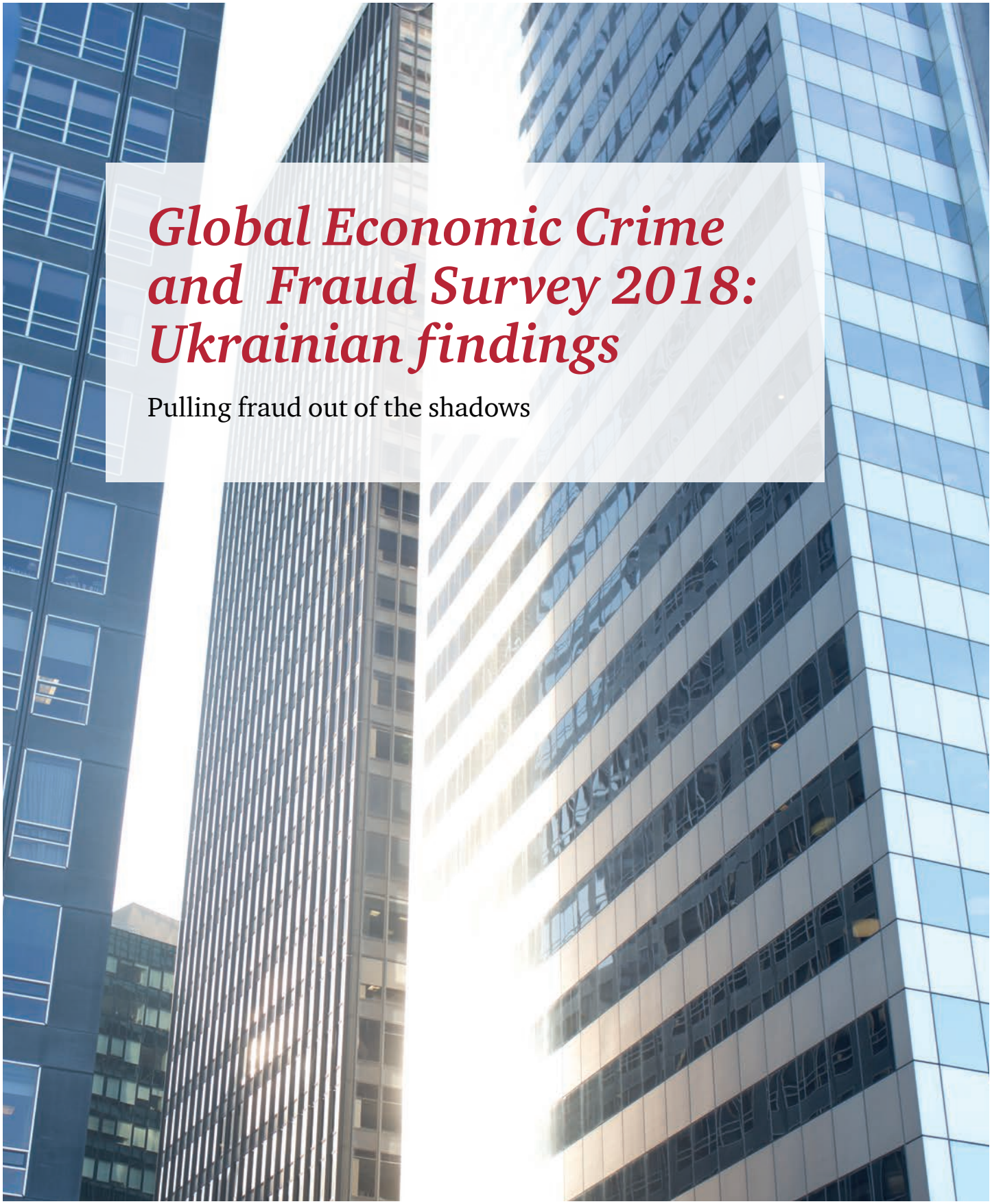


Global Economic Crime and Fraud Survey 2018: Ukrainian findings

Pulling fraud out of the shadows

pwc

pwc.com/ua/gecfs/en

Marcin Klimczak
Partner, Forensic Leader,
PwC Poland, Ukraine
and the Baltics

We are pleased to present our Report for Ukraine, which is based on the results of the Global Economic Crime and Fraud Survey 2018, one of the premier thought leadership publications on economic crime and fraud in the business world.

