www.pwc.com/bg

Economic Crime: Known and Emerging Threats to Your Business

Global Economic Crime Survey 2014

Bulgaria Country Supplement

GECS 2014, Bulgaria

April 2014

pwc

Table of Contents

Introduction

We are pleased to present the 2014 PricewaterhouseCoopers Global Economic Crime Survey results – the largest study of its kind now available worldwide. Our web based survey was completed by senior representatives of 5,128 companies from around the world, including 79 leading organisations in Bulgaria, providing us with unparalleled depth of insight into perceptions, awareness and impact of economic crime on business around the world and in Bulgaria.

Methodology

The seventh Global Economic Crime Survey was carried out during the period between 4 September 2013 and 25 October 2013. The survey questionnaire, containing 46 questions in total, was completed by 79 Bulgarian organisations, covering a wide range of industry sectors, such as retail & consumer, transportation & logistics, manufacturing, financial services, energy, utilities & mining, engineering & construction and others.

Of the total number of Bulgarian respondents, 63% were privately owned organisations and 32% were listed companies, while another 5% have not specified their organisation's ownership structure.

The findings in this survey come from respondents' reports of their experiences of economic crimes in their organisations. We obtained information from them on the different types of economic crime, their impact on the organisation (both the financial loss and any collateral damage), the perpetrator of these crimes, as well as what actions the organisation took in response to these crimes.

To ensure the complete confidentiality of responses all survey data have been separated from the organisation name and responses have been associated only with the industry, organisation size, and other demographic data. No references to individual organisations have been made in results or analysis of the survey data.

Highlights

Fraud

- *25% of surveyed organisations in Bulgaria have experienced economic crime in the last two years.*
- *One in four who reported fraud suffered losses of more than USD 100K.*
- *Asset misappropriation is the most common type of fraud reported in Bulgaria.*
- *Bribery & corruption is perceived to be the greatest threat to business.*
- *Cybercrime and procurement fraud emerged among the top six types of economic crimes in Bulgaria, accounting for 17% and 15% of all reported cases of fraud, respectively.*
- *Bulgarian organisations are aware of the risk of cybercrime – 92% of all respondents stated that their perception of the risk of cybercrime has either increased or remained the same over the last two years.*

The fraudster and the defrauded

- *Though companies have more confidence in their management systems, 20% of fraud is still detected by chance.*
- *The role of fraud risk assessment is underestimated – 35% of the surveyed organisations have not performed any such assessment.*
- *Surveyed organisations demonstrated zero tolerance to internal perpetrators – all have undertaken actions against fraudsters within their organisation. Internal fraudsters are identified primarily at middle management level.*
- *55% of the reported economic crimes were carried out by external fraudsters, suggesting that Bulgarian organisations do not pay sufficient attention to the selection process of their business partners.*

Fraud – a significant threat to businesses in Bulgaria?

Our 2014 survey reveals that 25% of the Bulgarian respondents reported that they have suffered fraud during the previous two years; slightly below the Southeast Europe ("**SEE**") average (27%) and globally (37%).

However, does this mean that economic crime is less of a problem in Bulgaria than elsewhere? The answer lies in the abilities of organisations to identify and report economic crime and – once risks are detected – to take appropriate measures to counter the threat.

Types of economic crime – any new threats identified?

Most common frauds

The most widely reported type of economic crime in Bulgaria is asset misappropriation (40%). It is also prevailing in the SEE (52%) and globally (69%). This is not surprising, given the fact that it is easier to detect compared to other types of economic crimes as it involves the taking of items with a defined value and provides a clear indication of where management should concentrate its immediate attention in order to manage avoidable losses.

The next most common type of fraud in Bulgaria is accounting fraud (30%), followed by bribery and corruption (28%). The reported incidents of both these types of fraud are significantly higher compared to the SEE and global results. The higher level of accounting fraud in Bulgaria (compared to 22% in the SEE and globally) suggests that management is still under pressure, six years after the onset of the global economic crisis, brought by the current tough economic climate, to maintain certain KPIs and financial targets. As for bribery and corruption, the Bulgarian survey results (28%) are close to the global figure of 27% and slightly higher than the SEE results (23%). The actual incidents of bribery and corruption are likely to be underreported as this type of crime is difficult to identify and often goes undetected.

