www.pwc.com/bg
April 2018

Global Economic Crime and Fraud Survey 2018

Bulgaria Country Report

Pulling fraud out of the shadows

31%
of Bulgarian respondents reported suffering from one or more economic crimes in the past two years

35%
of Bulgarian companies, victims of fraud, have lost between 100,000 and 1 million US dollars

56%
of the reported crimes are perpetrated by external actors

pwc

Contents

Foreword

Per A. Sundbye
Partner, Leader
Forensics in South East
Europe (SEE)

Reneta Mamassian
Forensic Leader
for Bulgaria

Welcome to our 2018 Global Economic Crime and Fraud Survey, covering the period from our last survey in 2016 to 2018. It is the largest survey of its kind worldwide with 7,228 participants from 123 countries.

In Bulgaria, we are proud to say that as many as 65 companies (the largest number of participants within South Eastern Europe) shared their experience with economic crime and its impact on doing business in the country. We see this as a testament to their belief that economic crime is a persistent threat that is too costly to ignore. And that it needs careful, systematic and well-thought handling.

31% of Bulgarian participants reported they have suffered fraud during the previous two years. This is lower than the global average and even the country's own results from 2016.

The fact that there is a decreased number of economic crime incidents can be a double-edged sword. It can easily build an impression that fraud is less of a problem in Bulgaria than elsewhere. On the other hand, it can be a result of either over-confidence in organisations' abilities to prevent and fight fraud or of declined fraud awareness.

In the era of fast digitalisation, it is not surprising that over the last two years Bulgarian companies have been victims of more "sophisticated" economic crimes / frauds such as cyber crimes. The good news is that respondents in Bulgaria also seem to be better prepared for responding than ever before – 57% have fully implemented cyber security programmes.

In our 2016 survey we have called for Bulgarian companies to continually define and implement controls and develop employee loyalty to establish a strong anti-fraud culture stemming from top management. We are pleased now to understand that local organisations have put efforts in this direction an evidence of which is the insignificant number of the reported incidents perpetrated by internal people.

The typical perpetrator in Bulgaria (the same result as shown in the wider SEE region) somewhat differs from global profile – 56% of economic crimes suffered by Bulgarian organisations were carried out by external fraudsters (vs. 40% globally). We see a significant room for improvement in this area and would encourage Bulgarian businesses to step-up their efforts in corporate intelligence / background checks of external parties to avoid dealing with potential unpleasant consequences at a later stage.

It is a bit disappointing to see that since 2016 local enforcement authorities have not advanced much on their way towards building confidence and demonstrating knowledge and capacity to fight fraud. In this context, it would be interesting to follow up the developments and how the work of the recently established anti-corruption body in Bulgaria would influence the results in our next survey.

We would like to thank those individuals and organisations that took the time to respond to our survey. Without your support, this report for Bulgaria would not be possible. We trust you will find this survey to be a useful tool to assist you and your organisations in your battle with fraud risks and to help improve the Bulgarian market overall.

Key Findings

Reported fraud decreases

- Less economic crime is reported in Bulgaria in 2018 (31%), compared to 2016 (38%). The Bulgarian result is also lower than the global level (49%) and South Eastern Europe (39%). In the same time, reported fraud is at an all time high globally (49%).
- Fraud committed by the consumer is the most common type of fraud in Bulgaria, followed by bribery and corruption and cybercrime. Asset misappropriation falls from the first to the fourth position.

