask deeper incursions into your organization, and that in some situations it may take weeks, not hours, to detect a breach and begin to stem the damage.
- Decide whether and to what extent to seek the involvement of law enforcement¬ — and whether the appropriate agency is local or federal. There are many factors to consider, and they will vary according to the type and scale of the attack. (This is a significant issue, considering that nearly half of responders doubt the government's ability to investigate cybercrime.)
- Consider secondary risks. For example, a simple email breach can reveal secrets to adversaries/ competitors. If networks are breached, and the company uses VOIP/networked phone service, the telephones are also likely to be compromised.
- Finally, when a breach occurs, remember: a cyber investigation is still fundamentally an investigation, and the principles of a criminal investigation still apply. In focusing on stopping an ongoing attack and getting back on line, it's crucial not to inadvertently destroy evidence that could help with that investigation — and with preventing the next attack.

Remedial actions

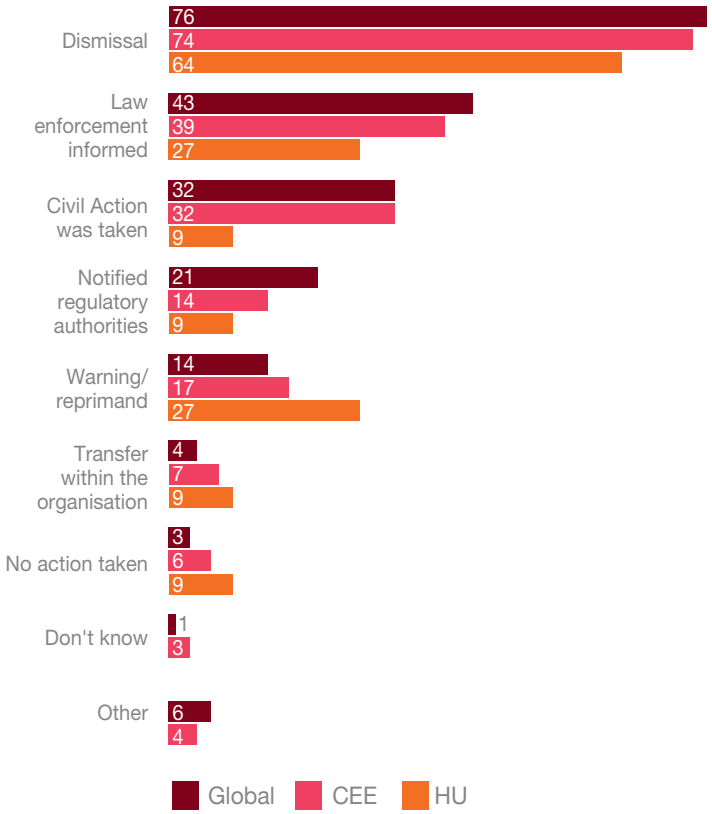
Remedial actions against internal – as well as against external perpetrators are clearly strict. Hungarian results show that 64% of companies dismiss the internal perpetrator. In CEE only 21% of internal fraudsters keep their jobs, in Hungary, our respondents tell us this is significantly higher, with 36% remaining employed.

If organisations are only warning or transferring perpetrators within the organisation rather than potentially dismissing them, the perpetrators will continue to remain within the organization and possibly find other ways to commit fraud and economic crime. It is important for organisations to demonstrate "zero tolerance" for fraud in order to set the right tone within the organisation. It is important that deterrent actions are taken and consequences of fraud are clearly communicated to all employees.

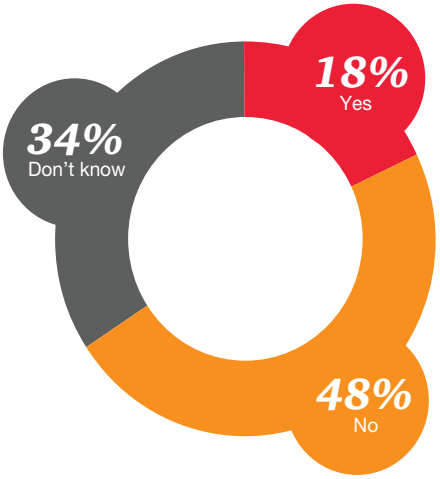
Regarding remedial actions against external perpetrators, an encouraging finding is that the majority of the organisations informed law enforcement in spite of not believing that the law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime. Only 18% of organisations believed law enforcement agencies are adequately trained.

