

Forensic Services

Economic crime: people, culture & controls

The 4th biennial Global Economic Crime Survey

Russia



MARTIN-LUTHER-UNIVERSITY
ECONOMY & CRIME RESEARCH CENTER
Prof. Dr. Kai-D. Bussmann

PRICEWATERHOUSECOOPERS 

Introduction

We are pleased to present the 2007 PricewaterhouseCoopers Global Economic Crime Survey results – the largest study of its kind now available worldwide. In our fourth biennial survey, we interviewed senior representatives of more than 5,400 companies in 40 countries, including 125 leading companies within Russia, providing us with unparalleled depth of insight into perceptions, awareness and impact of economic crime on business around the world.

To ensure the complete confidentiality of responses, the survey was conducted on behalf of PricewaterhouseCoopers by the internationally renowned market and social research institute, TNS Emnid. In subsequent data analysis, we cooperated with Prof. Dr. Kai Bussmann, Chair of Criminology & Penal Law at Martin-Luther University in Halle-Wittenberg, as well as the independent Economic Crime Research Center at the Martin-Luther University.

Apart from the actual company survey, in which companies report their experiences

in their own fight against economic crime, we added a case study section in which victimised companies provide detailed information on real-life crime incidents. We also look at a detailed profile of fraud perpetrators as well as the complicated interrelationship between comprehensive controls and corporate culture. We believe that the results of our analysis in these areas 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.

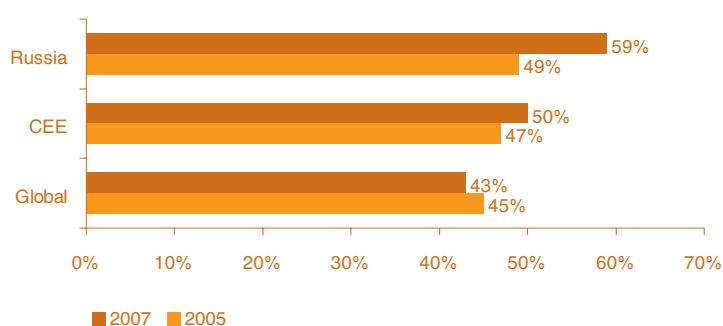
Our survey reveals that fraud remains one of the most problematic issues for businesses worldwide. Across the globe, 43% of companies have been the victims of economic crime in the last two years. In Russia, the overall figure is striking, at 59%; which is a 10% increase compared to our last Economic Crime Survey in 2005 (49%), and is well above the average for Central and Eastern Europe (CEE) (50%).