Risk-based approach is gaining ground

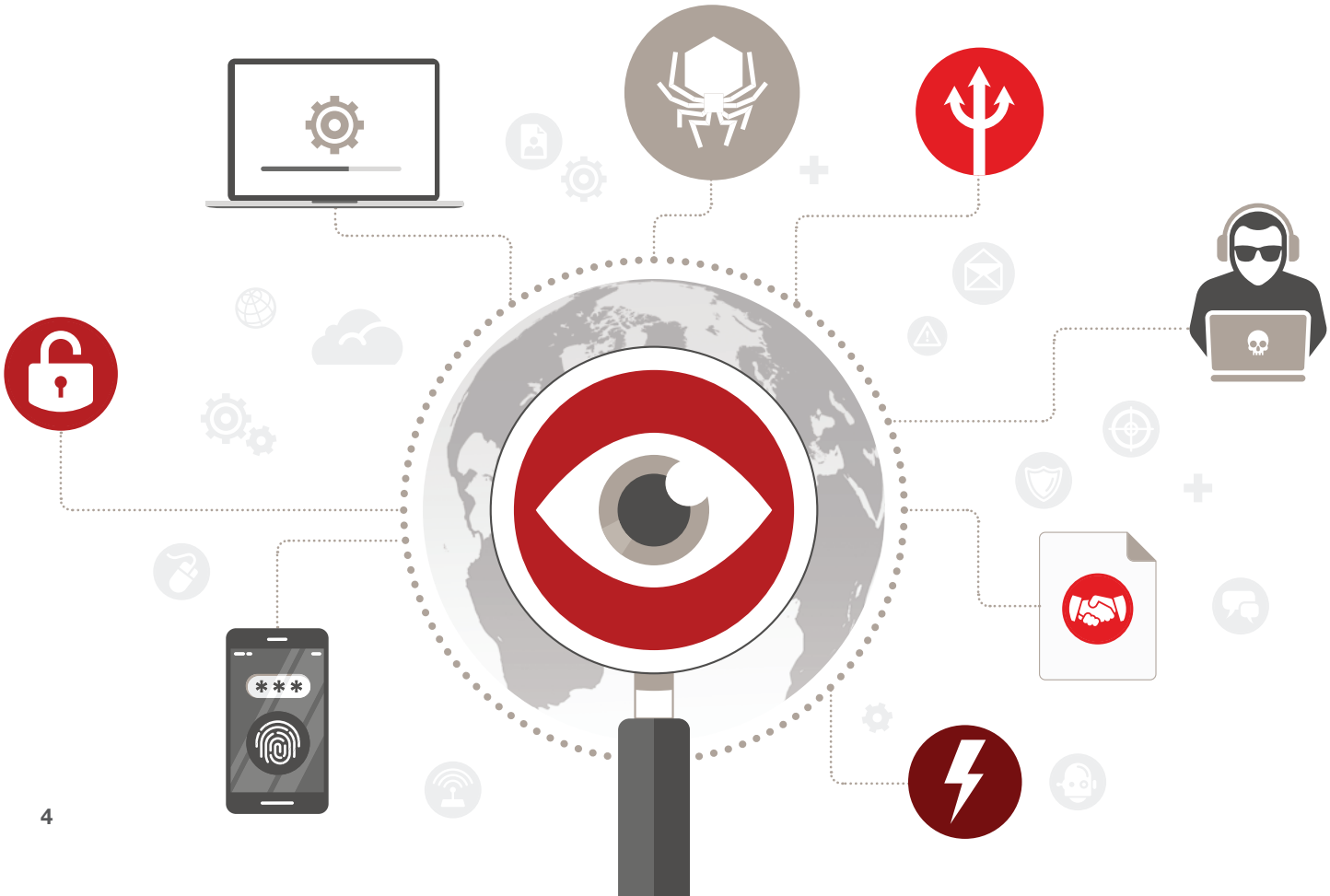
- Bulgarian companies have continued employing a risk-based approach in outlining their economic crime risks (12% increase) in the last two years.
- However, nearly half of the surveyed companies (48%) have not performed general risk assessments. Considering the importance of the risk assessments to reveal potential blind spots, these percentages are still high.

Cybercrime – evolving challenges for companies

- The number of Bulgarian companies having implemented a response plan for cyber threats has increased over the last two years by 20%. Further 12% of the respondents intend to implement such a program shortly.
- Just as much as technology has given fraudsters new means to perform cyber-attacks, it has evolved to help organisations build better fraud prevention strategies. 74% of our respondents in Bulgaria agree that implementing technology in combatting fraud and/or economic crime enables continuous real-time monitoring, while 72% consider that it also provides actionable insight.

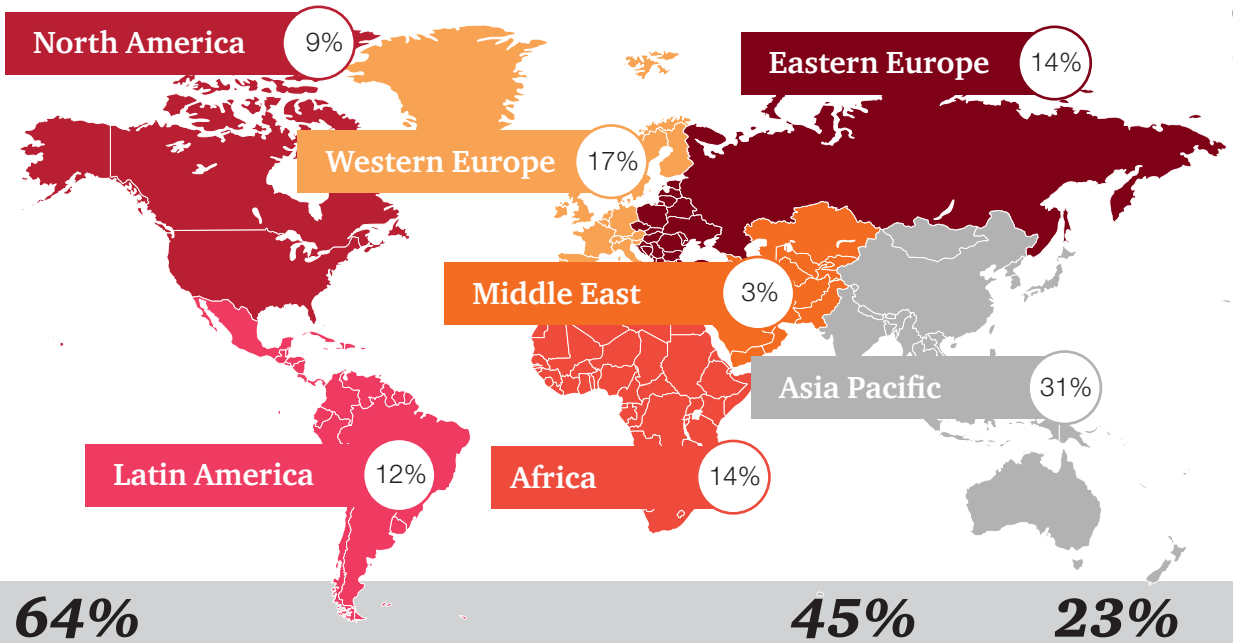
Main perpetrator's profile in Bulgaria differs from the global one

- While more fraud cases perpetrated by external actors in Bulgaria (56% of reported crime), the global scene shows a majority in favour of internal actors (52%).
- Fraud committed by internal actors in the country has halved since 2016 (from 34% to 17% in 2018) mainly as a result of tailored specific policies to address general fraud (nearly half of the local participants).



