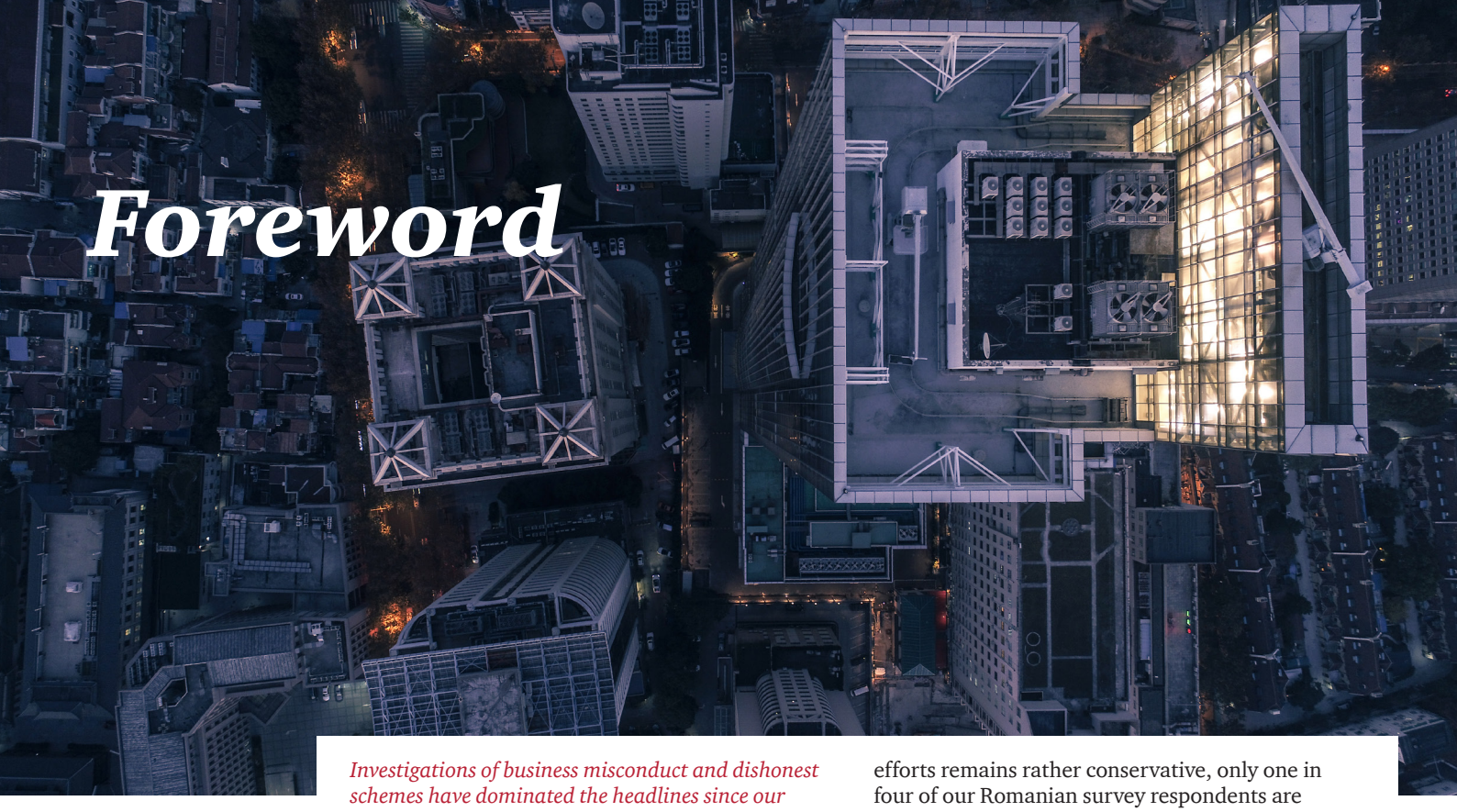
www.pwc.ro
April 2018

Global Economic Crime and Fraud Survey 2018

A front line perspective on fraud in Romania

pwc

Contents



Foreword

Investigations of business misconduct and dishonest schemes have dominated the headlines since our last survey. Romanian organizations have seen their reputation affected as fines were imposed by authorities. In some cases, executive directors/ owners were prosecuted and even sentenced to prison.

Per A. Sundbye
Partner,
Forensic Services
Leader in South-East
Europe (SEE)

Ana Sebov
Director,
Forensic Services
Leader in Romania

Our respondents tell us that 42% of surveyed organizations experienced economic crime. The true fact is that there is an increased public awareness of economic crime nowadays not just in Europe, but also in Romania. On one side, one can easily build an impression that fraudulent actions increased compared to previous years. On the other side, it can be a result of improved detection tools and a stronger determination to deal with the problem. Our experience supports the latter.

Not surprisingly, our respondents express particular concern about cybercrime, which is no longer a hollow word to be ignored. Cybercrime emerged as the second most frequent economic crime among Romanian respondents and the most disruptive in terms of impact.

Moreover, increased use of technology in every aspect of business operations has contributed to new developments around fraud risk management. In the current reality where most economic crimes have, to some extent, gone digital, and the technical sophistication of fraudsters continues to grow, investing in new technologies to combat fraud, including “old school” crimes, has become imperative.

While organizations have made some investments towards mitigating the risk of fraud, there is room for improvement regarding the specific measures implemented in light of the fast changing Romanian economic environment. Budgeting for anti-fraud efforts remains rather conservative, only one in four of our Romanian survey respondents are considering some increase in their investigative and compliance spend. To increase awareness of companies as to the fraud risks they are exposed to and help them elaborate a mitigation plan, there is a need for quality guidance.

It is with great pleasure that we present the 2018 Global Economic Crime and Fraud Survey, the largest survey of its kind. In Romania, 60 leading companies shared their experience with economic crime and how it may impact doing business in Romania. This provides us with unique insights into the current state of economic crime in this country as a whole, and the real life impact witnessed by each individual organization. It also allows us to identify trends and perception of future risks.

We would like to thank those individuals who took the time to respond to our survey. Without their support, a report for Romania could not be issued. We invite all business leaders to read this survey and share best practices in preventing and detecting fraud with other organizations. We trust you will find it a useful tool to assist in your battle against fraudulent actions and to contribute to an enhanced awareness of fraud risks in Romania.

Key Findings on the State of Economic Crime in Romania

General economic crime trends

- Economic crime continues to be a key issue for Romanian respondents. 42% of surveyed organizations have reported that they were subject to economic crimes in the last 24 months, a significant increase compared to the 2016 study (17%). Although the reported rate of economic crime in Romania is lower than the global (49%) and regional[1] (47%) results, it may be that fraud incidents are not always detected.
- Fraud committed by the consumer, cybercrime and business misconduct are the most common types of fraud reported in Romania. Asset misappropriation, the traditional leader in this category, fell into fourth place. In terms of the impact on the organization (monetary or otherwise), Romanian respondents have acknowledged cybercrime to have had the most disruptive effect on business operations.
- Romanian companies view cybercrime and fraud committed by the consumer as the main risks they will be faced with in the area of economic crime.

Cyberwarfare: threats and opportunities

- 65% of Romanian companies have been targeted by cyber-attacks in the last two years, in line with global and regional reported rates. Most common mechanisms used by attackers reported by over a third of Romanian respondents are phishing and malware.
- Cyber-attacks most frequently caused disruption of business processes, in almost half of the cases reported by Romanian companies. Cyber incidents also led to substantive losses to organizations: a quarter of Romanian organizations that were attacked suffered asset misappropriation and were digitally extorted.
- 72% of Romanian organizations reported having a fully operational cyber incident response plan in place. It seems that Romanian companies are becoming more and more alert to such sophisticated incidents and are starting to build the capabilities to detect them and mitigate their impact. While developments are very promising, one question remains: Will your cyber security program withstand the test of reality?
- In the fight against fraud, the future appears bright for technologies based upon artificial intelligence and machine learning. Despite only one in Romanian respondents currently using artificial intelligence in their control environment, the data indicates that a quarter of Romanian organizations plan to use this nascent advance as a tool to combat fraud.

Business ethics and compliance programs

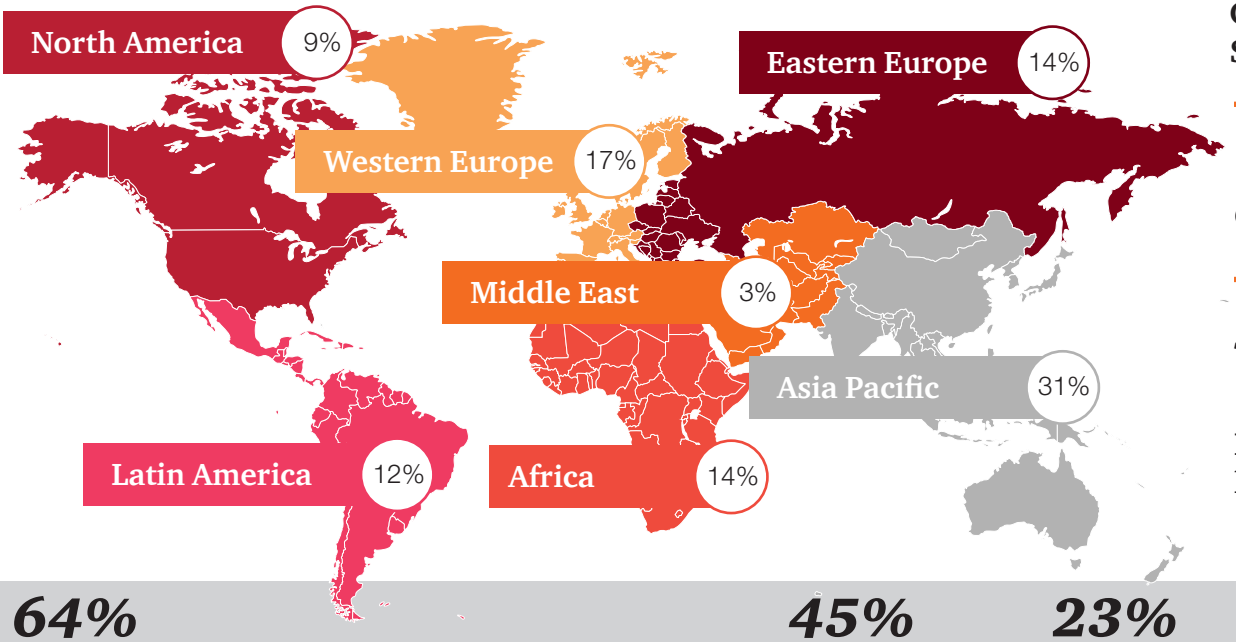
- One in ten Romanian respondents has not performed any risk assessment at all in the last 24 months. While the role of this fraud prevention tool is still largely underestimated, we see an encouraging development overall since our last survey when 24% of respondents reported not having performed such an assessment.
- Less than half of surveyed companies agreed that there are confidential channels in place for raising concerns, including a whistleblowing hotline. Employees may be reluctant to report ethical issues to their superiors or Internal Audit and are more likely to report incidents anonymously or to independent parties.