Key findings

- More than half of the Russian companies surveyed (59%) reported suffering one or more economic crimes in the past two years – a 10% increase from our previous survey.
- 63% of the companies surveyed had losses from fraud in excess of USD 1 million, and 20% of companies lost more than USD 10 million, with the average reported direct financial damage being USD 12.8 million. This means that the direct cost of economic crime in Russia has more than quadrupled since 2005 (USD 3.1 million) and is more than five times higher than the global average (USD 2.4 million).
- Recovery of financial losses in Russia remains difficult. 54% of Russian respondents said they did not succeed in recovering any part of the amount lost. However, this shows progress from our last survey, when 74% of companies did not recover any losses.
- 67% of Russian companies that suffered fraud also reported collateral damage to their business. The most serious types of collateral damage reported were: significant distraction of management time, significant time and expenses involved in litigation, damage to company reputation, and decline in working morale.
- The most widely reported type of crime is asset misappropriation (reported by 43% of companies), followed by corruption and bribery (34%). This is a reversal from 2005's survey, where corruption and bribery was reported by 54% of companies, followed by asset misappropriation (35%).
- Corruption and bribery is still perceived to be the greatest threat (30% of respondents). Almost half of all companies (48%) were put in a position in the last two years where they felt they were being asked to pay a bribe.
- Moreover, more than half of companies (51%) felt they had lost an opportunity to a competitor who they believe may have paid a bribe. This contrasts sharply with the global situation, where only 18% reported being asked for a bribe and 24% believed they had lost an opportunity.
- The majority of perpetrators were male, aged from 31 to 40 years old, with a higher education degree. Although the majority of the most serious economic crimes¹ reported by our Russian respondents for the past two years were perpetrated by external parties such as customers or business partners, an increasing proportion were perpetrated by individuals within the company (38% in 2007, compared with 13% in 2005). Worryingly, almost half (41%) of the internal perpetrators in Russia belonged to senior management. This is significantly higher than for global respondents (20%).
- In terms of fraud drivers, most frauds reported in Russian companies involved the perpetrator's financial/materialistic incentive (73%), low temptation threshold (38%) and lack of awareness that his actions were wrong (33%).
- The majority of economic crimes were initially detected by corporate security and internal audit functions, which is a remarkable change from the prior survey, where the overwhelming majority of cases were revealed by chance, and internal audit was a factor in only 7% of those surveyed.
- In most cases, companies brought criminal (35%) or civil (35%) charges against the perpetrators. Only 10% of the perpetrators, however, were sentenced. In CEE and globally, the sentencing rate is higher, 16% and 20%, respectively.
- 71% of Russian respondents believe that the government should take primary responsibility for combating economic crime in Russia. They also recognise that companies themselves should take significant measures (57%).
- While 59% of the companies reported to have fallen victim to economic crime in our survey, only 10% of those interviewed considered it likely that their company would experience fraud over the next two years. 20% of the surveyed companies do not plan on taking any specific actions to deal with economic crime.

1. Companies reporting fraud



¹ The profile of the perpetrator focuses on the main perpetrators of the two most serious offences each surveyed company reported.

Fraud – a most problematic business risk

Our 2007 economic crime survey reveals that 59% of the companies surveyed in Russia reported being subject to one or more significant economic crimes over the past two years. This is a 10% increase from our 2005 research and is well above the global (43%) and CEE (50%) averages.

Although the headline figures have increased, we believe that there are positive factors underlying these statistics, which have played a significant role in the increase in the number of reported economic crimes:

- A greater awareness of economic crime within organisations;
- A growing desire for transparency;
- A decrease in the stigma attached to reporting fraud, which is no longer perceived as a taboo subject²; and
- The introduction of more stringent controls and risk management systems, which enable companies to detect more cases of fraud.

Another factor will be the size of companies surveyed where, in Russia, 31% of respondents had more than 5,000 employees, compared to 9% globally.

The results of our global survey again show that economic crime affects companies of all sizes, but typically, the bigger they are, the harder they fall. The proportional difference in the reported levels of economic crime between large and small companies may be due to a number of factors, including a greater level of anonymity and devolved responsibilities among staff, as well as more complex and interconnecting processes and systems, leaving potential “control gaps” for fraudsters to exploit.

Types of economic crime – does perception equal reality?

When we compare the perceived and the actual incidence of economic crime in Russia, we see that companies generally thought that fraud was less present in Russia than what was actually reported. This should serve as a warning, since unsubstantiated optimism can lead companies to a false sense of security, exposing them to greater risk.

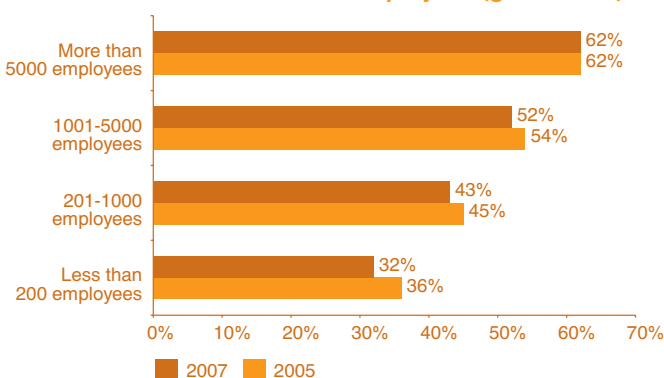
Although corruption and bribery continues to be perceived as the most prevalent

type of fraud (30% of companies believe it to be so), the most common type of fraud encountered was asset misappropriation (43%), followed by corruption and bribery (34%).