About GECFS 2018

Figure 1: Participation data



7,228
Completed Surveys

123
Countries

Surveyed in
18
Different languages

64%
of respondents in Executive Management, Finance, Audit, Compliance or Risk Management

45%
C-suite

23%
Head of Department or Business Unit

Bulgarian Participation Statistics

Figure 2: Surveyed industries in Bulgaria in 2018 and 2016

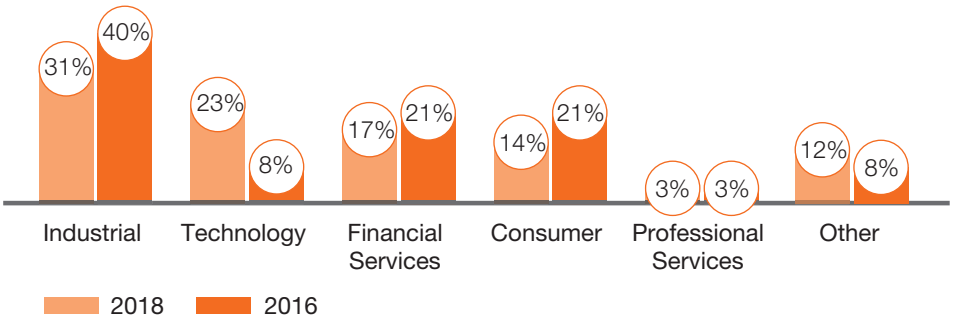
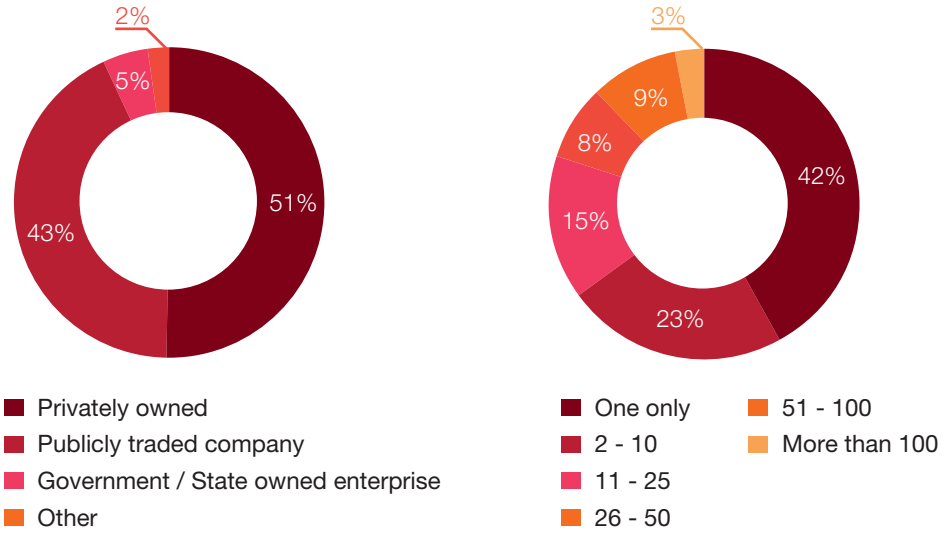


Figure 3: Surveyed organisations in Bulgaria in 2018 – ownership structure and number of countries with offices



The ninth Global Economic Crime and Fraud Survey was carried out by PwC during the period between June 2017 and September 2017. It is the largest survey of its kind with 7,228 survey participants from 123 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. It is comprised of 48 questions divided into seven sections: Organization profile; Fraud & Economic Crime Trends; Technology / New disruptive technologies; Profile of the Perpetrator; Business Ethics & Compliance Programs; Regulations - Anti Money Laundering; and The Global Context.

State of Economic Crime and Fraud in Bulgaria

Actual reported incidents and awareness of fraud

This year 31% of respondents to our survey in Bulgaria said that their companies had been victims of fraud or economic crime, down from 38% in 2016. To the contrary, the reported experienced fraud or economic crime globally is 49% (an increase of 13% since 2016). Does the result in Bulgaria reveal an actual decline in fraud in the country or it is signal of a lower awareness of fraud?

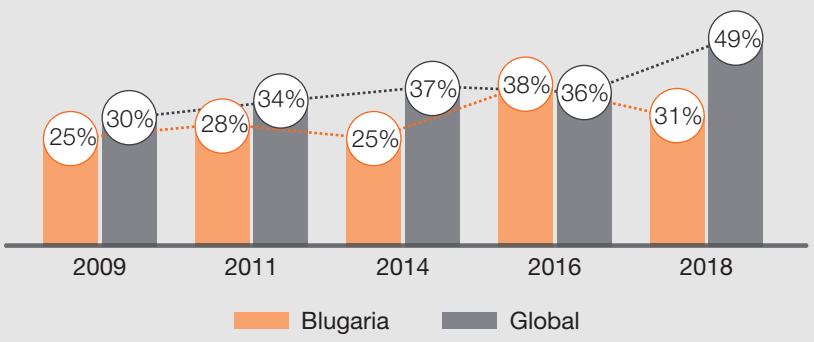
One reason behind the results in Bulgaria that might come to our mind can be evident – there is less economic crime.