1. Eastern Europe

About PwC's 2018 Global Economic Crime and Fraud Survey

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.



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

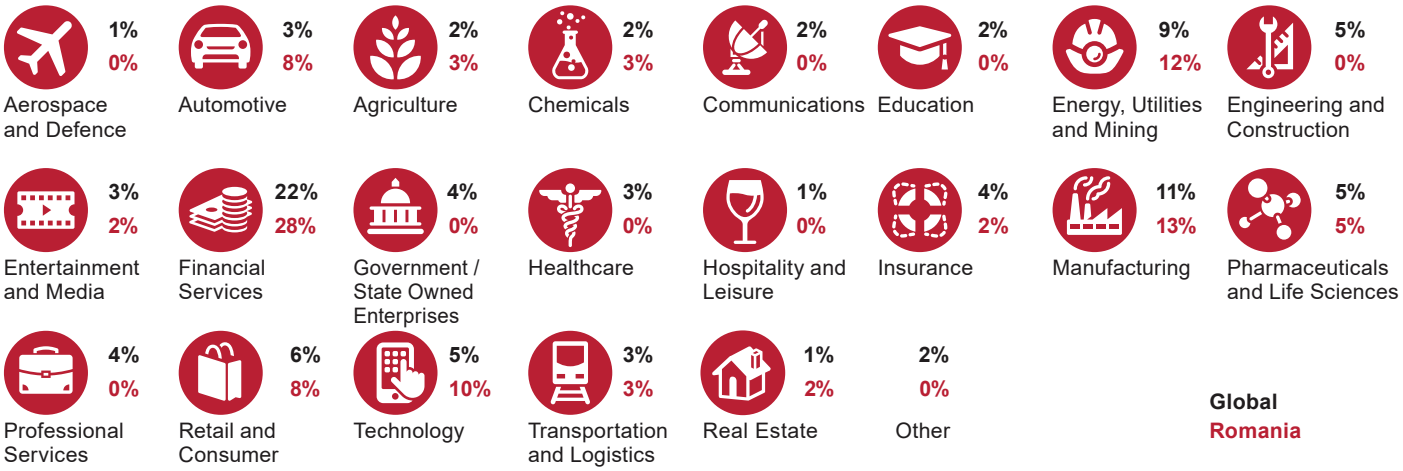
23%
Head of Department or Business Unit

Romanian Participation Statistics

In Romania, 60 companies shared their experience and perception of the economic crime on doing business in Romania and worldwide.

Organizations represented in this survey come from various industry sectors but predominantly from Financial Services, Manufacturing, Energy, Utilities and Mining, Technology, Automotive, Retail and Consumer and Pharmaceuticals and Life Sciences. Figure 1 shows the breakdown of industry sectors represented in Romania in comparison to the global industry representation.

Figure 1 - Surveyed industries in Romania and globally



Predominantly Chief Financial Officers or Controllers participated in the survey (38%), followed by Managers (18%), Heads of Department (12%) and CEOs, Presidents or Managing Directors (10%) (Figure 2).

Figure 3 shows the ownership of the companies surveyed in Romania. Half of them are publicly traded companies (50%), followed by privately owned companies (35%), portfolio companies of private equity funds (13%) and other (2%).

Furthermore, one in three of these companies are Romania based (30%) and around a quarter of them have offices in less than 10 countries (see Figure 4).

Figure 2 - Romanian participants in the survey

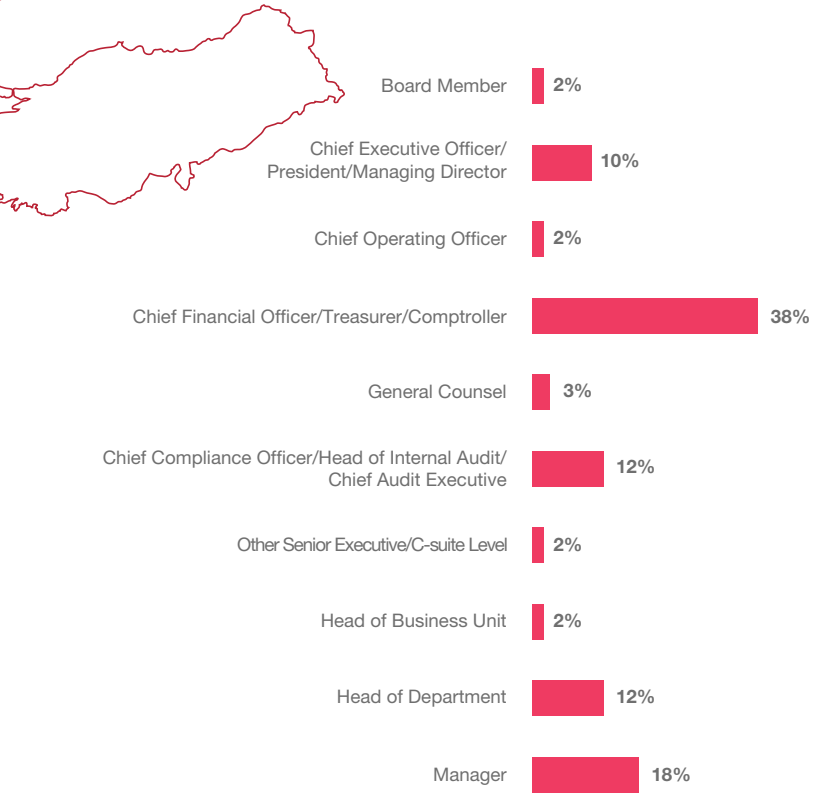


Figure 3 - Romanian companies' ownership

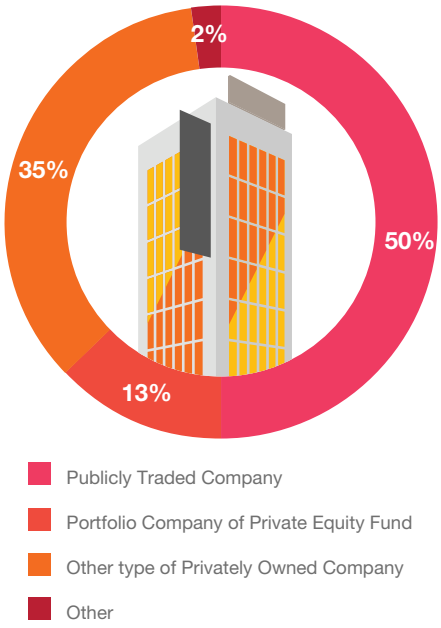
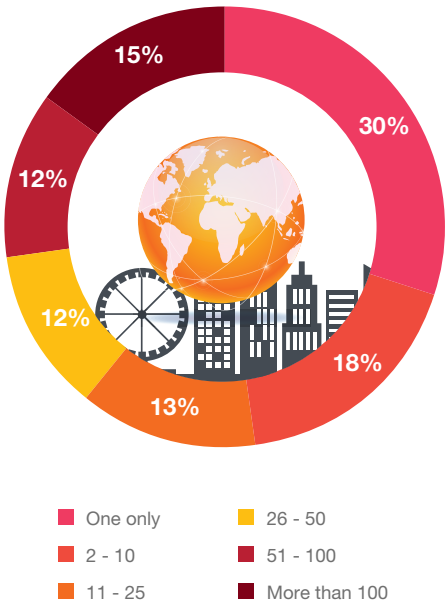
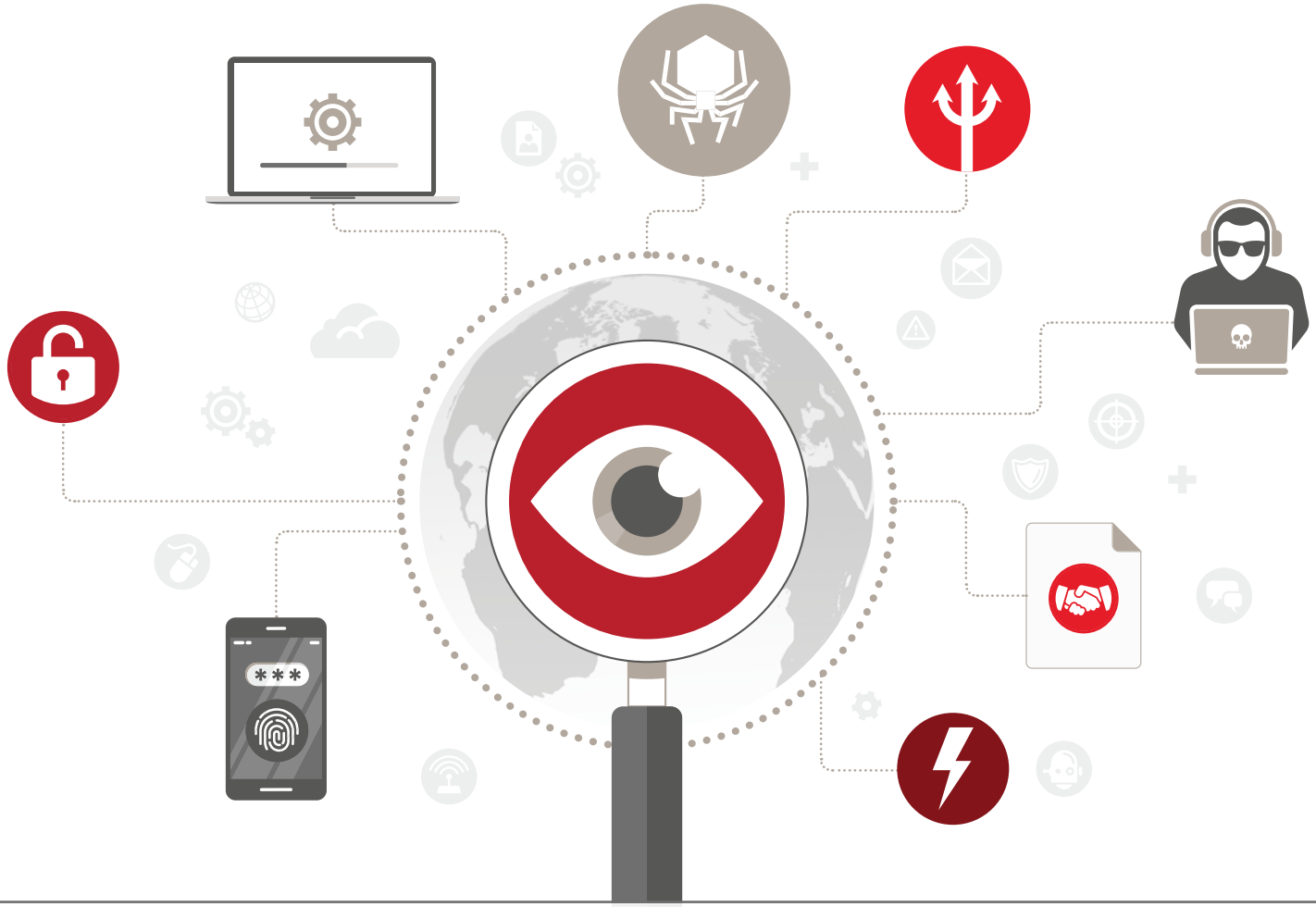


Figure 4 - Number of countries where Romanian companies have offices



General economic crime trends



How big is the problem?