This is the ninth time the Global Economic Crime and Fraud Survey has been prepared with over 7,000 respondents from 123 countries contributing to the survey results.

The survey has been carried out biennially in Ukraine since 2009 and this has allowed us to observe trends of the most common types of fraud and its impact on Ukrainian organisations, as well a oversee changes in fraud prevention efforts taken by organisations.

According to this year report, 48% of respondents in Ukraine said their organisations had suffered from fraud in the last two years, up from 43% in 2016. Bribery and corruption remains the one causing serious negative effect on individual organisations and business in general – an alarming 73% of Ukrainian organisations had experienced this type of economic crime over the past two years. Among other top-5 reported economic crimes in Ukrainian organisations are: asset misappropriation, procurement fraud, HR fraud and cybecrime.

While Ukrainian organisations are increasingly aware of fraud, this year's study found that almost every seventh economic crime is still discovered by accident.

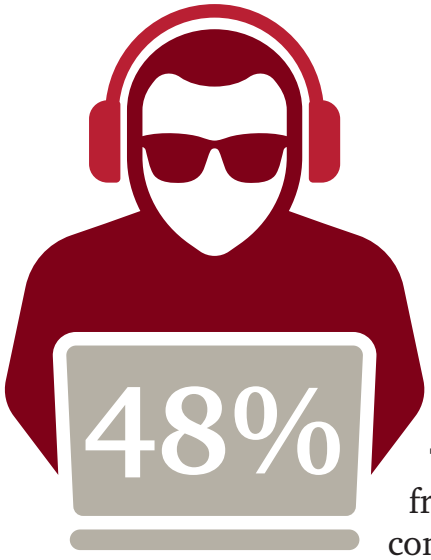
Our survey shows that fraud is hitting the wallets of organisations in Ukraine with 12% respondents pointed the losses of their organisations between $1 million and $50 million. But, the fallout does not stop with only financial impact. Ukrainian organisations reported that reputation / brand strength, business relations and relations with regulators suffered significantly from economic crime.

As such findings underline, it is now more important than ever to ask: are we doing our best to fight economic crime or are we still missing something crucial in the battle against fraud?

When digital technology continues to develop it becomes a double-edged sword: both as threat and protector for organisations. Like every part of an organisation, fraud has gone digital. But, when it comes to using more advanced techniques to make fraud visible and respond (e.g. data analytics, transactions testing, email monitoring, etc), Ukrainian organisations seem to be lagging behind the rest of the world. What is more, most organisations in Ukraine are still not adequately prepared for cyber attacks: only every third organisation has a cyber security programme in place.

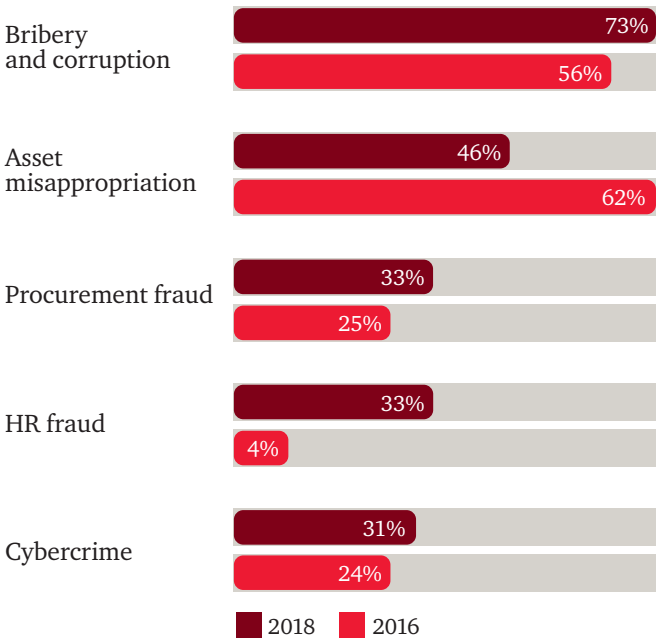
Therefore, this year's Global Economic Crime and Fraud Survey turns the spotlight on the growing threat of blind spots in combating economic crimes and fraud to which every organisation are exposed, regardless of size, industry and location. We will unveil the principal trends in fraud-fighting measures so that Ukrainian organisations can pull fraud out of the shadows.