It is also interesting to note that anticompetitive behaviour is considered as a serious threat by many business leaders in Bulgaria when talking about doing business globally (29%). This high perception of risk appears typical for the European region as a whole – both Western European (25.3%) and Eastern European (24.5%) respondents reported breaches of competition law as a higher risk. The major driver seems to lay with the regulations of the EU Commission and alignment of local anti-trust laws and agencies with the EU. For further details in this respect, please refer to the Global Report.

Bulgarian respondents stated that financial loss was the most obvious impact resulting from breaches of competition law (24%), which is similar to SEE (24%) and slightly higher than global (17%) results. The second biggest impact was damage to the reputation of organisations (18%), compared to 22% for SEE and 21% globally.

Emerging threats

Though being introduced as new distinct survey classifications for Bulgarian respondents, cybercrime and procurement fraud immediately registered among top six reported economic crimes.

For our survey questionnaire these two categories were defined as:

Cybercrime	Procurement fraud
"'an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."	*"'an illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his/her organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation."*

17% of the surveyed Bulgarian companies reported they have suffered cybercrime in the last two years. While this is below the average for SEE (22%) and globally (24%), it could be expected for the number of incidents of cybercrime to increase in the next years.

92% of Bulgarian respondents stated that their perception of the risk of cybercrime has either increased or remained the same over the last two years, suggesting that Bulgarian organisations are aware of the risk of cybercrime.

When assessing the effects of cybercrime on their business, Bulgarian respondents have pointed out IP theft, including theft of data (38%), and reputational damage (37%) as their major concerns. These are considered among major threats for both SEE and globally, with IP theft accounting for 44% and 36%, respectively, and damage to reputation –39% and 41%, respectively.

53% of the respondents considered cybercrime threat mainly as an external one, while 28% are seeing it as an internal as well as an external threat. Only 8% have stated that it is merely an internal threat.

According to two thirds of the respondents, vendor selection is the stage where procurement fraud primarily occurred.

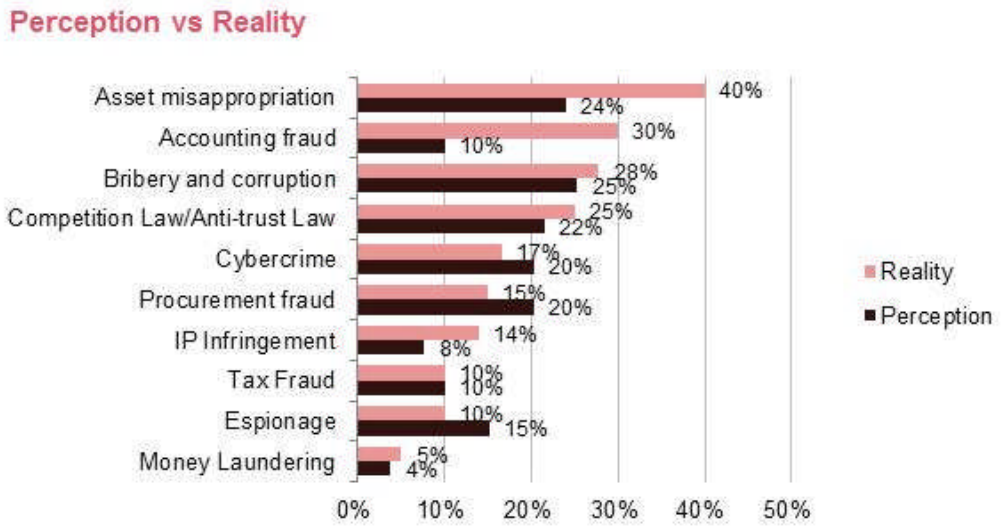
Perception vs. reality – is there a gap?

Survey results for Bulgaria reveal that there is still a gap between the historically reported fraud and the perception of the likelihood of future occurrence.

Despite the fact that 40% of Bulgarian organisations had suffered from asset misappropriation in the last two years, only 24% assumed it likely that their organisation could experience such fraud in the next two years.

A wider gap is observed between the actual incidences and perception of accounting fraud. This may be a sign of over-confidence, especially taking into account that 1 out of 5 incidences of fraud is still being detected by chance or through means that are not under the control of management.

Cybercrime, procurement fraud and espionage are categories in which perception of risk outweighs reality.