Economic crime continues to be a key issue for Romanian respondents. 42% of surveyed organizations have reported that they were subject to economic crimes in the last 24 months.

Although the reported rate of economic crime is lower than the global (49%) and regional (47%) results, it may be that fraud incidents are not always detected.

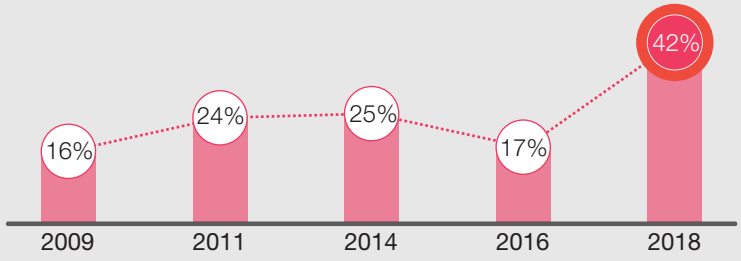
This year's survey results show that the level of fraud reported by Romanian respondents significantly increased compared to the 2016 rate (17%).

Possible explanations for the discrepancy reside in the increased awareness of the benefits of periodic fraud risk assessments coupled with a larger spending to combat fraud.

One in ten Romanian respondents has not performed any risk assessment at all in these 24 months. While the role of this fraud prevention tool is still largely underestimated, we see an encouraging development overall since our last survey when 24% of respondents reported not having performed such an assessment.

In terms of spending, in our 2016 survey 35% of Romanian organizations reported having increased the amount of funds allocated to fight fraud. If we consider that a fraud incident takes on average two years to be detected, the benefits of increased spending in the past are becoming visible now.

Figure 5 - Reported rate of economic crime in Romania



What kind of fraud is being committed?

Fraud committed by the consumer, cybercrime and business misconduct are the most common types of fraud reported by Romanian companies.

Asset misappropriation, the traditional leader in this category, fell into fourth place, only one in three Romanian respondents having experienced this type of fraud in the last 24 months. The downward trend of asset misappropriation could be the result of a tightening of organizational controls – and that Romanian organizations are getting better at preventing traditional economic crime. Emergence of the "new" frauds, fraud committed by the consumer and business misconduct, is also partially responsible for the decrease (from 56% in 2016 to 32% in 2018) in the larger category of asset misappropriation. However, at both global and regional level, asset misappropriation is still the most frequent type of economic crime reported, with 45% and 42% respectively, of occurrences.

Cybercrime does not feature in the top three types of economic crimes experienced in Eastern European countries. At a regional level, incidents of bribery and corruption are more common.

However, Romanian organizations seem to follow the global trend as far as cyber incidents are concerned. With the raising importance of technology in today's economic environment and the extensive adoption of technology-based business models, cybercrime was the second most common fraud experienced by Romanian respondents in the last two years. As the threat is growing, Romanian organizations are becoming concerned about cybercrime, giving it the attention it deserves.

Figure 6 - Top types of fraud affecting Romanian organizations

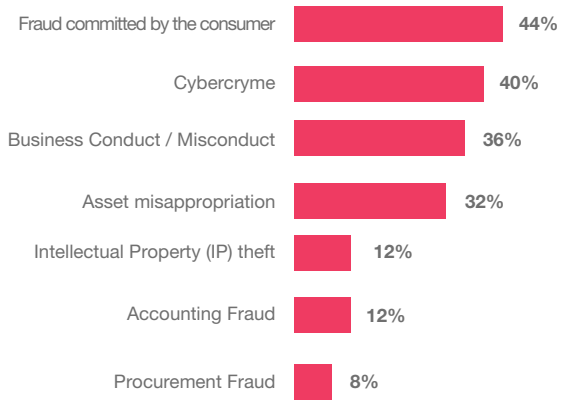
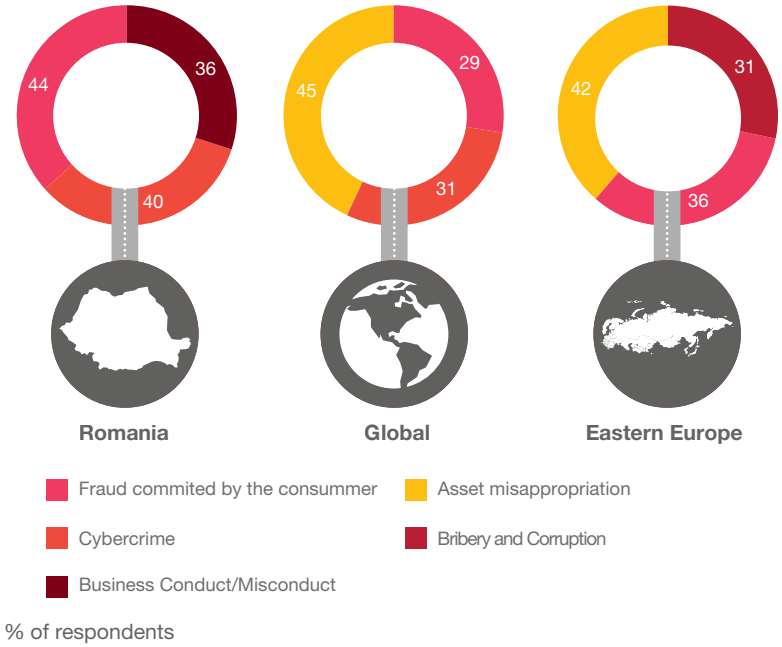


Figure 7 - Top three types of economic crime in the last 24 months

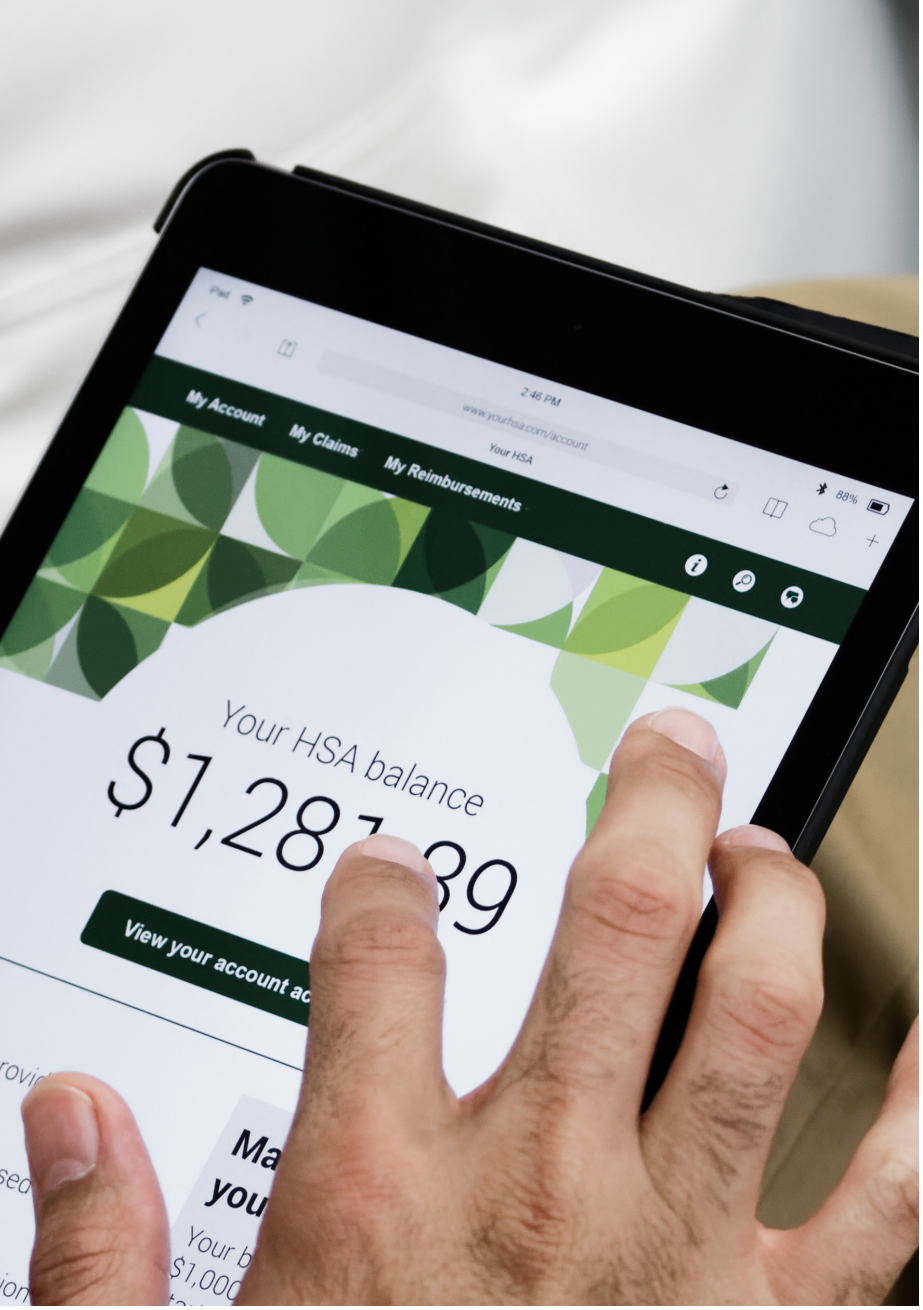


% of respondents

Figure 8 - Top three most pervasive economic crimes reported by Romanian organizations

% of respondents

In terms of the impact on the organization (monetary or otherwise), Romanian respondents have appreciated cybercrime to have had the most disruptive and serious effect on business operations. Though reported as the most common type of economic crime in Romania, fraud committed by the consumer came in second in terms of impact. At global and regional level, the top three list of reported economic crimes was the same from both a frequency and impact point of view.