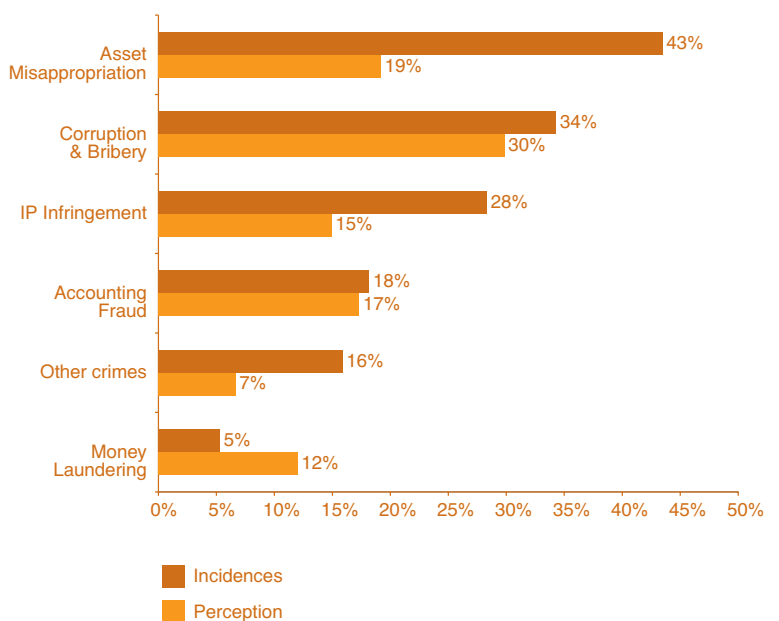
Asset misappropriation is the most common type of fraud reported globally, as well as in CEE. The prevalence of this type of fraud in Russia is not surprising, as it is among the easiest to detect; it involves taking of items with a defined value and provides a clear indication of where management should concentrate its immediate attention in order to avoid losses.

That corruption and bribery is perceived as the major threat is consistent with our 2005 survey, where it was also the most prevalent economic crime. The change in the most prevalent type of fraud in 2007 compared to 2005 may be explained by the fact that more Russian companies reviewed their anti-corruption compliance policies in the last two years.

2. Companies reporting fraud, according to their number of employees (global data)



3. Perceived prevalence and actual incidence of frauds



² Indeed, these results should be compared to our 2003 survey, where not one company reported an incidence of economic crime.

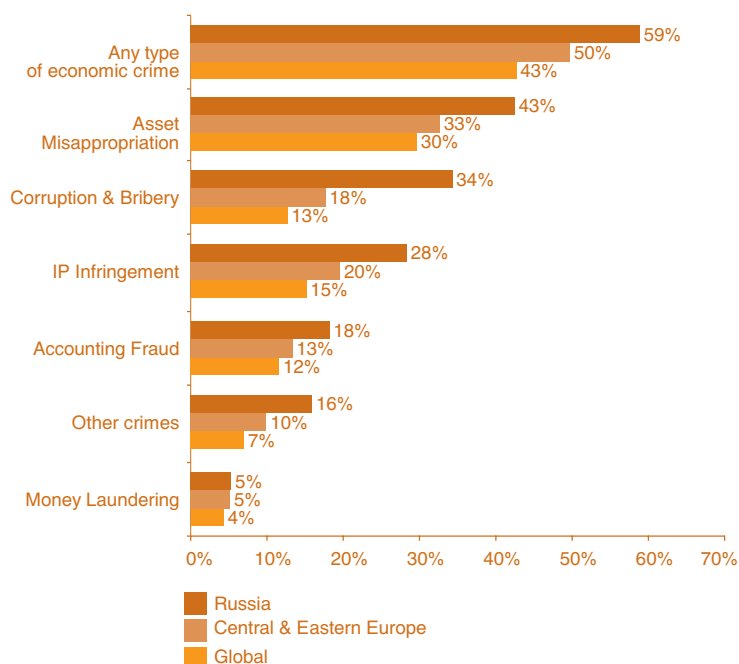
Key Elements of Effective Anti-Bribery Compliance Programs