Therefore, 45% of organisations that notified regulatory authorities took civil action or ceased a business relationship in response to an external fraud perpetrator.

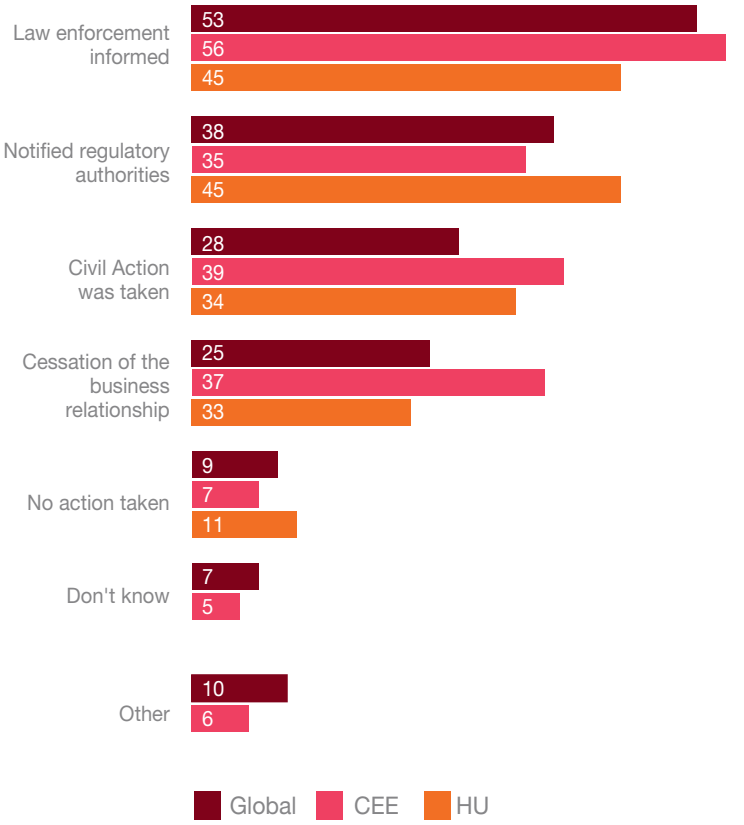
What actions, if any, did your organization take against the main internal perpetrator? (%)