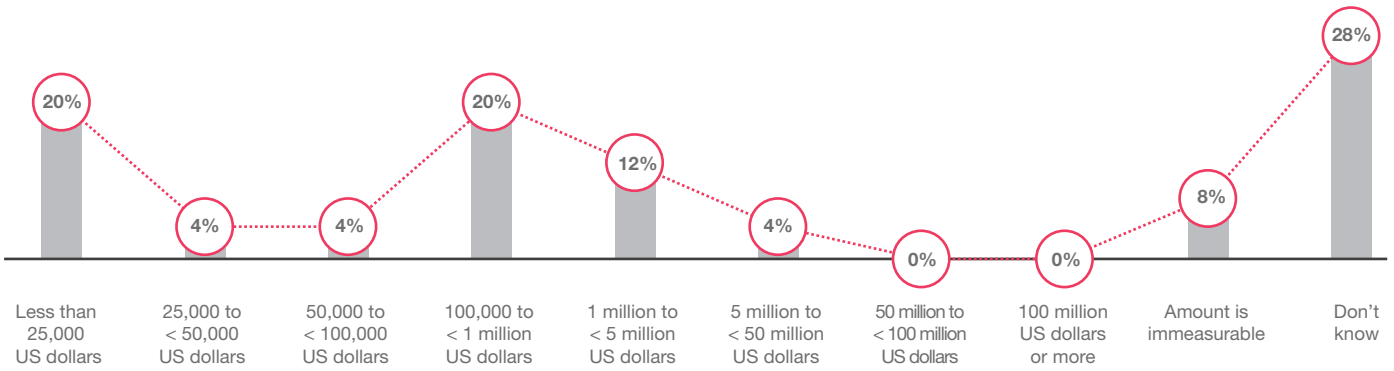
What is the price tag?

The total cost of fraud cannot be determined with precision, mostly because many incidents of fraud remain undetected. Losses can be heavy.

Across the globe, 19% of organizations have incurred losses over $1 million — with 1% recording losses in excess of $100 million over the past two years.

In Romania, organizations experienced losses in less substantial amounts. This year's survey shows that a fifth of Romanian organizations suffered losses of between $100,000 and $1 million, while 16% of respondents reported losses of more than $1 million. These are significant sums of money and are representative of a trend of rising costs of individual frauds.

Figure 9 - Financial impact of economic crime among Romanian respondents

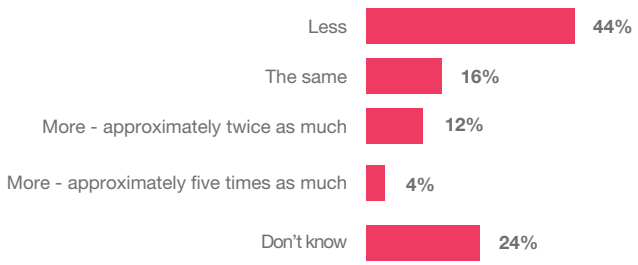


Costs related to fraud incidents are actually significantly higher if we consider investigation related costs such as legal or consulting services. The amount spent by one third of Romanian respondents on investigations and other interventions was either the same as or higher than the amount lost through the crime.

Such secondary costs could go as high as more than 10 times the amount lost through the fraud incident itself. The reported rate in Romania is slightly lower than the regional rate (35%) and significantly below the global one (46%).

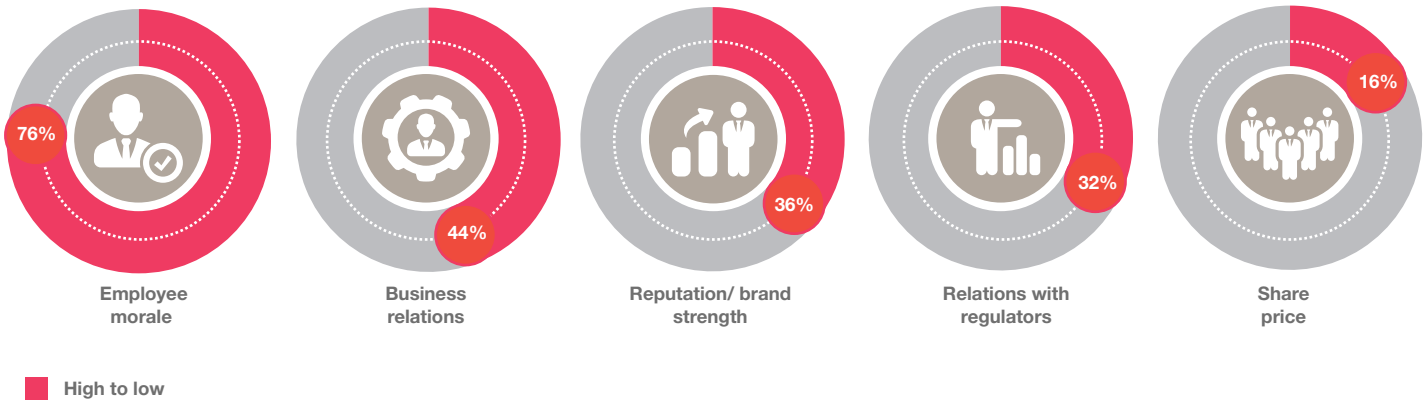
As one in four Romanian respondents were not aware of the extent of amounts involved in conducting such investigations, the accessory costs of economic crime could be even greater. They cannot be ignored. Unfortunately, in some cases, the costs increase as a result of inexperience, lack of focus and crucial mistakes or poor judgement.

Figure 10 - Amount spent by Romanian respondents on investigations compared to amounts lost through the economic crime



However, the true cost of economic crime should not be judged only in monetary terms. There are also other, intangible costs associated with fraud. Irreparable damage to reputation, negative impact on the employees' morale or existing business relations could be even worse than the severe financial losses. Consequences might go as far as bankruptcy.

Figure 11 - Non-financial impact of economic crime among Romanian companies



Cyberwarfare: threats and opportunities

What is at stake?

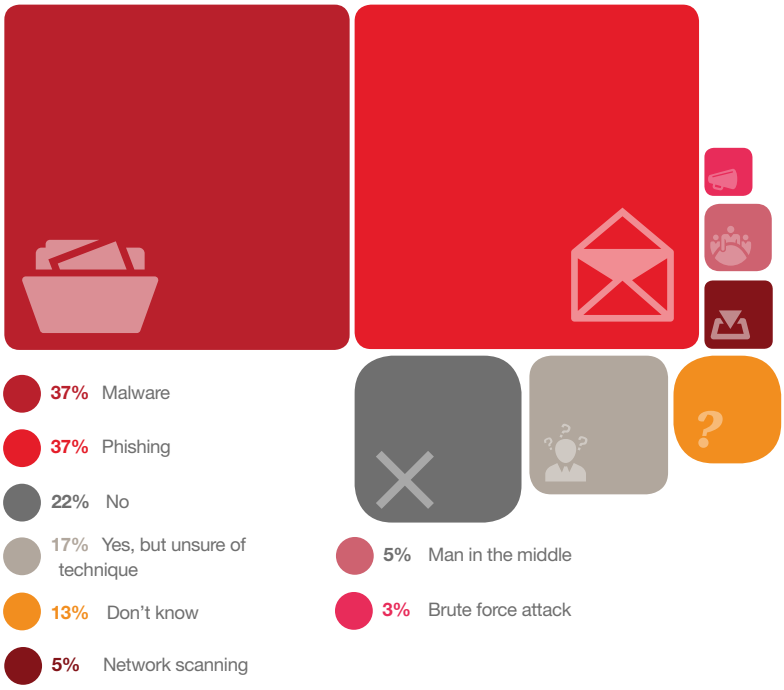
Cybercrime and cyber security are issues that are now at the forefront of everyone. The last two years have proved to be very profitable for cybercrime which jumped to the second most reported economic crime among Romanian companies.

Cyber incidents arise at a higher frequency than ever before, while cyber attack methods continue to advance, creatively escaping existing security measures. According to our study, two out of three Romanian organizations have been targeted by cyber-attacks in the last 24 months. This is in line with global (64%) and regional (65%) reported rates.

Cyber-attacks have become so pervasive that quantifying their manifestations and effect is becoming less strategically important than focusing on the specific techniques used by the fraudsters. Most common mechanisms used by attackers reported by over a third of our survey respondents worldwide are phishing and malware, with Romanian statistics following global trends.

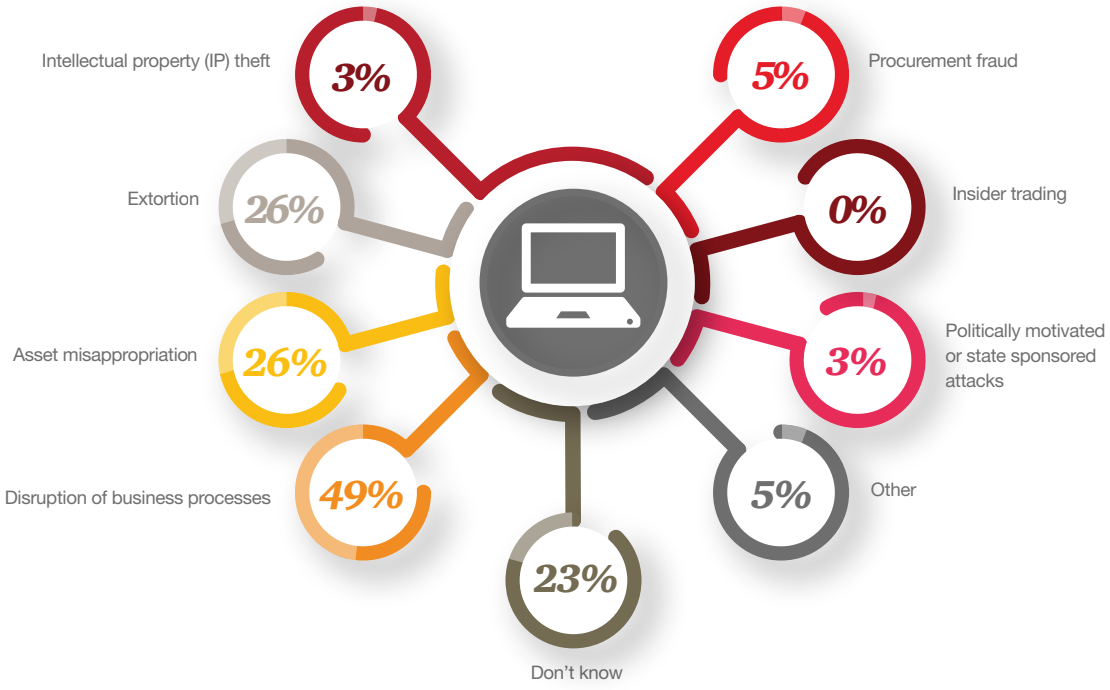
A successful cyber-attack can severely impact a business. Almost half of the Romanian survey respondents have experienced disruption of business processes. The reported rate by Romanian companies (49%) is significantly higher than the global (30%) and regional (36%) results.