Another reason could be the fact that the half of surveyed organisations have relied on utilisation of corporate controls for detecting occurrences of fraud. This is a positive trend outlined by our 2016 report and it is encouraging that a continuous growth in the area is observed now.

It could be argued however whether the controls introduced by organisations are effective. This argument could become stronger when put into the context of the global rate of 49% reported cases of fraud. Even the SEE level (39%) is higher than the result in Bulgaria.

The sharp increase in the "don't know" responses in this year survey (from 3% in 2016 to 25% in 2018) may also have influenced the rate of reported fraud cases. From our experience – not only with Bulgarian businesses but also worldwide - we know that organisations are vulnerable to blind spots, which usually become apparent only after an incident.

Figure 4: Reported rates of economic crime globally and in Bulgaria

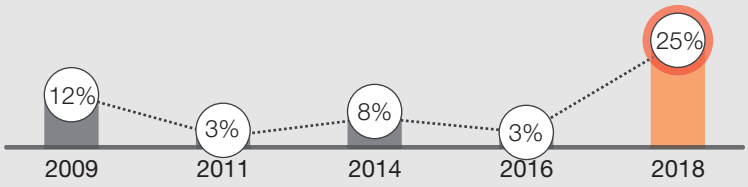


Throwing light onto blind spots before anything happens has proven to be less costly than responding to actual incidents

The increase of the "don't know" respondents' category (by 8 times since 2016) outlines a concerning trend in Bulgaria as the percentage is significantly higher than the globally reported level of 7% in 2018.

Combined with the fact that 60% of our local participants are part of multinational organisations, this suggests that businesses in general may have been still experiencing difficulties in sharing alerts and findings on fraud across entire organisation.

Figure 5: "Don't know" rates in Bulgaria over the years



Prevailing Types of Economic Crime

This year's survey introduced two new types of fraud as options for respondents– fraud committed by the consumer and business misconduct.

Of the respondents who indicated their companies experienced fraud in the last two years, 45% reported fraud committed by the consumer, which, as a result, tops the list of most frequently reported frauds in Bulgaria toppling asset misappropriation from its traditional leading position. The second most reported type of economic crime and fraud is bribery and corruption (40%), followed by cybercrime (30%).

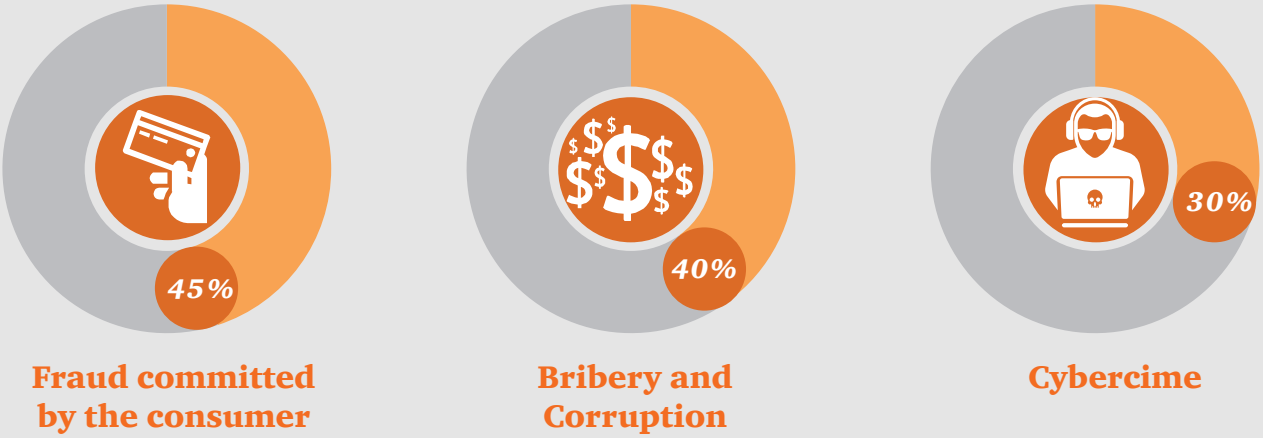
For the first time, asset misappropriation is far behind the top three most common types of fraud in Bulgaria. Out of the respondents who have experienced economic crime/fraud in the last two years, 25% have placed this "old school" type of fraud in fourth position in Bulgaria. The decrease in the percentage (down from 66% in 2016) is consistent with the observed global trend and indicates a shift to more sophisticated types of fraud.