1. Create a control environment with the right structure and tone:
 - CEO communication on “zero tolerance” for illegal acts and misconduct
 - Establish high quality, compliance organisation with well trained staff and clear processes
2. Focus on the most important compliance risks:
 - Perform risk assessments to identify high-risk areas
 - Adapt processes based upon the nature and source of risk
3. Design compliance control activities to minimise risk of non-compliance:
 - Establish control procedures for high bribery risk areas
 - Adopt protocols for investigating allegations of misconduct, illegal acts and non-compliance
4. Establish processes and systems supporting compliance:
 - Ensure effective reporting to key corporate governing bodies
 - Embed compliance into the IT systems

The corruption and bribery situation, however, appeared to be more serious when we asked companies about what was happening around them: almost half (48%) had been put in a position where they felt they were being asked to pay a bribe in the last two years, and 51% felt they had lost an opportunity to a competitor who they believe may have paid a bribe. These numbers are above those for CEE (30% and 45%, respectively) and are considerably higher than elsewhere in the world: only 9% of companies in Western Europe and 3% of companies in North America report having been asked for a bribe, and 15% of companies in Western Europe and 6% in North America believe they had lost an opportunity to another company that had paid a bribe.

Taking into consideration the above information, it is surprising that only 15% of Russian companies believe that it is likely that they will be subject to corruption and bribery in the next two years.

4. Actual incidence of frauds



unsubstantiated optimism can lead companies to a false sense of security, exposing them to a greater risk of fraud

The cost of fraud

While the reported number of incidents of economic crime in Russia increased by 10% from two years ago, the average financial loss reported more than quadrupled, from USD 3.1 million in 2005 to USD 12.8 million in 2007. Globally, the average cost of economic crime per company over the last two years was approximately USD 2.4 million (up from USD 1.7 million). Most companies in Russia (63%) suffered losses of more than USD 1 million, with 20% of companies suffering losses of over USD 10 million. By way of comparison, only 3.7% of companies globally experienced losses of over USD 10 million.

As discussed above, one factor that will affect the average loss suffered is the size of company concerned. 67% of companies surveyed in Russia employed more than 1,000 employees, compared with 30% globally.

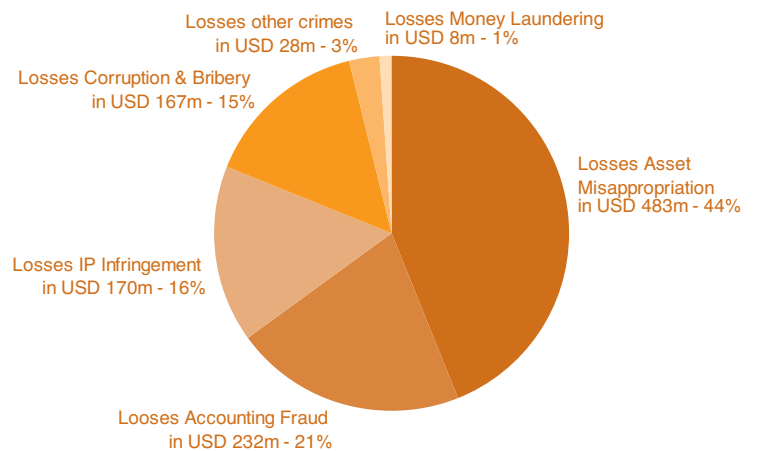
Another explanation for the high losses reported by Russian companies may lie in the fact that most frauds in Russia are committed by members of senior management (see page 9), who are highly educated and, as a result, are capable of causing more damage. Senior management can circumvent controls using executive privilege and devise more elaborate fraud schemes.