Figure 12 - Cyber-attack techniques affecting Romanian respondents in the last two years



But the consequences of cyber-attacks do not stop here. Most of such security breaches also led to substantive losses to organizations: a quarter of Romanian organizations which were attacked suffered asset misappropriation and were digitally extorted.

Figure 13 - Types of fraud experienced by Romanian organizations through a cyber-attack



The art of cyber defense

To stay one step ahead of cybercriminals, businesses should stay alert to the ever-evolving threat landscape. Organizations that understand the specific cyber risks they face can work to actively prevent those risks, for example by instructing their employees to decrease the amount of potentially damaging actions such as responding to phishing attacks or clicking on malicious web links.

Cyber threats must be recognized and addressed in much the same way as any other business risk with an incident response plan, roles, responsibilities and monitoring tools.

It seems that in the past two years Romanian organizations have been more and more the target of sophisticated incidents such as cyber-attacks and, as such, have started building the capabilities to detect them and mitigate their impact. This year's survey shows that over the last 24 months, 59% of Romanian companies have assessed their vulnerability to cyber-attacks.

Moreover, 72% of Romanian organizations reported having a fully operational cyber incident response plan in place. The fact that the number of businesses prepared to deal with cyber-attacks almost doubled in the last two years confirms the elevated level of awareness about the growing threat of cybercrime incidents among Romanian executives.

Implementing an effective cyber security program has become a top priority for Romanian companies. Central elements of the cybersecurity and incident response strategy adopted by Romanian businesses include: cybersecurity policy, network monitoring appliances, cybersecurity personnel and training exercises, penetration testing and vulnerability assessments, application security and breach notification protocols.

Figure 14 - Romanian organizations having a Cyber Security Program in place

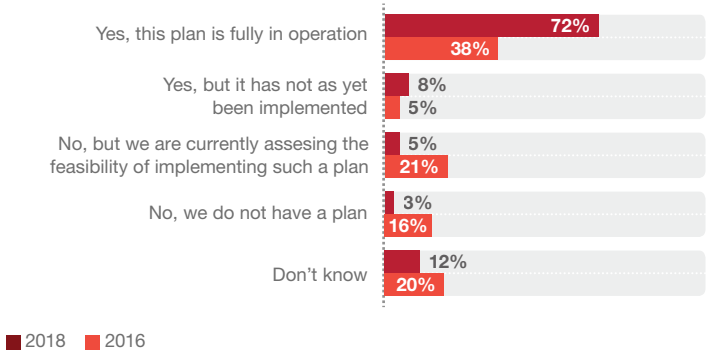
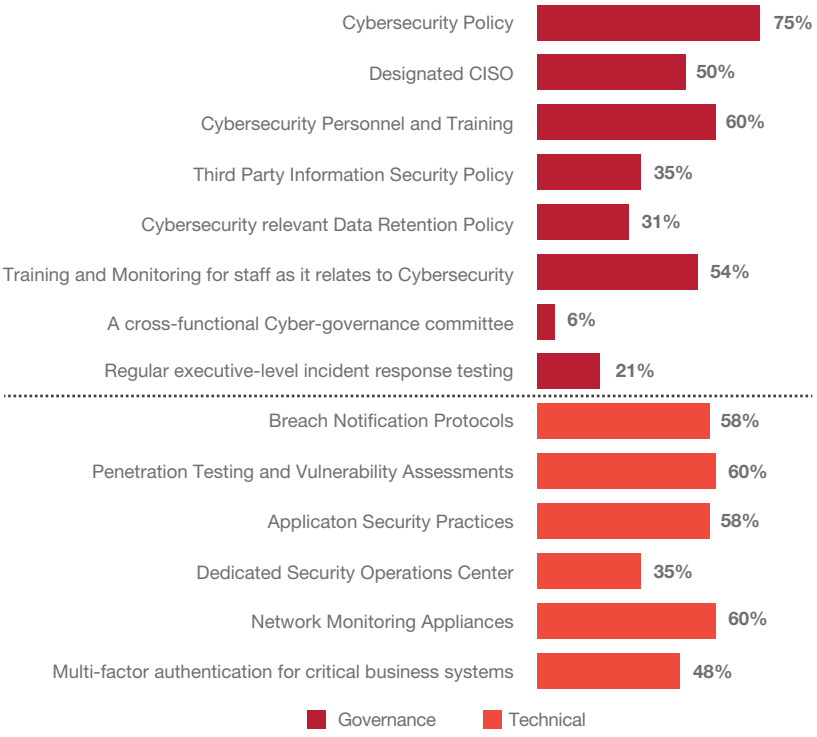


Figure 15 - Key elements of the Cyber Security Program among Romanian respondents



Evolution of cyber preparedness is also positive at global and regional level, with 59% and 60% of organizations respectively, having put into effect a cyber-response plan.

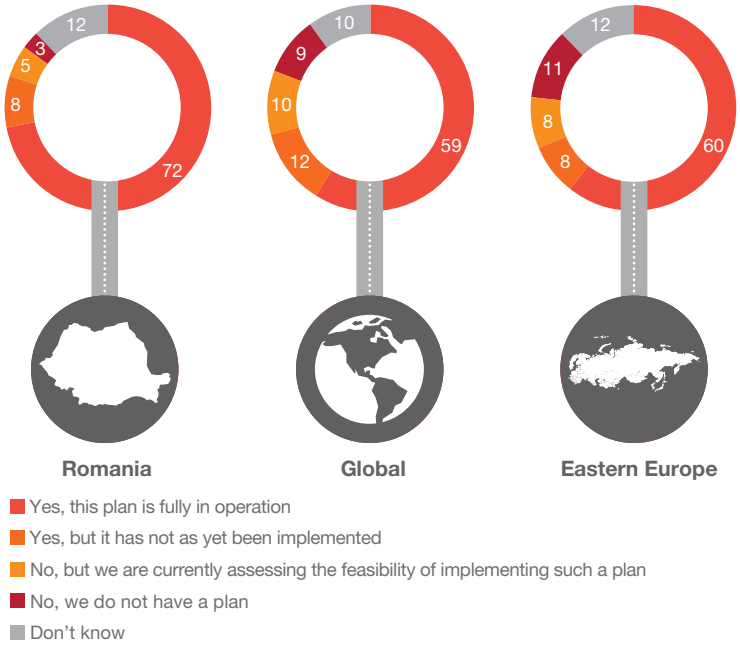
While developments are very promising, with more and more companies seemingly prepared to understand and address the risks faced, one question remains: Will your cyber security program withstand the test of reality?

Our study reveals that over the last two years, only 41% of Romanian respondents have performed an assessment of their cyber response plan. While reported rates for Romania are well above the global (30%) and regional (28%) average, it is crucial for companies to understand that cyber threats are not static. As technology is constantly changing, regular monitoring and examination of the cyber response plan implemented is key to maintaining it relevant.

Cyber-attacks are here to stay, what all companies must do is to enforce data protection policies, to set up proactive defenses and focus on being ahead of the curve in cyber security.

Moreover, 2018 is the year when the General Data Protection Regulation comes into effect in Romania, this means companies will be required by law to protect themselves against data loss. Since the penalties for failure to enforce this new European Union policy are potentially prohibitive, companies will need to invest more time and effort in securing themselves better by having a valid cyber security agenda.

Figure 16 - State of the implementation of a Cyber Security Program



% of respondents who said their organisation uses and derives value

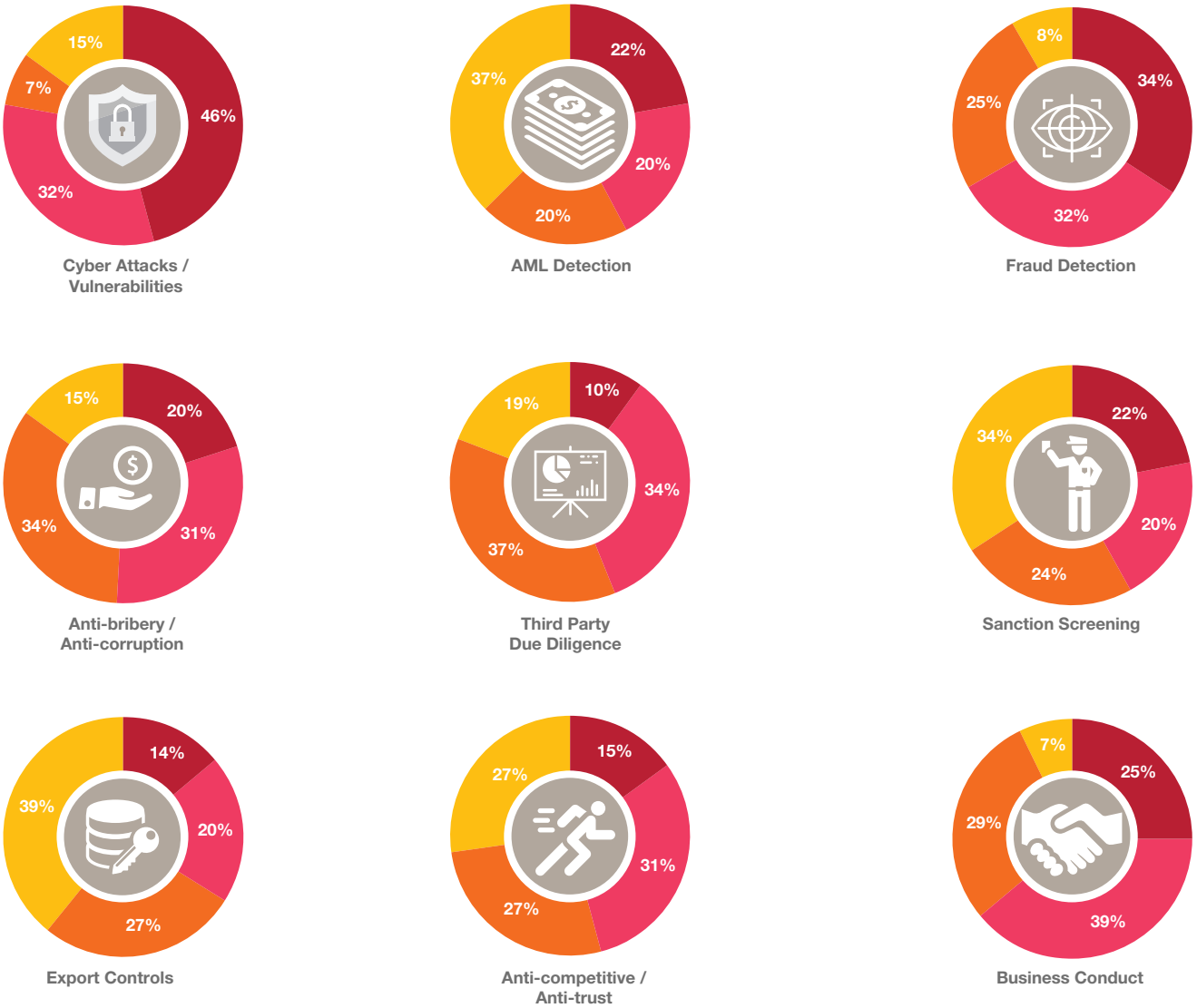
How is technology shaping the fight against fraud?