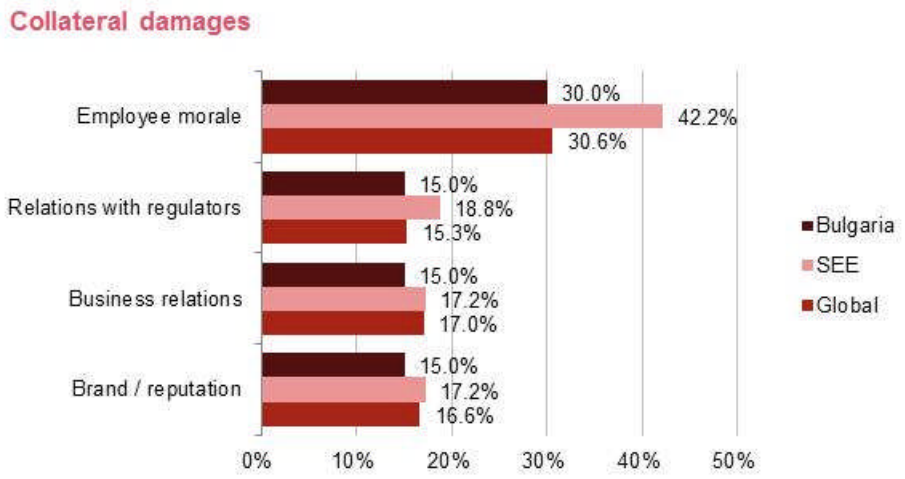
The fight against fraud is a constant struggle and organisations must not drop their guard, especially as the fraud risk profile in any market is dynamic and likely to change over time, with new types of fraud constantly emerging. While it is impossible to eradicate economic crime completely, organisations must continually define and implement controls and develop employee loyalty to establish a strong anti-fraud culture stemming from top management, i.e. the right “tone at the top”.

The cost of fraud – should intangible impact be also considered?

25% of organisations who suffered economic crime in Bulgaria lost over USD 100K

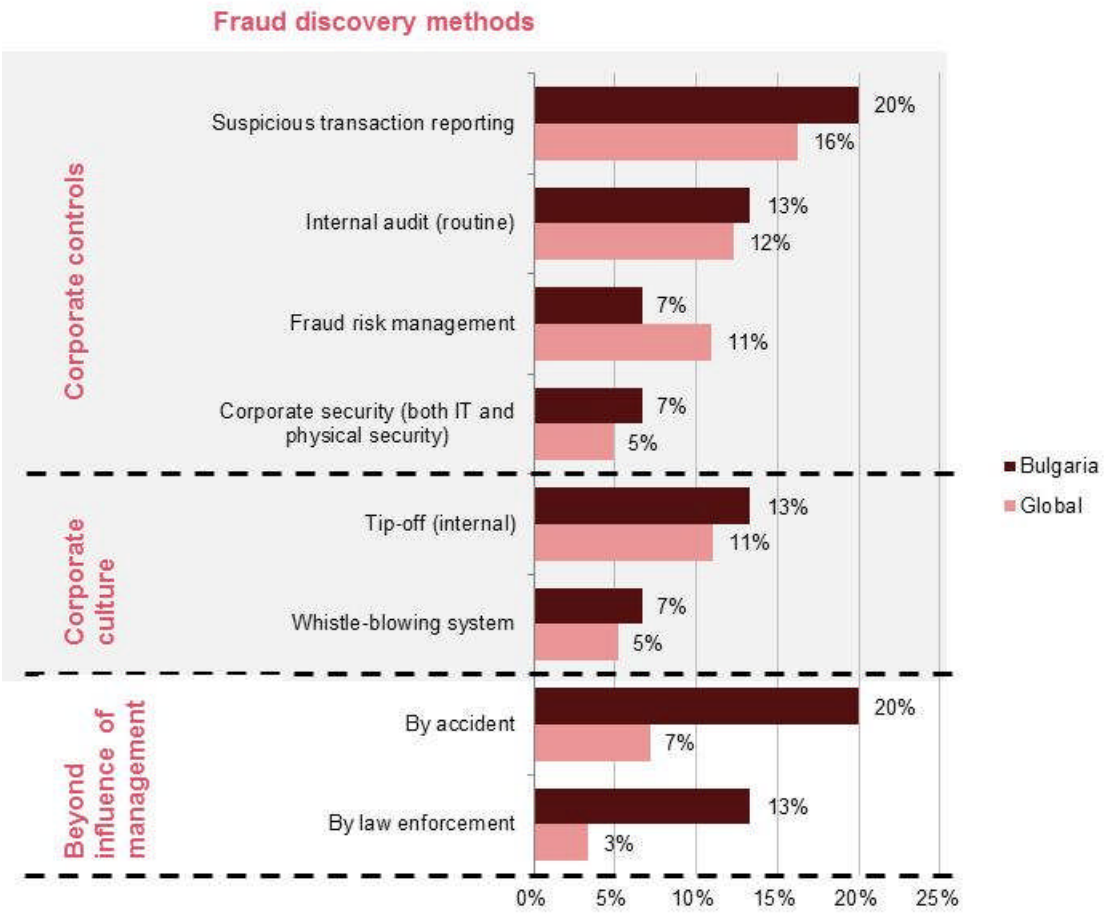
Fraud is costly to any business: 25% of organisations who suffered economic crime in Bulgaria lost over USD 100K and further 5% reported losses in excess of USD 1 million.