In addition, companies in our Russian survey that have suffered fraud reported having spent, on average, more than USD 1.6 million over the last two years in “management costs” related to dealing with the fall-out from a significant fraud, from the reallocation of management time to the possible costs of litigation in retroactive action, and from the need to manage additional public relations and investor relations campaigns to dealing with renewed regulatory oversight demands.

While the direct reported costs of economic crime seem alarming enough, one should not ignore the collateral damage from fraud, i.e. damage to company’s brand and customer trust, to the share price and shareholder trust, to the company’s relationships with its suppliers, and decline in staff morale which can result in high staff turnover and loss of productivity. Although difficult to quantify, collateral damage can be a significant cost to a business. 67% of Russian respondents who had suffered fraud reported collateral damage to their business as a result. This is significantly higher than the global figure (54%).

the average financial loss from economic crime reported by Russian companies more than quadrupled over the last two years to USD 12.8 million

5. Cost of the most important types of economic crime - Russia



The drivers for fraud

For someone to commit fraud, it is generally accepted by criminologists and fraud investigators that three conditions must be present: the opportunity to commit fraud, the incentive to commit fraud, and the fraudster's ability to rationalise their own actions.

For this research, we simplified these into two areas:

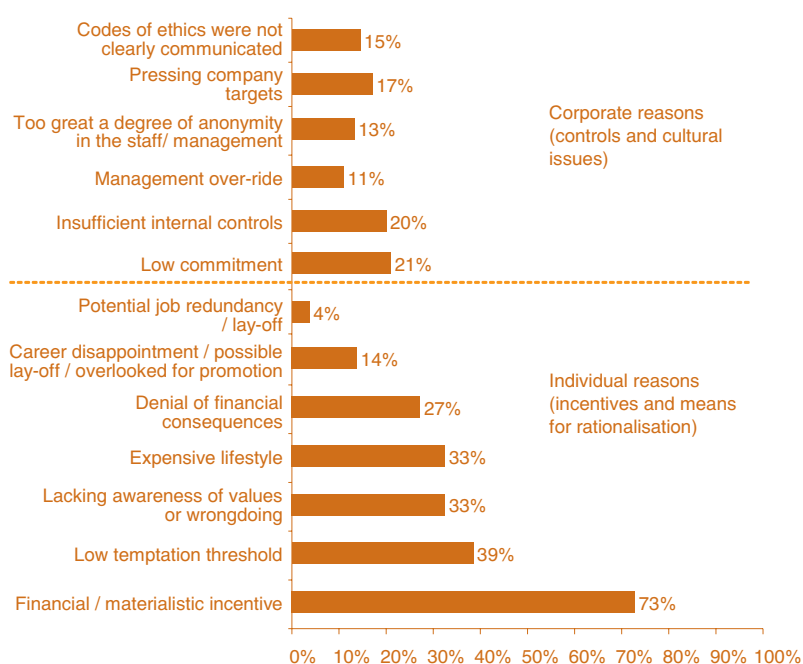
- The perpetrator's personal reasons for committing fraud (i.e. their incentive and ability to rationalise their actions to themselves).
- The organisational reasons that allowed fraud to occur (i.e. the levels of control and the ethical culture of the firm).

When asked to categorize the perpetrator's incentives, opportunities, and means of rationalizing their crimes, respondents highlighted the following:

- The perpetrator's financial/materialistic incentive (i.e. greed — 73%) and the need to maintain an expensive lifestyle (33%) — incentives;
- The perpetrator's low temptation threshold (39%) and the perpetrator's lack of awareness of values or of their own wrongdoing (33%) — means of rationalisation;

In terms of corporate causes, it is important to notice that while insufficient company controls appear to have played a significant role in 20% of the cases, perhaps an even more important role is played by a company's culture (and the employee's relation to it). In 21% of cases, the employees appear to have had low commitment to the firm, they had maintained a degree of anonymity among the staff (13%), and they had been able to state that they were unclear about the company's ethics (15%). A company's culture is therefore vital in establishing an ongoing, effective fraud risk management programme.