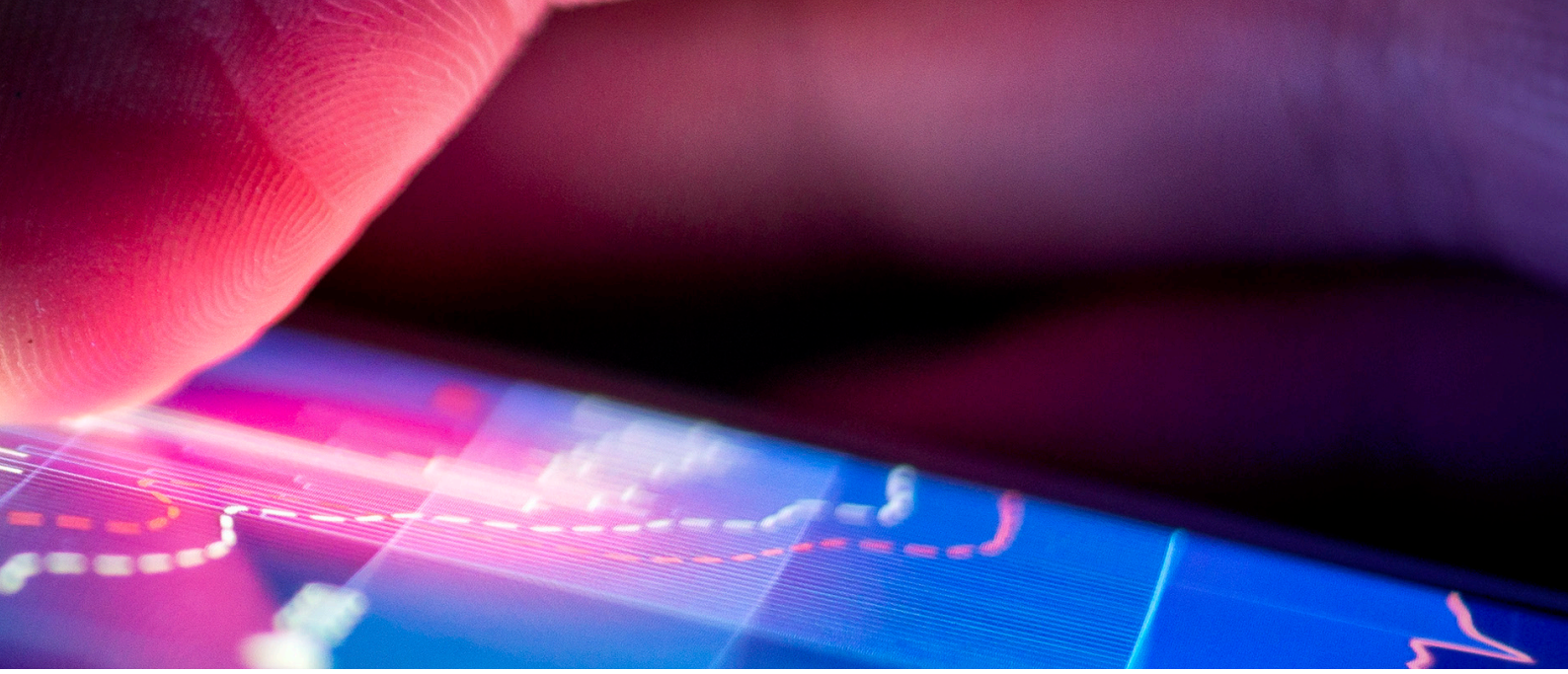
#1 Economic crime/ Fraud in Bulgaria – Fraud committed by the consumer

Fraud committed by the consumer is considered to be fraud against a company through illegitimate use of, or deceptive practices associated with, its products or services by customers or others. Examples of such fraud include mortgage fraud and credit card fraud. Considering that 23% of the survey respondents in Bulgaria represent the technology sector and another 17% are operating in financial services, it is not surprising that almost 50% reported their organisations have been victims of this type of fraud. The lack of effective mechanisms to check business partners and their integrity prior to start working with them may have also contributed to the top scoring of fraud committed by the consumer.

Fraud committed by the consumer is strongly leading the ranking of most widely spread types of economic crime / fraud within the SEE region while on a global level it accounted for just 29%.

Figure 6: Top three most frequently reported frauds in Bulgaria





#2 Economic crime/Fraud in Bulgaria – Bribery and corruption

Though registering an 8% decrease (vs 2016 results), bribery and corruption remain the second most reported crime/fraud in the country.

Considering the SEE reported rate of 16% and the global rate (25%), there is no doubt that bribery and corruption has been seen as one of the largest risks in doing business globally.

The result in Bulgaria is probably of little surprise as corruption has been a hot topic over the last years. The challenges which the country generally faces in the fight against corruption and the common perception of it could be part of the reasons for the high occurrence of this type of crime. Corruption and bribery are often highly publicised, yet sometimes difficult to prove.

#3 Economic crime/Fraud in Bulgaria – Cybercrime

This year's survey provides a very broad definition of cybercrime:

Any criminal offense committed by or facilitated through the use of computer equipment

As simple as this may sound, dealing with it is far more challenging. To top the constantly evolving technology, industry lines today become more and more blurred – non-financial services enter the area of payment systems (Directive (EU) 2015/2366 on payment services). Not being heavily regulated up to this moment might reveal a lack of advanced anti-fraud measures and culture and a more shallow knowledge of money laundering risks or data protection rules.

In Bulgaria, cybercrime climbed to the third most prevalent economic crime in just two years. The fact that in 2016 40% of our respondents were unsure whether cybercrime was likely to happen in Bulgaria, and in 2018 it scores as the third most reported crime is probably one of the best illustrations of how dynamic and evolving the situation is.