In addition to direct costs, collateral damages such as loss of reputation or brand, decreased staff motivation and employee morale, declining relationships with regulators and business partners should also be considered as they may be just as damaging: 30% of Bulgarian respondents highlighted the negative impact on employee morale as the most significant indirect cost of economic crime over the last two years, while an equal amount of respondents stated that the other categories of collateral damage (15% for each individual category) had the most significant adverse impact on their business.



Detecting fraud – are fraud controls effective?

The means by which fraud is detected can be split into two broad categories: detection by chance and detection through means within management's influence and control, such as risk management and internal audit.



Despite the fact that 27% of detected fraud resulted from effectively operating corporate controls such as fraud risk management, regular internal audit procedures or corporate security, 1 out of 5 incidences of fraud is still being detected by chance or through means beyond the control and influence of management. This is an alarming signal suggesting that there continues to be room for improvement in this area:

- 35% of Bulgarian respondents reported that they had not performed any fraud risk assessment in the last 24 months with the main reason being the perceived lack of value (39%) and lack of knowledge about what risk fraud assessment involves (18%); and
- In only 7% of the reported cases fraud has been detected through a whistle-blowing mechanism. This is quite surprising as in our experience anonymous whistle-blowers have helped organisations discover fraud in cases when other means of fraud detection have proven ineffective.

The typical fraudster – do you know your enemy?

The typical perpetrator in Bulgaria (similar to SEE) somewhat differs from global profile: i.e. 55% of the economic crimes Bulgarian organisations experienced (and 56% in the SEE) were carried out by external fraudsters (vs 40% globally).

36% of Bulgarian companies reported that the external perpetrators were customers and 27% reported that they were agents or intermediaries. Another 36% reported "others", which may have included organised groups and other unknown individuals. This is higher than both the SEE (19%) and global (24%) figures.

Compared to the global and SEE results, Bulgarian companies have not reported fraud perpetrators occupying senior management positions. It suggests that companies are successful at establishing the right "tone at the top".

While the "right tone at the top" is definitely a must, it is not a sufficient fraud preventive tool. Given the fact that the middle management (78%) was identified in Bulgaria as the main perpetrator of internal fraud (higher than the global average of 42%), organisations have to increase their efforts on the prevention front by knowing their employees and managers prior to hiring them, as well as checking/assessing the effectiveness of their fraud prevention and detection systems regularly. From a corporate point of view this is less costly than dealing with the consequences of fraud, as prevention is always cheaper and less painful than the cure itself.

We asked respondents who had stated that the main perpetrator of economic crime came from within the organisation to profile the age, gender, length of service and educational level of that perpetrator.

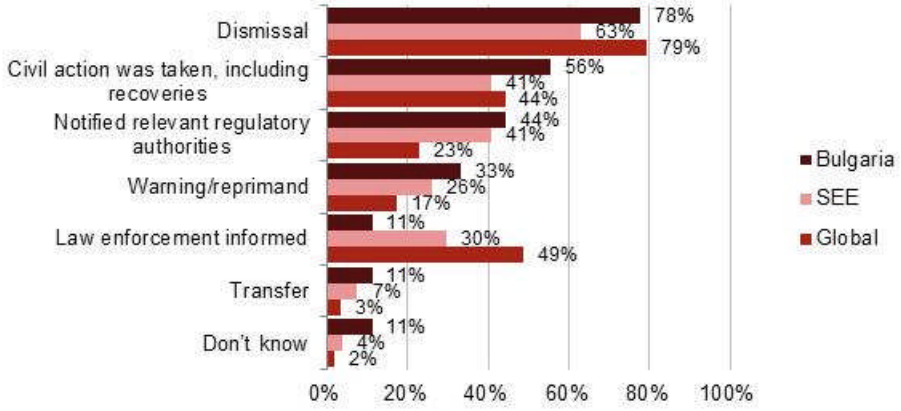
The results for Bulgaria indicate that the typical internal fraudster is a middle-aged employee with a university education or higher, and who has been with the organisation for a period of three to five years. These features seem to be common for internal perpetrators within SEE and globally; an interesting difference is observed, however, in terms of the perpetrator's gender. Reported results for Bulgaria are equally divided between the two genders (44.4% for both male and female) while based on the SEE and global survey data, the internal fraudster is predominantly male (63% and 77%, respectively). 11.2% of Bulgarian respondents did not know or were not willing to share the gender of the perpetrator.