6. Reasons cited by companies to explain why fraud was committed



a company's culture is vital in establishing an ongoing, effective fraud risk management programme

Means of detecting and preventing fraud

The means by which fraud is detected can be split into two broad categories: detection by chance and detection through risk management controls and systems.

The majority of economic crimes in Russia were initially detected by corporate security and internal audit functions (28% and 20%, respectively), which is a significant change from the prior survey, when the overwhelming majority of cases were detected by chance³ (35% in 2005, down to 21% in 2007) and internal audit was a factor in only 7% of those surveyed. In fact, detection by chance continues to play a predominant role globally (40% of initial detections).

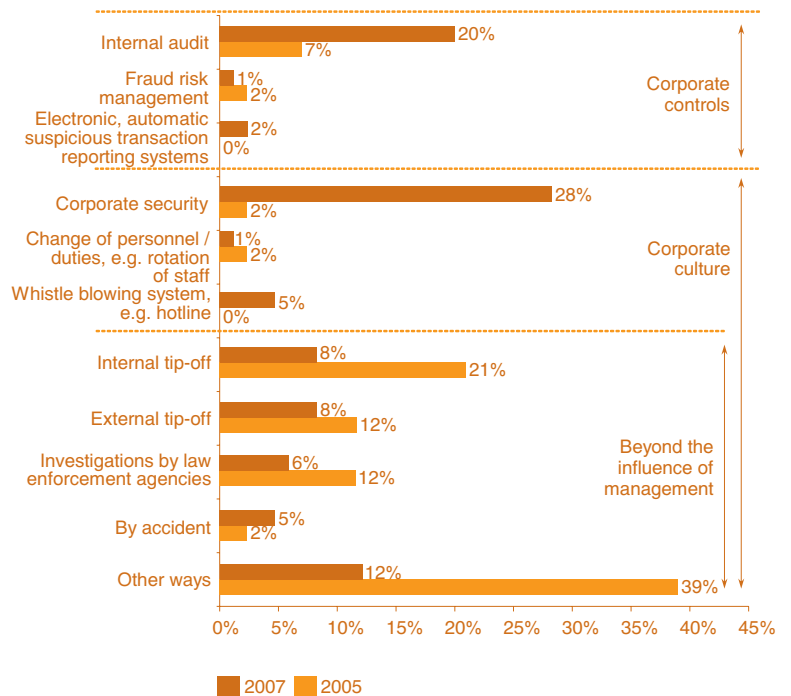
Therefore, it is encouraging that almost all Russian respondents (98%) reported having some prevention measures in place against fraud. Indeed, Russian companies surveyed had, on average, over 11 of these types of measures, while global and CEE companies' average is nine. Our respondents considered corporate security and internal audit to be the most effective measures.

24% of Russian companies had implemented new control measures, and 37% had strengthened their existing control measures during the past two years. Nearly 20%, however, had no plans for dealing with economic crime.

While carefully implemented and regularly updated controls can themselves be effective in detecting and, over a period of time, deterring fraudsters, our research also shows that it is the culture of a company – one that supports a holistic compliance programme working in conjunction with a clearly understood, and lived, code of ethics – that is the true foundation for an effective anti-fraud programme.

our research shows that it is the culture of a company that is the true foundation for an effective anti-fraud programme

7. Detection methods



³ A combination of internal/external tip-offs and accidental detection.

Fraud's perpetrators

More than three quarters (82%) of Russian companies that have become victims of economic crime in the past two years know or believe that a party external to the company played a role in the fraud. Of those 82%, nearly 20% know or believe that the external party was located in a foreign country.