When looking ahead, 23% of our respondents consider it as most likely to be the most disruptive economic crime in the next 24 months, putting it at the top of the list. In fact, cyberattacks have become so pervasive that measuring their occurrences and impacts is becoming less strategically useful than focusing on the mechanism that the fraudsters used in each case.

Where to look for fraud?

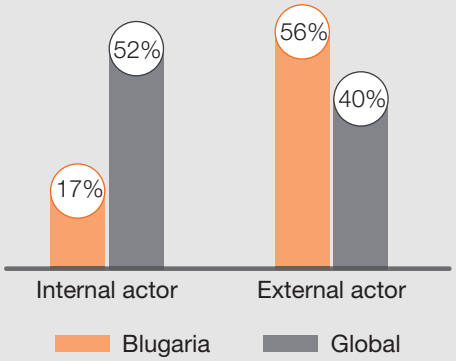
Our survey revealed that in Bulgaria the economic crime committed by internal actors has decreased twice since 2016 (from 34% to 17% in 2018). The result can be attributed to enhanced controls implemented by companies. Alternatively, as the awareness levels within organisations seem to have lowered, less fraud is detected, thus, creating a perception that internal actors do not commit fraud. Which brings in to question whether there is a gap between perception and reality.

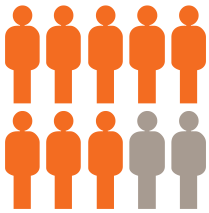
On the other hand, fraud committed by external actors has increased from 48% to 56% in 2018. Having in mind that the most reported economic crime is fraud committed by the consumer, this is probably of little surprise. Furthermore, according to 80% of those respondents who reported external actors as perpetrators of the most disruptive crime, customers were seen as most probable to have committed the crime. This result emphasises one of organisations' biggest fraud blind spots – business partners or so-called *frenemies*. Those include third parties with whom companies can have regular and profitable relationships such as agents, vendors, shared service providers and customers. In other words, the people and organisations with whom a certain degree of mutual trust is expected, but who may actually be stealing from the company.

Which measures are companies enforcing to prevent this from happening? Implementing a 'know your customer' (KYC) approach might turn out to be beneficial for mitigating this risk. Focusing on improving the processes of identifying and verifying the identity of customers, vendors, agents and intermediaries decreases the risks of potential blind spots for the businesses.

Due diligence of third parties before a business relationship can be adopted to mitigate risks, including reputational ones. Should an organisation start a business relationship, being aware of only fragmented information about what has happened, it could be exposed to a serious reputational risk. It can find itself punished from all quarters for its perceived inability to respond appropriately – well before the board has a plan for what to do. In Bulgaria we have seen a couple of similar examples in recent years.

Figure 7: Main perpetrators of fraud globally and in Bulgaria for 2018





80%

of the external actors committing fraud in Bulgaria are customers

Effects of economic crime

When speaking of economic crime or fraud, costs of it are an inseparable part of the discussion. There is no doubt that sometimes it is difficult to assess the losses – may be not so much in financial terms, but as indirect loss as well. 35% of the Bulgarian respondents who experienced fraud reported losses mostly between 100,000 to 1 million US dollars. Nevertheless, 10% of them claimed that the amount is immeasurable indicating for collateral damages such as degraded employee morale, damaged business relationships, worsened relations with regulators, etc.

The Bulgarian organisations who suffered from economic crime/fraud in the last 24 months noted that the most disruptive crime has affected their business relations (80%) and employee morale (50%). The results are consistent with the global rates of 67% and 78%, respectively.

Figure 8: Financial impact of economic crime

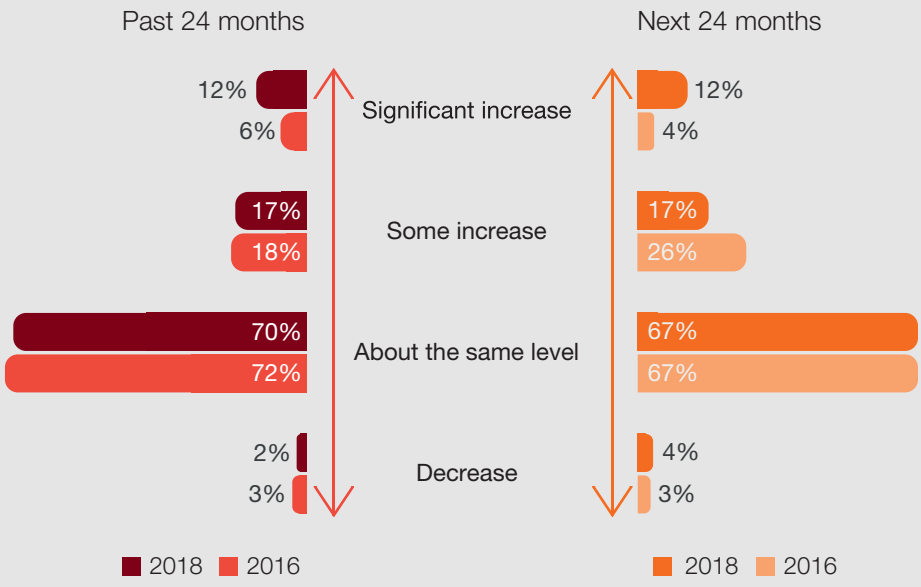
The financial impact of fraud involves not only direct losses suffered by victims, but also additional costs incurred by organisations for investigation and remediation

Combating Economic Crime and Fraud

The fight against fraud is a constant struggle and organisations must not drop their guard, meaning they should constantly invest both in people and technology.