Know what fraud looks like



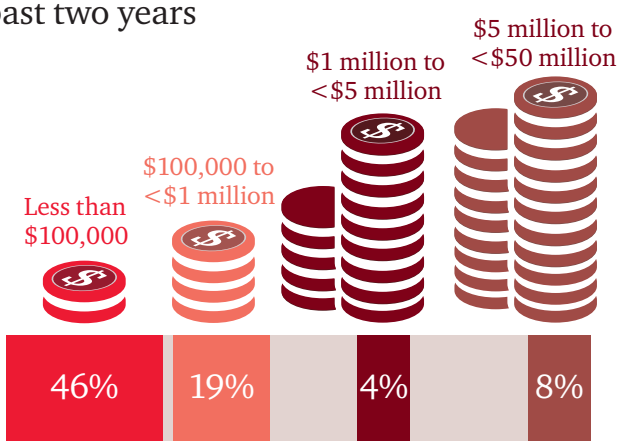
of Ukrainian organisations had experienced economic crime in the last two years, in line with the global average of 49%. This is an increase from 43% compared to 2016

Top 5 types of reported fraud in 2018:

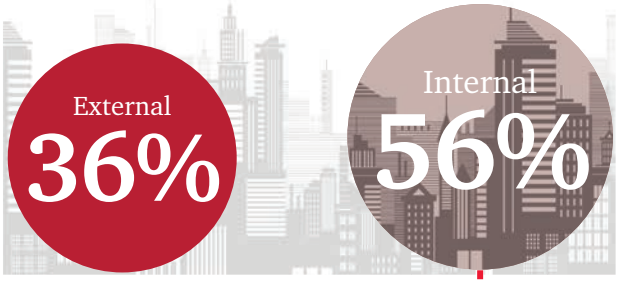


Top 5 fraud that Ukrainian respondents think are most likely to be the most disruptive for their organisations in the next two years

Amounts lost through fraud in the past two years



36% of fraud was committed by external perpetrators (Global: 40%). **56% was committed by internal perpetrators** (Global: 52%)



remaining respondents either do not know or prefer not to say

55% of fraud, committed by internal perpetrators, was committed by senior management, up from 27% in 2016

70%

of respondents ranked "opportunity" as the leading factor that had contributed to incidents of fraud committed by internal perpetrators

1 in 3 organisations in Ukraine has a Cyber Security Programme

14% of fraud was detected through suspicious activity monitoring or internal tip-off

14% of fraud was detected by accident

33% of Ukrainian respondents reported that their organisations had been asked to pay a bribe in the last two years – up from 13% in 2016

Are you aware of fraud in your organisation?

Fraud is more public, more detectable and more visible than ever before – but are we seeing all of it?

Our study shows that fraud in Ukrainian organisations is up from 43% in 2016 to 48% in 2018. In reality, these numbers are probably more useful as a metric of fraud that has been identified than of actual fraud.

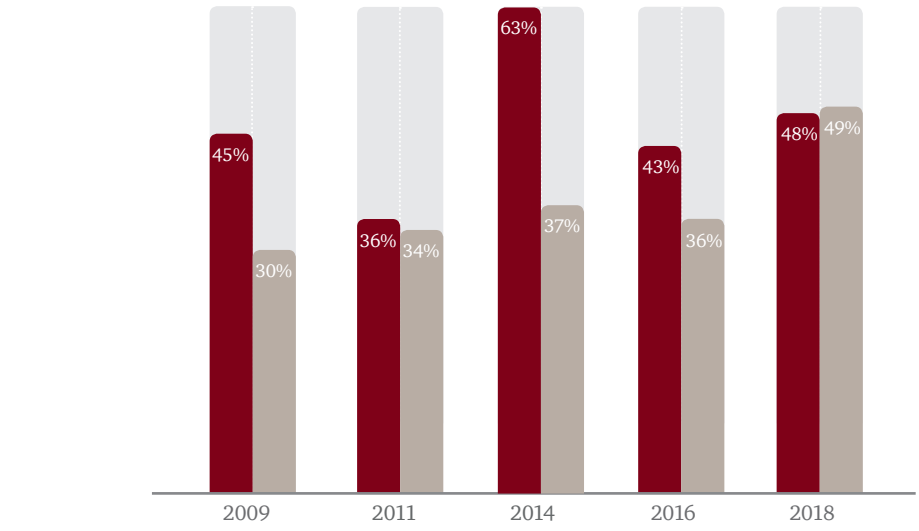
While Ukrainian ogranisations are increasingly aware of fraud, this year's study found that **1 in 7 economic crimes in organisations is still discovered by accident.** It is therefore fair to ask: what is being missed? And more importantly: why?