Our digital footprint in everyday life is growing, companies are developing ever faster when they start to employ digital standardization and process mapping. It is no wonder that organizations are making more use of technology to combat fraud.

While eight out of ten Romanian companies are making use of technology to minimize the potential damage of cyber-attacks and vulnerabilities, advanced technologies are not as frequent when it comes to monitoring fraud in the more traditional areas.

As such, 37% of Romanian respondents do not use technology for monitoring third party due diligence processes. In the areas of anti-bribery and anti-corruption or business conduct the rates are slightly lower, 34% and 29%, respectively. However, actual rates could be higher if we consider that a significant proportion of respondents were not aware to what extent technology is used for fraud monitoring purposes.

Figure 17 - Extent to which Romanian organizations use technology as an instrument to monitor fraud



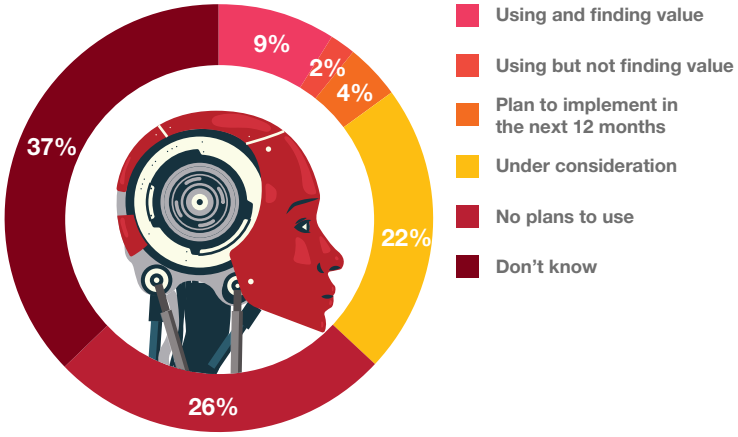
In the present reality where most economic crimes have, to some extent, gone digital, companies also need to adapt the fraud prevention and detection tools employed and invest in new technologies to stay ahead of perpetrators.

In the fight against fraud, the future appears bright for technologies based upon artificial intelligence (AI) and machine learning (ML).

Despite only one in ten Romanian respondents currently using AI in their control environment, the data indicates that a quarter of Romanian organizations plan to use this nascent advance as a tool to combat fraud. Applying AI to fraud prevention and detection tools is a relatively new and developing use, and has the prospect for major impact in the future as it evolves into standard practice.

Our survey also shows that 32% of the Romanian companies use, plan to implement in the following year or take into consideration the leverage of ML, while the regional rate is 33% and the global one much higher, 38%. This discrepancy points out that Romania is lagging behind on what everyone else is doing,

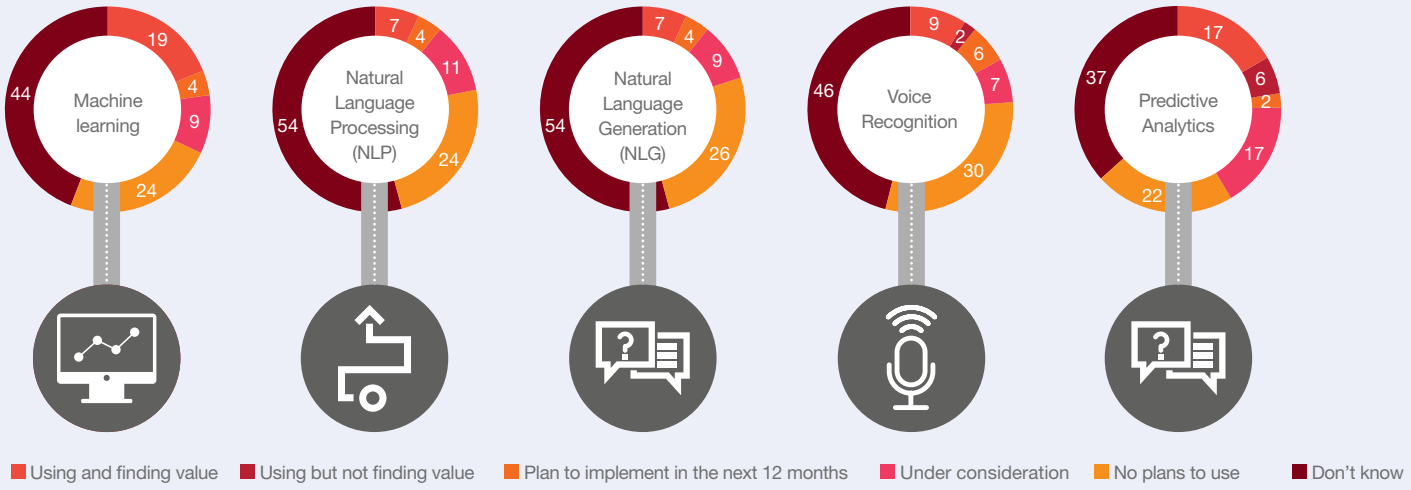
Figure 18 - Degree to which Romanian organizations are using or considering Artificial Intelligence in their control environment



although it has the highest usage ratio to date, 19%, while the Eastern European or global average is 12% and 13%, respectively.

As AI and ML gather pace and start to become integrated in more and more industries, they are sure to play a greater role in the efforts to combat economic crime.

Figure 19 - Use of Machine Learning and Advanced Analytics to combat fraud by Romanian organizations



% of respondents who said their organisation uses and derives value

Business ethics and compliance programs

Are compliance risks effectively mitigated?

Fraud risk preventive measures are yet to become business as usual in Romanian organizations.

Our study reveals that over the last two years, only 54% of Romanian respondents have performed a general fraud risk assessment. And a little over one-third of Romanian organizations have conducted risk assessments in the critical areas of anti-bribery and corruption, anti-money laundering (AML), anti-competitive / anti-trust or industry specific regulations.

Romanian executives need to acknowledge that risk assessments are critical in understanding the specific threats to each business, identifying gaps in internal controls and developing an effective and efficient plan to mitigate those risks.

Only in four out of ten cases, the risk assessment performed by Romanian companies was part of a larger Enterprise Risk Management (ERM) strategy. The lack of an ERM strategy company-wide can prove to be very costly and damaging to businesses, as proven by recent actions taken by Romanian authorities.

As far as acquisitions and other transactions are concerned, a fraud risk assessment is even more important as part of the pre-deal due diligence process. Enhanced due-diligence will allow acquirers to understand the threats they face so that appropriate consideration is given pre-deal or corrective actions can be taken post-deal.

Our survey shows that three out of four Romanian respondents perform regulatory and tax compliance exercises as part of the acquisition process, while more than half conduct anti-bribery and corruption and anti-competitive/ anti-trust due diligence. Reported rates by Romanian organizations are above global and regional rates. This proves that Romanian companies have started to recognize the benefits associated with enhanced due-diligence.

Figure 20 - Areas covered by the risk assessments performed by Romanian organizations in the last two years

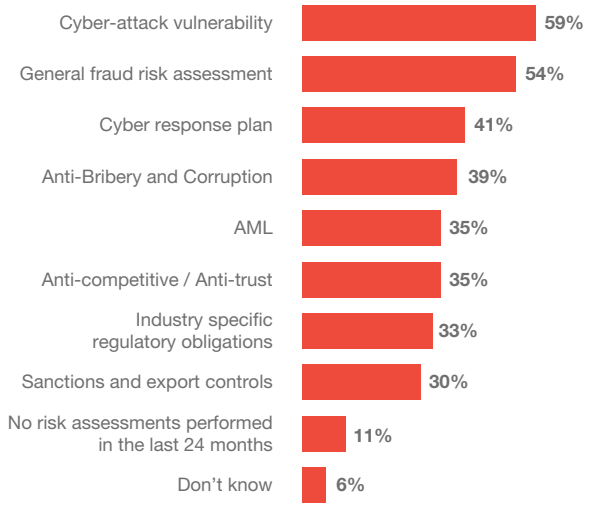
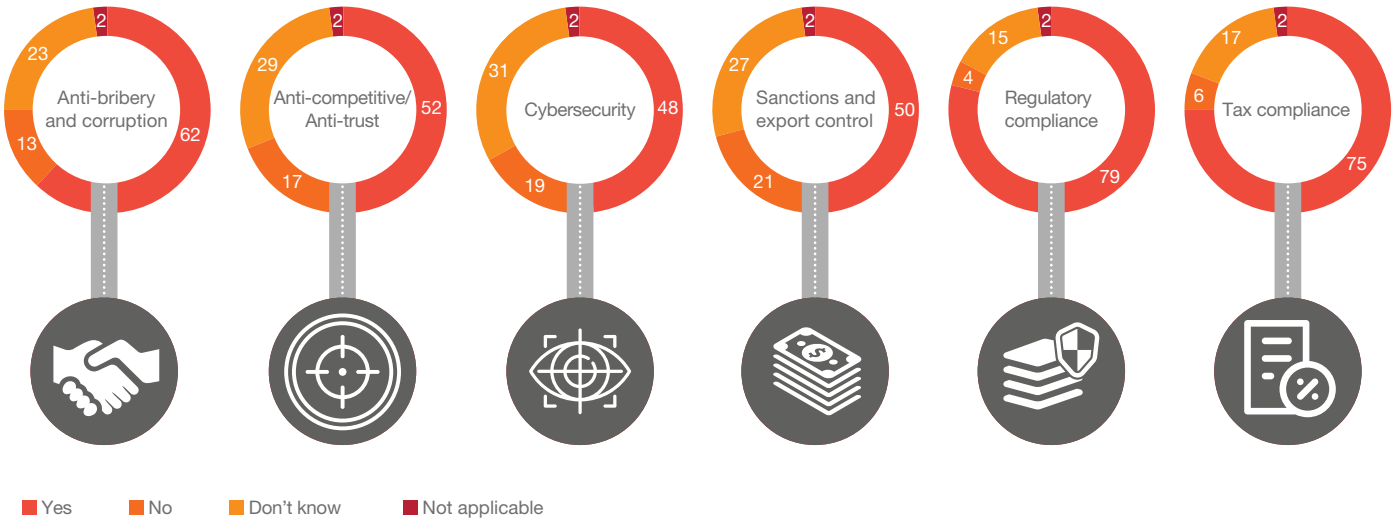