Seven out of ten of the Bulgarian surveyed organisations noted they spent about the same amount of funds to combat economic crime/fraud in the last 24 months as before. Furthermore, 67% of respondents believe that their spending in this regard would be the same in the next two years. Could it be that companies developed a sense of security that would mislead them? As noted, technologies evolve and fraudsters are fast to adapt.

Figure 9: Organisations' spending on combatting fraud



Fraud Prevention

As in 2016 (just a marginal 2% drop is registered) this year survey reveals that the majority of participants in Bulgaria (75%) understand that having formal business ethics and compliance programmes is a "must-have" step towards better fraud prevention – but far from self-sufficient. We note that a sizeable number of the Bulgarian organisations who have enforced compliance programmes have not enforced specific anti-fraud provisions. For instance, out of those having a formal compliance programme 35% do not yet have specific policies addressing general fraud. Further, no more than 17% of the respondents' compliance programmes provide for tailored controls on general fraud.

Considering that fraudsters embrace new and more sophisticated means to achieve their goals, a "tick-the-box" or "only on paper" approach to compliance would render it inefficient. Adequately tailored controls and sufficient resources (human and technology) would actually be beneficial to those compliance programmes in terms of minimising existing blind spots.

As the fraud risk profile in any market is dynamic and likely to change over time, risk assessments are another pre-requisite for efficient fraud prevention and detection as they help organisations identify unique and specific risks. In this regard, only half of Bulgarian organisations (52%) said they had conducted such an assessment in the last two years and only 40% have assessed their vulnerability to cyber-attacks. Less than half of the organisations (40%) have conducted an anti-bribery/anti-corruption risk assessment, which is worrisome as this type of economic crime ranks second in the most frequent ones in the country.

It should be noted however that the number of Bulgarian companies that have not performed any risk assessment has continued decreasing in the last two years, registering a level of 14% (vs. 26% in 2016).

Yet, the majority part of performed risk assessments have been done either as part of organisations' annual or routine processes (66%) or as part of their audit plans (49%) or as part of their Enterprise Risk Management (ERM) strategy - 43%.

In view of the above, we strongly encourage all organisations to implement risk assessments on a regular basis.

When it comes to acquisitions and other transactions — with the risk of 'buying' successor liability and bad controls — a fraud risk assessment is even more critical, as part of pre-deal due diligence. Enhanced fraud, cyber and anti-corruption due diligence will allow acquirers to better recognise what risks they face and how they can either be carved out of a deal or remediated post-deal.

As part of their acquisition process, Bulgarian organisations as well as their global counterparts, mostly perform regulatory compliance and tax compliance due diligences. Anti-bribery and corruption and cybersecurity due diligences are done less frequently in Bulgaria than globally.

Besides investing in developing an internal culture and processes to prevent economic crime and ensuring staff are trained to be fully aware of their legal and ethical obligations, companies also have to be aware of external threats. Our survey again showed that the most serious economic crimes experienced by Bulgarian organisations were perpetrated by external entities or individuals. This means that developing mechanisms to minimise external threats has to become an imperative for Bulgarian organisations.

Figure 10: Organisations with formal business ethics and compliance program in Bulgaria