Every organisation – no matter how vigilant – has blind spots. And shining the spotlight on fraud as early as possible can greatly boost fraud-fighting efforts.

48%

of Ukrainian respondents reported their organisations being victims of economic crime in the last two years

Has your organisation experienced any economic crime and/or fraud within the last two years?



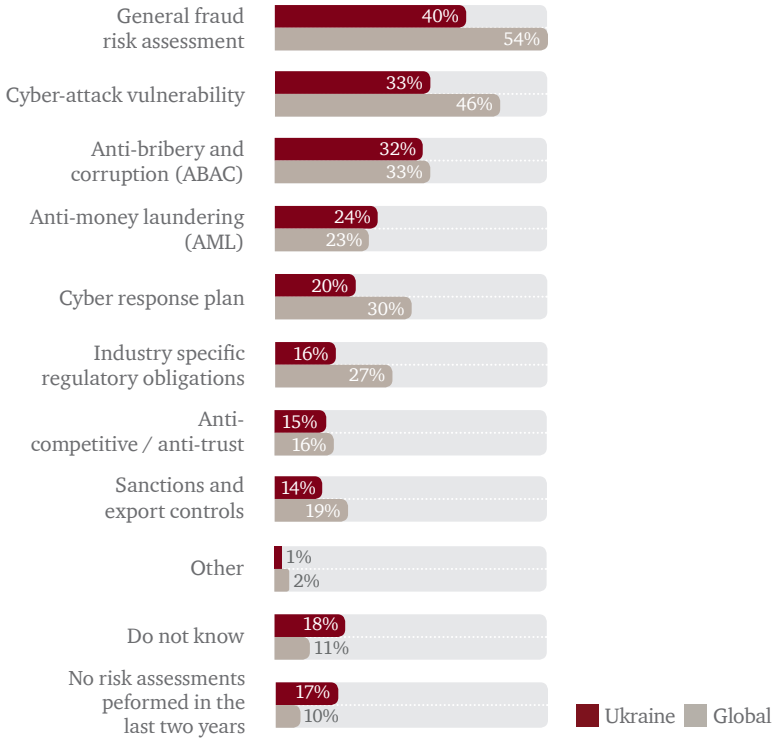
Respondents that answered 'yes'

Fraud risk assessments are the first step in preventing fraud before it takes root

Despite the increase in spending, many Ukrainian organisations are still addressing fraud prevention using a reactive, defensive approach:

- **Only 40% of organisations in Ukraine said they had conducted a general fraud risk assessment in the past two years.**
- About a third said they had conducted a cybercrime risk assessment.
- Fewer than a third said their organisations had performed risk assessments in the critical areas of anti-bribery and corruption, anti-money laundering, or sanctions and export controls. Also, only 27% of Ukrainian organisations had performed the anti-bribery and corruption (ABAC) due diligence as a part of any acquisition process (comparing to 45% globally).
- **Almost every fifth organisation (17%) had not performed any risk assessment at all in the past two years.**