Figure 21 - Additional due diligence performed by Romanian organizations as part of the acquisition process



% of respondents who said their organisation uses and derives value

Making sense of fraud

Understanding an individual's motivation for engaging in fraud can prove to be very challenging. The fraud triangle illustrates three drivers that are regularly found when fraud occurs: opportunity, incentive or pressure, and rationalization. Since all three of these conditions must be present for an act of fraud to take place, all three need to be addressed individually.

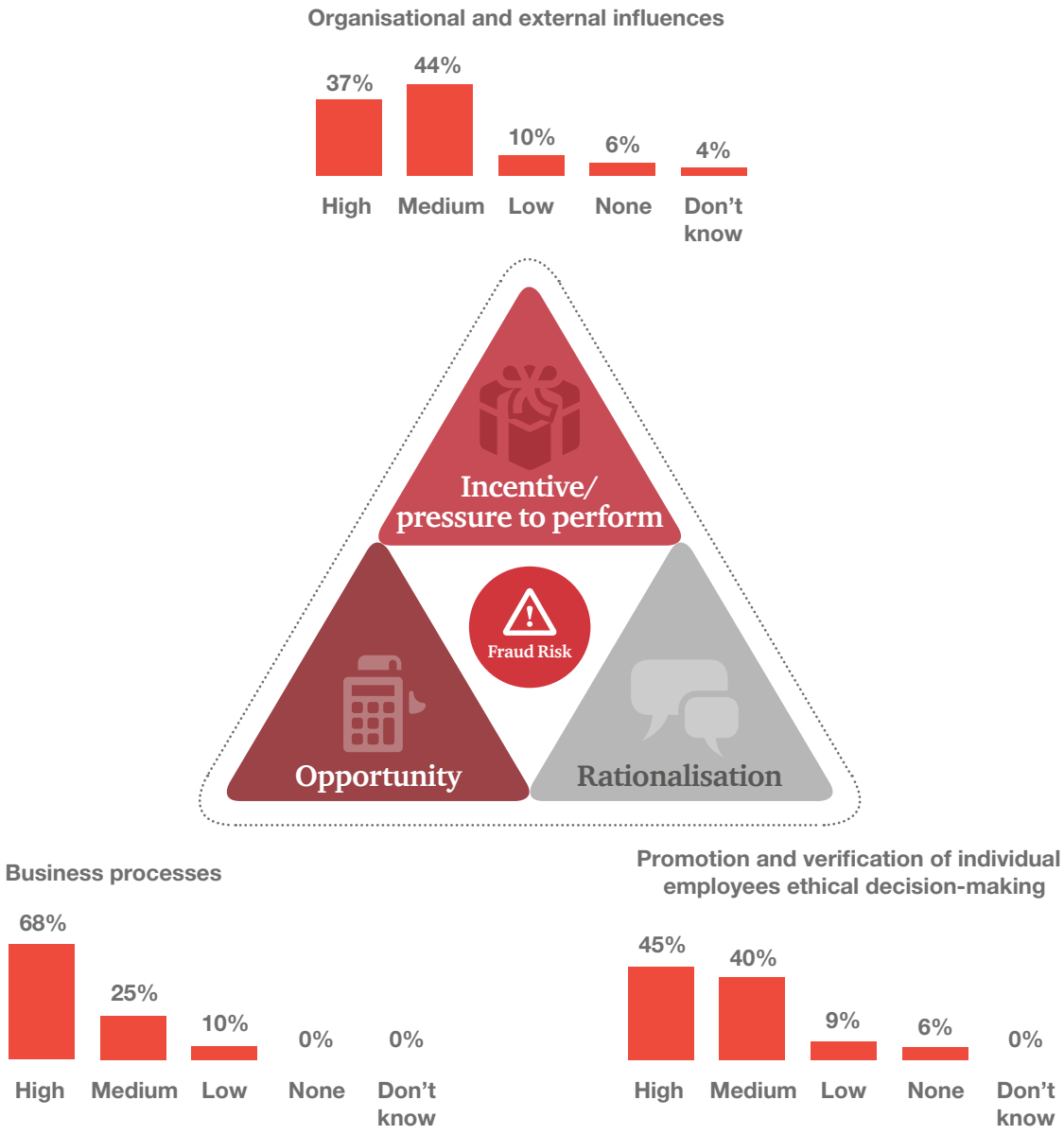
Areas where organizations can focus efforts to help combat these drivers are:

- Business processes to fight opportunity;
- Promotion and verification of individual employee ethical decision-making to combat ability to rationalize the crime, and
- Organizational and external influences to address incentives or pressure.

Of the three sides of the fraud triangle, most efforts have been focused at reducing the opportunity to commit fraud - with 68% of Romanian respondents indicating that they spend a high degree of effort in building up business processes such as internal controls. Similar with global and regional trends, Romanian organizations are putting less effort into actions meant to combat pressures and rationalization, with only 37% and 45% respectively, making it a top priority.

Since more than half of the survey's respondents worldwide revealed that the most disruptive fraud was perpetrated by an internal actor, companies also need to focus on the culture enabling the internal misbehavior. Just as fraud is not driven by a single factor, companies need to find the right formula of technology, processes and people measures.

Figure 22 - Measures taken by Romanian organizations to combat fraud internally



Our survey revealed that a significant number of Romanian organizations (87%) have a formal business ethics and compliance program in place, above the global and Eastern European averages of 77%.

As part of the compliance program, most companies have implemented standards and policies that build upon the foundation of their internal Code of Conduct. This year's study shows that approximately eight in ten Romanian companies have specific policies in place covering issues such as general fraud, anti-bribery and corruption or industry specific regulations, while more than half have implemented policies addressing AML or anti-competitive and cyber behaviors.

Figure 23 - Romanian companies having a formal business ethics and compliance program in place

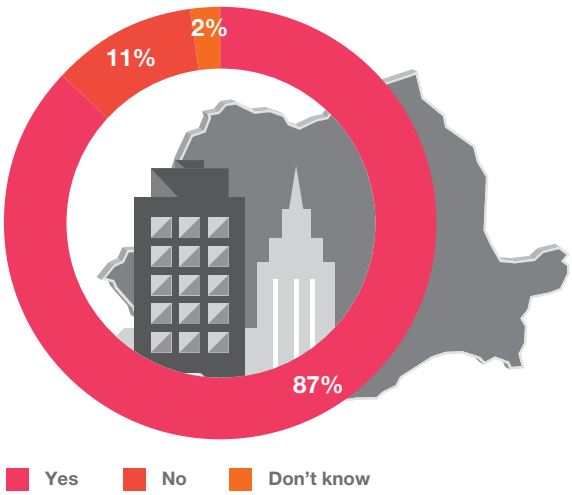
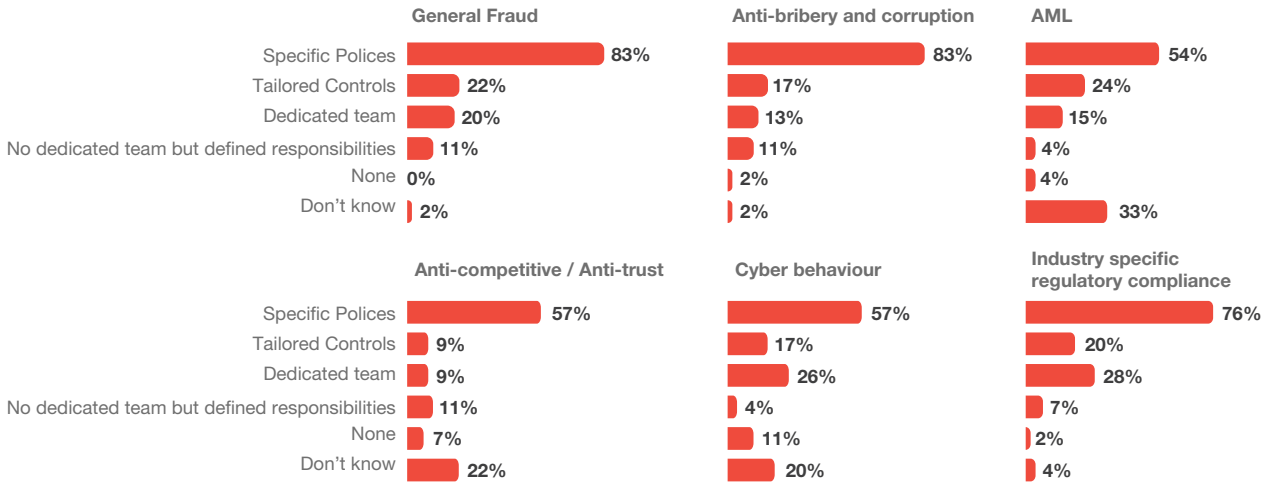


Figure 24 - Risk categories addressed by the compliance programs implemented by Romanian companies



Ultimately, a compliance program is not just words on a piece of paper and organizations need to ensure that policies are followed and enforced and compliance issues are detected and remediated in real-time. Internal controls tailored to the organization's specific risks and dedicated compliance teams usually achieve these goals.

However, there are some consistent elements which organizations need to start paying additional attention to. Only one in five Romanian respondents have implemented tailored controls in the area of general fraud and have a dedicated team to monitor the adherence of employees to the compliance program.