Dealing with fraudsters – is a rapid and appropriate action vital?

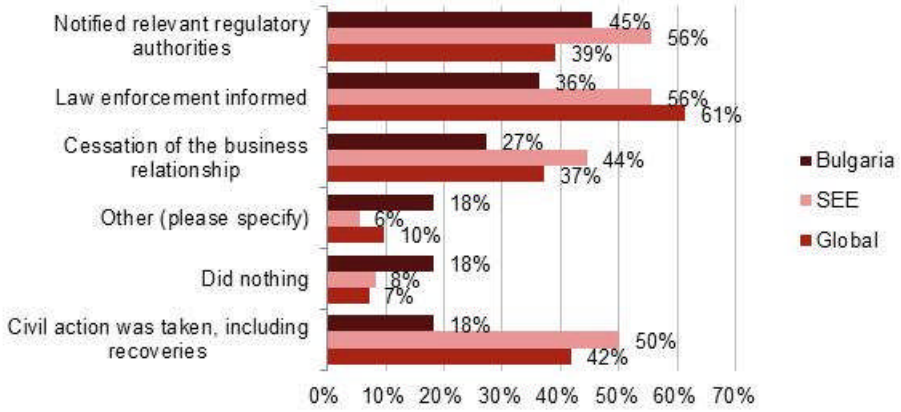
Once an organisation confirms a suspected fraud, appropriate action against the perpetrator is essential in order to deter other potential fraudsters and to show stakeholders in the business that the organisation will not tolerate such malpractice.

Our survey shows that Bulgarian organisations are not afraid to take action against fraudsters, which is an encouraging sign.

Actions against internal perpetrator



Actions taken against external perpetrator



In the case of the internal perpetrator, organisations seem to be more determined to demonstrate that they do not tolerate malpractices, i.e. they state that they have always taken actions, with dismissal being the most frequent action taken (78% of cases); this is in line with both the SEE (63%) and global (79%) trends.

When external fraud is detected, organisations appear to have been more cautious in their actions against perpetrators, ceasing business relationship in only 27% of cases, while in 18% of cases no actions were undertaken. Notifying the relevant regulatory authorities and law enforcement informed appear to be the preferred action against external perpetrators.

Terminology used in the supplement

Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

Asset misappropriation, including embezzlement/deception by employees

The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

Bribery and Corruption

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

Competition Law/Anti-Trust Law

Law that promotes or maintains market competition by regulating anti-competitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

Cybercrime

Also known as computer crime is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a byproduct in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information.

Financial loss

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to “loss of business opportunity”.

Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

i. The fraud risks to which operations are exposed;
ii. An assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence);
iii. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
iv. Assessment of the general anti-fraud programmes and controls in an organisation; and
v. Actions to remedy any gaps in the controls.

IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing with off as genuine.

Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

Procurement Fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

Forensic contacts for Bulgaria

Reneta Mamassian
Forensic Services, Bulgaria
9-11, Maria Louisa Blvd.
1000 Sofia, Bulgaria
Tel: +359 2 9355 200
Email: reneta.mamassian@bg.pwc.com

Bojidar Neytchev
SEE Advisory Leader
9-11, Maria Louisa Blvd.
1000 Sofia, Bulgaria
Tel: +359 2 9355 205
Email: bojidar.neytchev@bg.pwc.com

Forensic Services

The PwC forensic services network is comprised of forensic accountants, economists, statisticians, former regulators and law enforcement, fraud examiners, and forensic technologists. We help organisations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyse complex business issues, and mitigate the future risk of fraud.