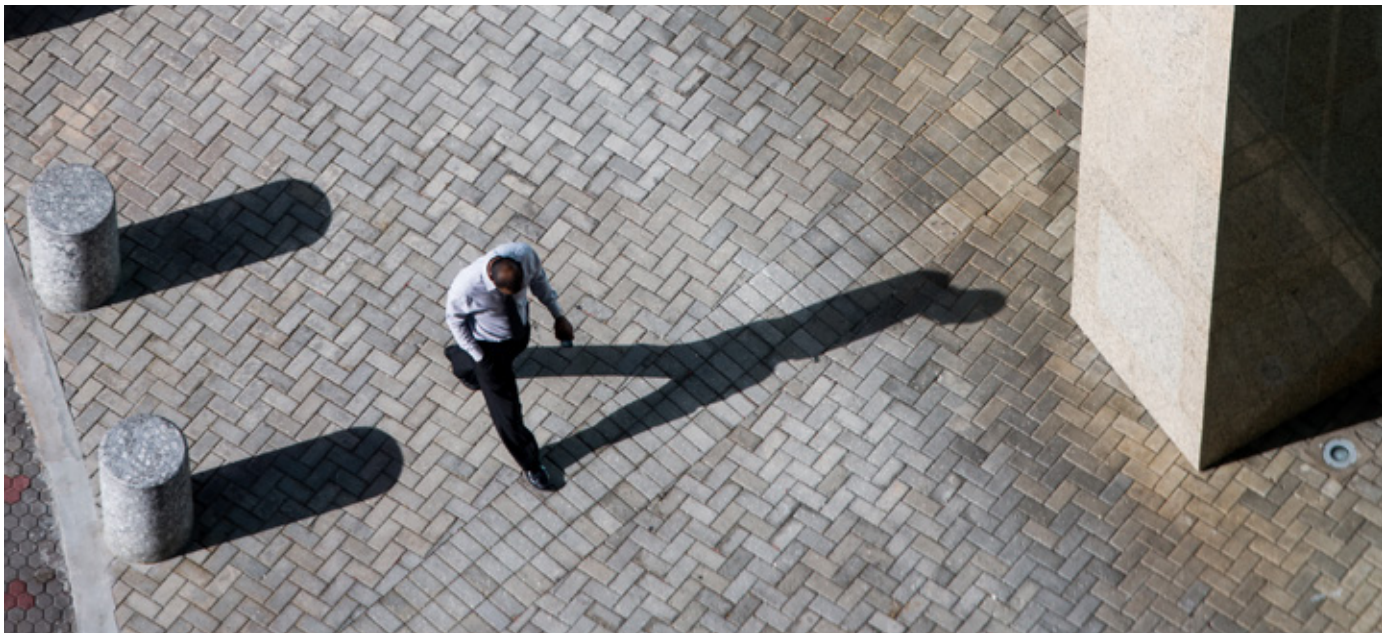


Do you believe the law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime?



What actions, if any, did your organization take against the main external perpetrator? (%)



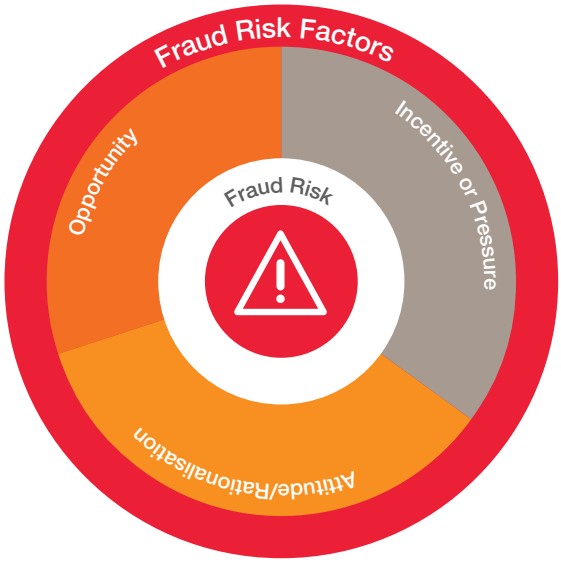


Ethics & Compliance: Aligning Risks and Responsibilities with Values and Strategy

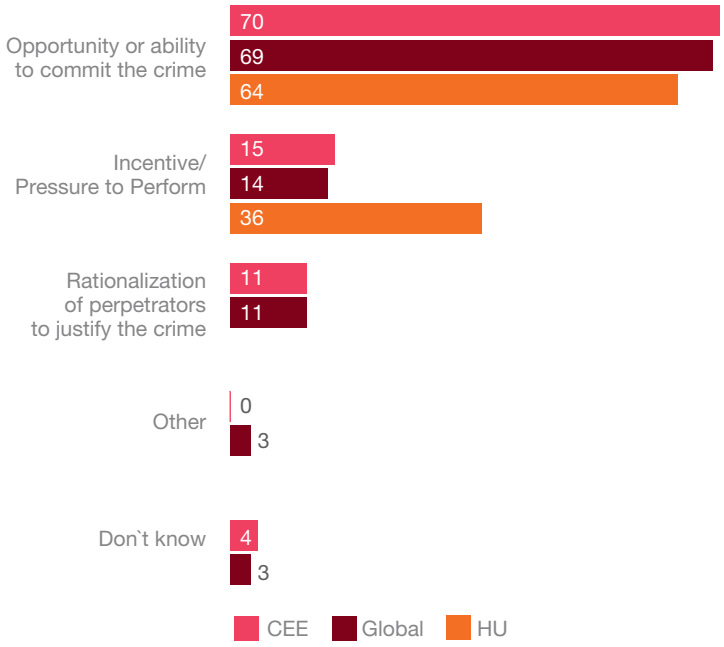
As already mentioned earlier in the report, the crucial factor contributing to the committing of economic crime is simply the opportunity to do it (64%). This far outweighs the other two elements of the fraud triangle, which are incentive/ pressure to perform and rationalisation of the crime. So the best way to prevent this opportunity is to strengthen the controls.

Examples of opportunities:

- Internal controls are not adapted to the rapidly changing business environment and to the "new" types of threats including cybercrime
- Limited detection capacity, understaffed detection teams with inappropriate skill set
- Reactive (rather than proactive) approach
- Corporate culture (level of tolerance of fraudulent behaviour), poor tone from the top



What factor do you feel has contributed the most to economic crime committed by internal actors? (%)



Compliance programmes

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

1. People and culture. Clear processes and principles, culture where compliance is hard-wired to values, measuring and rewarding desired behaviours.
2. Roles and responsibilities. Formal compliance structure. Ensuring they are correctly aligned with current risks.
3. High-risk areas. Better implementing and testing in high-risk markets and divisions
4. Technology. Better use of detection and prevention tools, including big data analytics

Our survey revealed that approximately one in five (19%) of all respondents told us they knew of no formal ethics and compliance programme in place in their companies.