Reported rates are even lower in the case of internal controls addressing other risk categories such as anti-bribery and corruption, anti-competitive / anti-trust behavior, cyber behavior or industry specific regulations.

Implementation of specific policies and procedures is best practice, but these will not effectively mitigate compliance risks unless they are deeply embedded into the organization's culture through regular monitoring and training.

A successful compliance program can only be established on a strong foundation of ethics that are fully supported by the senior management team. In other words, the correct "Tone-at-the-top".

Of the 87% of Romanian organizations having a formal compliance program, responsibility for that program is widely dispersed among roles. Four out of ten Romanian respondents reported that their organization's Chief Compliance Officer (CCO) was responsible for their business ethics and compliance program, while in one fifth of the cases this responsibility belongs to the Chief Executive Officer (CEO).

While leadership is undoubtedly a key element of the compliance program, all employees need to closely observe its principles and understand their roles and responsibilities in ensuring that business is aligned with its ethics and compliance program.

Whistleblowing: valuing a transparent business culture

Almost nine out of ten Romanian respondents (87%) stated that they are relying on periodic internal reviews as part of their approach to evaluate the effectiveness of their compliance programs.

While internal reviews are undoubtedly very important in assessing an organization's ethical and compliance program, they are not a sufficient investment to ensure compliance, being both periodic and historical.

Since prevention should be a priority at the time decisions are made, not after detection, periodic internal reviews should be doubled by other means, such as management reporting and real-time monitoring of business so that potential issues are detected and prevented in due time.

According to our survey respondents, however, less than half of Romanian organizations stated that there are confidential channels in place for raising concerns, including a clear whistleblowing policy. While the reported rate is slightly above global (44%) and regional (41%) averages and shows an encouraging evolution since our 2016 study (33%), the job is only half done.

Whistleblowing programs have demonstrated to be a successful method of fraud detection globally and form an essential part of a strong fraud risk management framework. Employees may be reluctant to report ethical issues to their superiors or Internal Audit function and are more likely to report incidents anonymously or to independent parties. Providing a range of reporting methods enhances the probability that employees may feel comfortable enough to use at least one of the available options.

Therefore, all companies, regardless of size, should consider supplementary whistleblowing facilities and external monitoring and reporting mechanisms.

Figure 25 - Methods used by the Romanian organizations to ensure their compliance programs are effective

The global context - beneficial ownership

Compliance, however, is not set up to observe the complex, trans-border nature of aspects such as beneficial ownership.

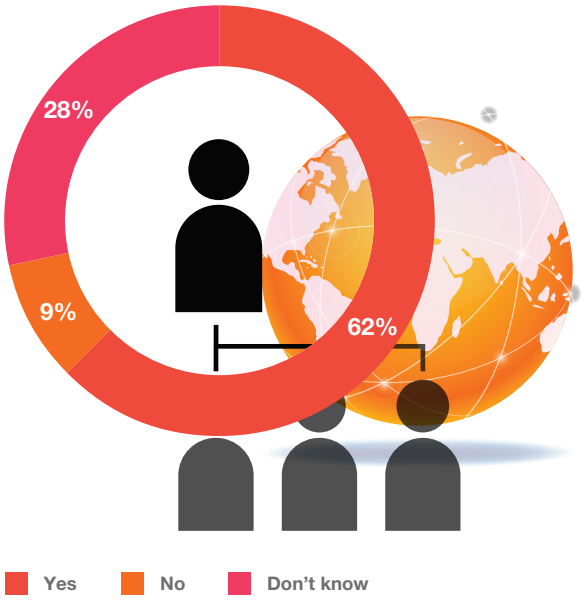
The fight against economic crime has made financial transparency a global priority, beneficial ownership still being an area cloaked in secrecy worldwide. Conducting business transactions with a company without full knowledge of real owners / controllers might pose significant threats to an organization.

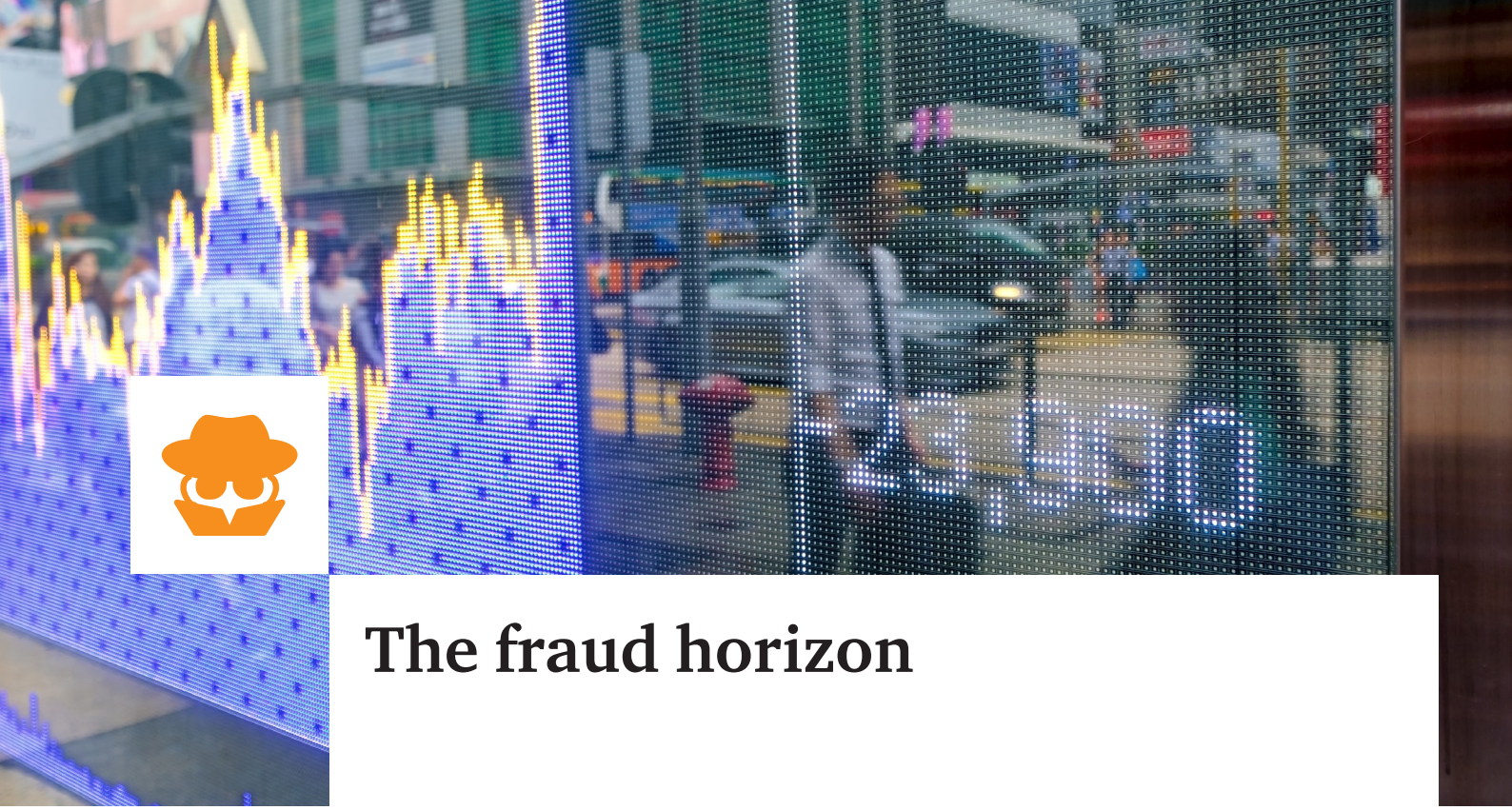
There has been some movement towards corporate transparency with the enactment of the EU Fourth AML Directive in 2015, though many countries, Romania included, failed to meet the implementation deadline. If information on beneficial owners was made public, investigators worldwide could be better placed to unveil the true ownership of anonymous companies.

The drive for increased transparency has also convinced 62% of the Romanian respondents to our survey that the implementation of Global Beneficial Ownership standards will be useful in fighting fraud. It is worrying that almost one in three respondents were not aware of the extent to which the adoption of legislation on beneficial ownership could help their organizations in combatting economic crime.

Companies need to get quickly up to speed with the proposed implementation of beneficial ownership standards because these are bound to change forever the way in which business risks are assessed.

Figure 26 - Perception of Romanian organizations of the positive effect of the implementation of Global Beneficial Ownership standards





The fraud horizon

Economic crime has never been more present in the Romanian media than in the last two years. What our survey and day-to-day experience tell us is that despite all attempts, efforts, energy and competencies organizations put in place for fighting unethical and illegal conduct, instances of fraud, bribery and corruption are unlikely to disappear. No organization or economy is corruption-free and the adverse impact of economic crime incidents cannot be disregarded.

Thinking about the next two years, cybercrime is recognized as the type of fraud most likely to seriously affect business operations worldwide. The views of Romanian respondents are no different from globally and regionally revealed perceptions.

In terms of funds allocated to fight fraud, only one in four Romanian organizations are considering some increase in their investigative and compliance spend in the next two years, significantly lower than global rate (44%). This rather conservative approach to budgeting for anti-fraud efforts might translate in Romanian companies' slight disregard of the changing business environment and of the seriousness of the new emerging threats.

Our 2018 survey findings exhibit present and future fraud red flags and trends whose effects Romanian organizations must attempt to reduce. Fraud is damaging for a business and perpetrators adapt their methods on an ongoing basis. As one barrier is implemented, fraudsters will pursue and exploit other weaknesses within organizations. Facing such motivated adversaries, businesses must seek to adjust to an ever-evolving environment, prevent, above all, but also uncover and correct potential fraud occurrences.

Fraud is not going away, but a forward-thinking organization can be one step ahead and mitigate the challenges posed by economic crime.

Figure 27 - Trends in perception of fraud in Romania in the next two years

Contacts

Want to know more about what you can do in the fight against fraud? Our subject matter experts can help

Per A. Sundbye
Partner
Forensic Services Leader in
South-East Europe
per.sundbye@pwc.com
Mobile: +386 51 687 079

Ana Sebov
Director
Forensic Services Leader in Romania
ana.sebov@pwc.com
Mobile: +40 723 179 127

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 organizations tackle the major financial and reputational risks associated with economic crime. We identify financial irregularities, analyze complex business issues and mitigate the future risk of fraud.

pwc

PwC firms help organisations and individuals create the value they are looking for. We are a network of firms in 157 countries with close to 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2018 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.