Fraud Detection

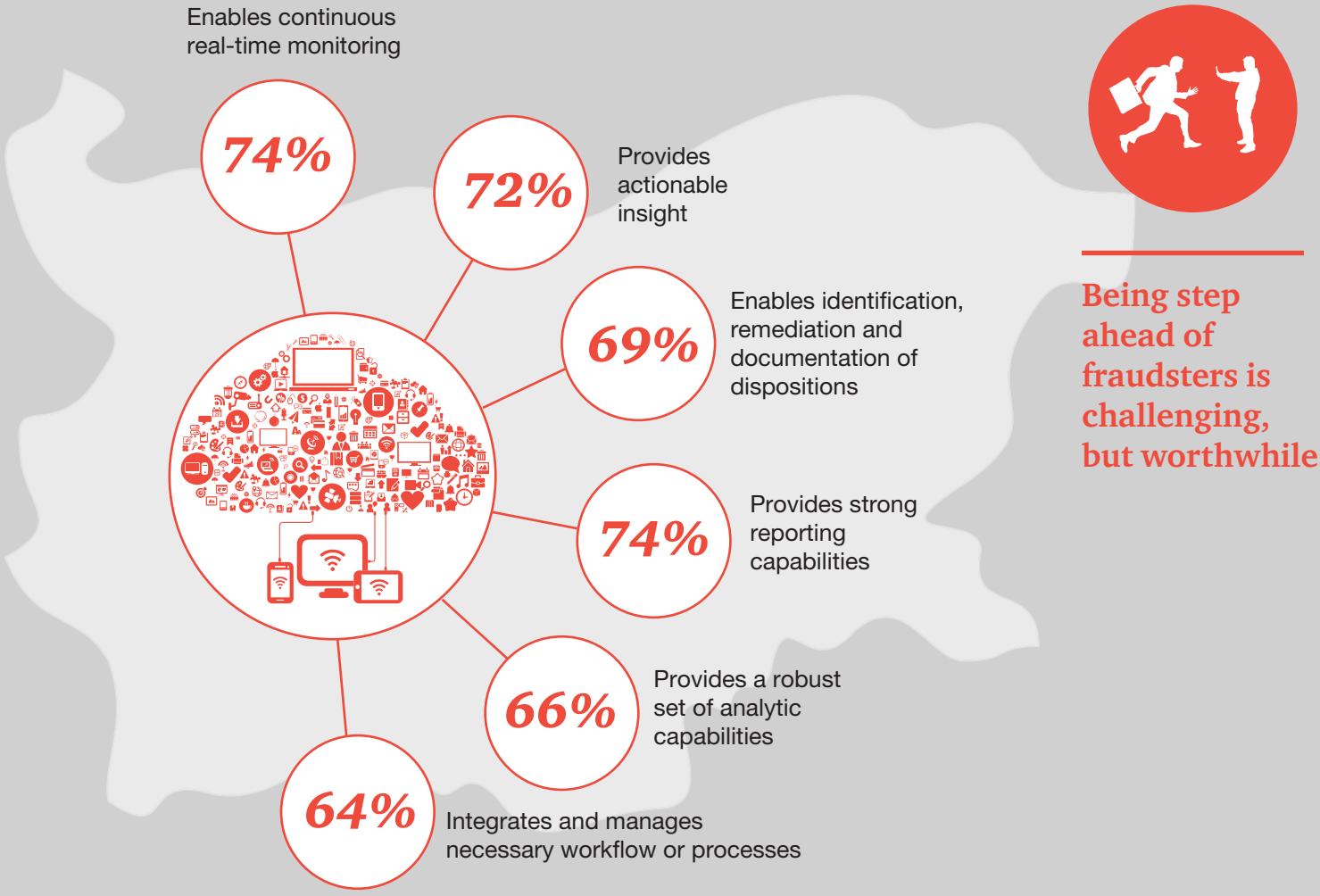
In the fight against fraud, organisations today have at their disposal ever-more powerful technologies aimed at monitoring, analysing, learning and predicting human behaviour. And the data shows they are using them.

74% of our respondents in Bulgaria agree that implementing technology in combatting fraud and/or economic crime enables continuous real-time monitoring, while 72% consider that it also provides actionable insight. To put this in a practical perspective, more than half of the respondents are using continuous monitoring in their control environment and another 8% plan to do so in the next 12 months. Almost a quarter of the companies use or plan to use artificial intelligence to combat fraud, which is in line with the global tendency (25%).

Technology can enable effective proactive action and reduce the occurrence and costs of economic crime, but it comes with its own costs for the company. In the end, the challenge lays in finding the (hopefully) perfect balance between a technology's effectiveness and its cost while remaining ahead of the fraudsters.

The growing threat of cybercrime is recognised by Bulgarian companies – the number of those having implemented a Cyber Security Program ("CSP") has increased over the last two years by 20% (up to 57% in 2018). A further 12% of respondents intend to implement such a program shortly. The main elements of the CSP that Bulgarian organisations have are cybersecurity policy, designated Chief Information Security Officer (that usually reports to the Board level executives), cybersecurity personnel and cybersecurity training and monitoring for staff.

Figure 11: Organisations find value in using technologies to combat fraud*



Being step ahead of fraudsters is challenging, but worthwhile

* A multiple choice question

Regulatory and enforcement efforts

When it comes to sharing information concerning a suspicion of or subjection to cyberattacks with enforcement authorities, 37% of our respondents in Bulgaria claim that it is likely that this will happen. This is almost half the global level. What is more worrying is that almost the same percentage of the respondents (35%) noted this as neither likely nor unlikely. Out of those who consider this unlikely, 74% do not believe law enforcement agencies have required expertise and 39% consider the risk of uncontrolled public disclosure as high.

Thinking Ahead

54% of the Bulgarian respondents consider that changes in the regulatory environment have an increasing impact on their organisations, while only 36% responded that changes in the enforcement of regulation in their organisations would have greater impact. These results align with the perceptions of organisations being re-active and not so pro-active regarding fraud prevention. The potential concerning point here is that this might lead to a grey area inhabited by blind spots for the organisation.

When asked about disruptive or serious fraud and/or economic crimes that their organisation will experience, 23% of Bulgarian companies indicated cybercrime. Considering the ever-evolving nature of technology, the re-activeness of organisations seems like a far more worrying situation. Possible vulnerabilities of controls could become an easy target of fraudsters.

Shining a light on blind spots and having a clear understanding of what constitutes fraud would unlock significant opportunities for companies, for instance making the business stronger and acting in a more strategic way. This includes a focus not only on improving controls intended for preventing fraud committed by external actors, but also on creating a cohesive and resilient culture within the company. Overall, pro-activeness could pull fraud out of the shadows and minimise the blind spots.

Figure 12: Economic crime most likely to be the most disruptive over the next two years

Be prepared
Face the fraud
Emerge stronger

Forensic Contacts for Bulgaria

Albena Markova
Partner
Consulting Services Bulgaria
albena.markova@pwc.com
Tel: +359 2 9355 200
Mobile: +359 897 921 094

Reneta Mamassian
Manager
Forensic Services, Bulgaria
reneta.mamassian@pwc.com
Tel: +359 2 9355 200
Mobile: +359 896 693 485

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.

www.pwc.com/fraudsurvey