To ensure that the company´s compliance and business ethics program is effective, 84% of companies pursue internal audits, 65% pursue management reporting and 42% monitor whistleblowing hotline reports. Thirty-one percent also carry out an external audit. While internal audit is an important piece of the framework for assessing a compliance programme's effectiveness, it is not by itself a sufficient means of assuring compliance, due to the fact that its interventions are both periodic and historical. Moreover, the fraud risk profile has changed (e.g. an increase in new frauds such as cybercrime), and incidence of some fraud types is rising or persistent in certain types of organisations.

It is important that all people across the business — not just compliance professionals — understand their roles and responsibilities in ensuring the business is aligned and delivering its ethics and compliance programme and priorities. Still, many companies exhibit a degree of

"In terms of compliance, there is still room for improvement for Hungarian companies. It is worth recalling that while compliance does not readily generate revenue, it ultimately affects the bottom line: by assessing and managing risks, it is an important safeguard against losses. Successful compliance also requires involving the broadest possible range of staff already in the implementation phase."

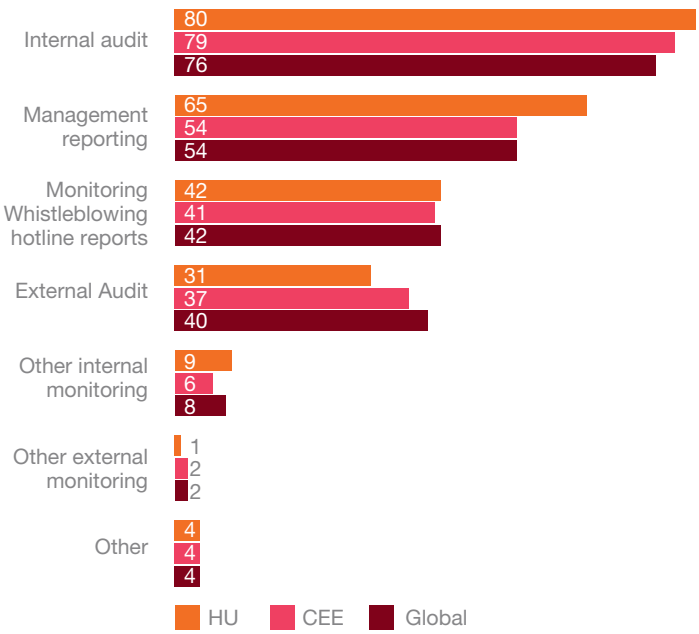
Tibor Hurton
PwC Hungary,
Manager,
Forensic services

confusion about who has ownership of what. Forty-four percent of Hungarian companies have a Chief Compliance Officer responsible for their business ethics and compliance program. In the remaining companies, part this function is included in other functions such as HR or Finance.

"Ownership" of the programme should belong to the first line — business-unit management — whose responsibility it is to understand the risks and determine the unit's appetite for that risk. The role of the compliance function, on the other hand, is oversight and guidance. In some organisations, however, there is a tendency to view compliance as a kind of insurance policy upon which a passive responsibility can rest.

Ultimately, all members of the business need to be working towards the same compliance outputs. Forward-thinking organisations position themselves as being a broader "compliance community," wherein the roles and responsibilities of ethics and compliance become part of day-to-day business for everyone.

How does your organisation ensure that your compliance and business ethics program is effective? (%)



81%

More than 81% of Hungarian survey participants have a formal ethics and compliance programme.

46%

The share of fraud is heavily weighted towards internal perpetrators, as opposed to external perpetrators (33%).

25%

In the past two years, a quarter of Hungarian companies have experienced one or more incidents of economic crime.

Contacts

Dr. Csaba Polacsek

Executive Director
Advisory Services
+36-1-461-9751
csaba.polacsek@hu.pwc.com

Tibor Hurton

Manager
Forensic services
+3630-598-1633
tibor.hurton@hu.pwc.com

pwc

http://www.pwc.com/hu/en/crimesurvey