When looking at the relationship between the main perpetrator of an economic crime and the affected company⁴, 38% of Russian companies reported that the main perpetrator was a member of their own staff. This represents a substantial increase since 2005 (13%) but is still significantly lower than the global (50%) average. In our experience, a significant proportion of economic crimes is perpetrated by or in conjunction with individuals internal to the company. This may be because those inside the company tend to have

a better understanding of the business (including its strengths and weaknesses) than do outsiders and are therefore in a better position to perpetrate fraud. The low reported figure of internal perpetrators in Russia's case may indicate that the frauds identified and reported by Russian respondents are only the most flagrant cases of fraud, while the more sophisticated internally perpetrated frauds are either going undetected, or companies are reluctant to speak about them⁵.

The typical fraudster was male (89%), between 31 and 40 years of age. With 84% of Russian fraudsters holding university degrees, they are generally better educated than their CEE and global counterparts (61% and 50%, respectively).

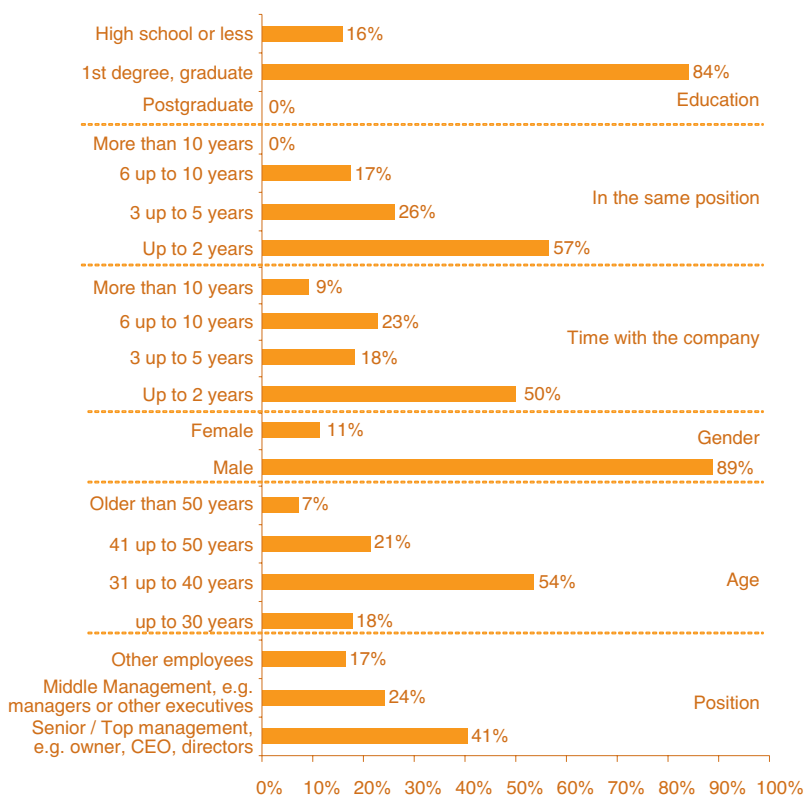
An alarming finding in our 2005 report was that in Russia, senior management was responsible for 50% of the cases. Although

this figure is lower in 2007 (41%), it is still double the global average (20%), with perpetrators around the world being mainly middle management and line personnel. There are two possible explanations:

1) top managers in Russia are highly educated and are able to devise more elaborate fraudulent schemes; 2) weak corporate governance, which, among other things, results in situations where business owners and shareholders generally have limited control over their top managers.

While concerning, it should not be surprising, as being in a high position does not limit an individual's desire for material gain and, in some cases, it may help fraudsters bypass sophisticated control systems. More importantly, our global research shows that the frauds committed by senior and middle management cause the greatest financial and collateral damage to businesses.⁶

8. Profile of perpetrator



frauds committed by senior and middle management cause the greatest financial and collateral damage to businesses

⁴ In this case we asked respondents to focus specifically on their two most serious fraud cases in the past two years, and their main perpetrator.

⁵ Indeed, the results of our global study indicate that companies may be less reluctant to report cases of fraud perpetrated by someone outside the company than those cases that were perpetrated by an employee. (See: PricewaterhouseCoopers: Economic crime: people, culture and controls. The 4th biennial Global Economic Crime Survey, pg. 14)

⁶ For more details, see PricewaterhouseCoopers: Economic crime: people, culture and controls. The 4th biennial Global Economic Crime Survey, pg. 14

Dealing with fraudsters

Once an alleged fraud has been detected, steps must be taken to investigate and authenticate the claims. According to our survey, once an allegation had been made, most companies launched an internal investigation (75%), involved an in-house counsel (71%) and internal audit (58%). In the majority of cases, the offence was internally reported to the board of executive management (69%) and the board of non-executive management, including the audit committee (49%). In approximately 50% of cases, offences were reported to law enforcement, and/or they were called in to investigate.

An important step in creating a corporate culture that does not tolerate fraud is being consistent when responding to economic crime. In our view, once an incidence of economic crime has become known, it is vitally important to inform the staff that all of the perpetrators will be treated the same way, regardless of their position within the company. Low prosecution rates of members of senior management can affect overall company morale and have a negative impact on the total number and volume of frauds occurring within a firm.

Once a company confirms a suspected fraud, appropriate action against the perpetrator is essential in order to deter other potential fraudsters and to show stakeholders in the business that the organisation will not tolerate such malpractice. Our survey indicates that Russian companies principally take

the following actions against the main perpetrator: pressing criminal charges, civil charges, and cessation of business relationship (35% each), or in case of internal perpetrators, dismissal (25%). Alarmingly, though, 19% of companies stated that they took no action against the perpetrator. In addition, only 10% of charged perpetrators in Russia were sentenced, while in CEE as well as globally, the sentencing rate is higher, 16% and 20%, respectively. This highlights the importance of conducting investigations in a way that ensures the integrity of evidence for court purposes.

Recovery of lost assets

Besides deterring other fraudsters with a prompt and decisive response, recovering financial losses is another important aim for companies. Recovery of financial losses in Russia remains low: 54% of Russian respondents said they did not succeed in recovering any part of the amount lost. Compared to our last survey, however, this represents a definite improvement (in 2005, 74% of companies did not recover any losses).

On average, Russian companies recovered 35% of their losses from economic crime, which is higher than the CEE (25%) and global (28%) averages. However, 71% of companies in Russia do not have insurance to cover the losses and costs of economic crime, compared to a global average of 61%.

Fraud in the future

Fraud remains a serious problem. On a global scale, levels of economic crime have not dropped significantly over the course of the decade, but despite that, companies remain confident — as they have in our previous studies — that their controls will limit their exposure to fraud in the future. The same goes for Russia, where an alarming 71% of companies believe that it is unlikely that their organisation would be subject to economic crime over the next two years (compared to 43% of companies in our last survey⁷). In our opinion, this may well be a sign of over-confidence.

The fight against fraud is a constant struggle. Our biennial study continues to show that in order to assess and manage its risks, a constant re-evaluation of all fraud risk management activities is necessary. Equally importantly, companies must strive to establish a culture that supports anti-fraud controls with clear and ethical guidelines, engendering loyalty to the organisation's brand and showing (through retroactive action) that every perpetrator, no matter what their position in the company, will be subject to equivalent sanctions. As with all crimes and unwanted business risks, a move from after-the-fact reaction to prevention is the most valuable.

it is simply impossible
to eliminate economic
crime completely:
it is like fighting the
mythical Hydra, cutting
off one form of fraud
merely allows another
to grow

⁷ Two years ago, we asked respondents about a longer — 5 year — outlook.

Contact information



Roger Stanley

Partner, CEE Forensic Services leader
r.stanley@ru.pwc.com



Irina Novikova

Senior manager
irina.n.novikova@ru.pwc.com

Tel.: +7 (495) 967-6000

www.pwc.ru/forensic

www.pwc.ru/forensic