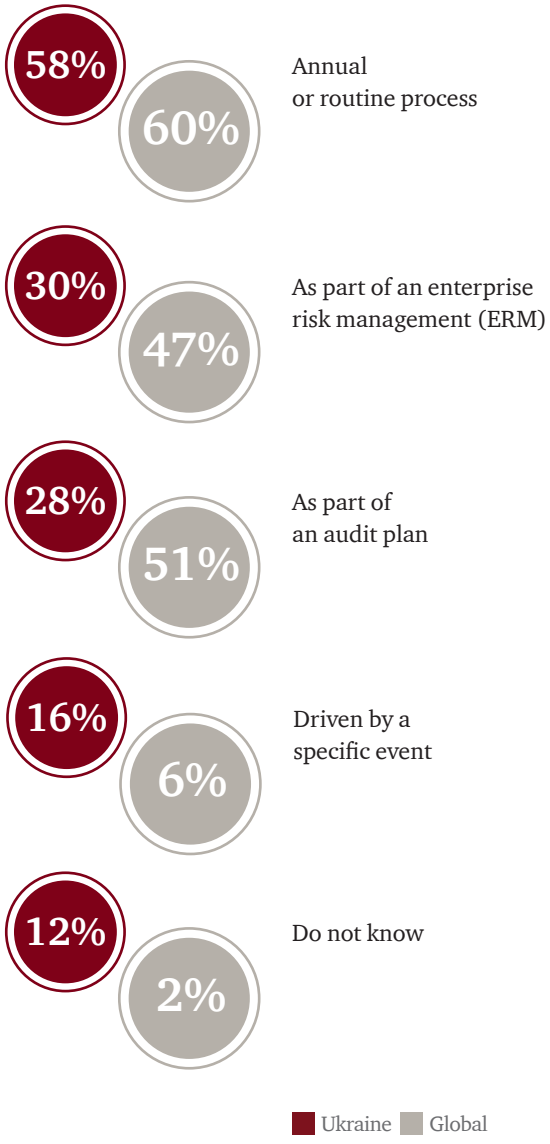
In the last two years, has your organisation performed a risk assessment in any of the following areas?



However, the rules of the game are changing profoundly and irreversibly. Public tolerance for corporate and/or personal misbehaviour is vanishing.

This points to a heightened risk when fraud or economic crime spill into public view – and a greater need for organisations to take steps to prevent fraud before it can take root. Fraud risk assessments can help organisations to do so by identifying a specific fraud they need to look for.

What prompted your organisation to perform a risk assessment?



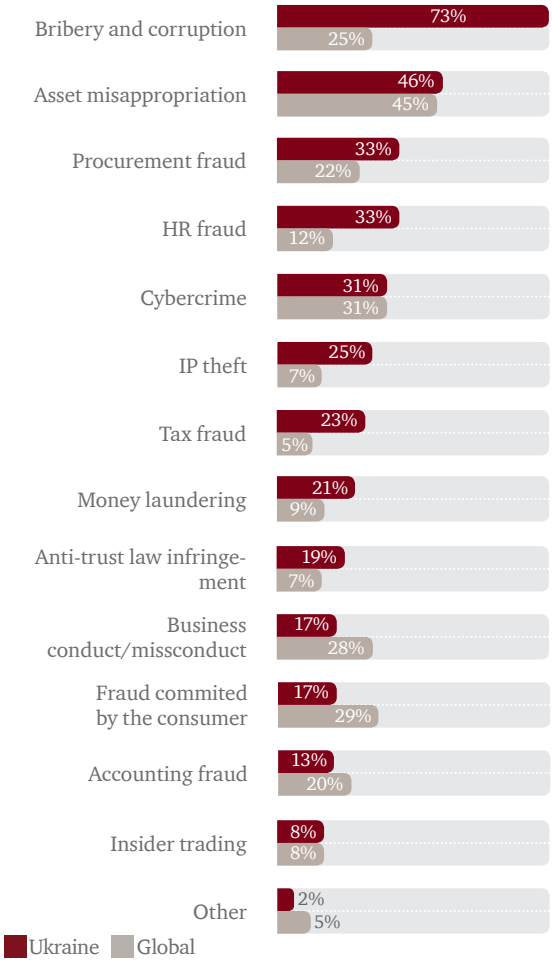
"Old friends" or "new faces" – major types of fraud experienced

Bribery and corruption, asset misappropriation and procurement fraud continue to be the most common economic crimes reported in Ukrainian organisations.

However, this year's top results was not without a "newbie". For the first time, HR fraud made the top five of the most commonly reported economic crimes in Ukrainian organisations, sharing the third and fourth place with procurement fraud.

Cybercrime is also not falling back, consistently appearing in the top five most widespread types of fraud in Ukrainian organisations, since its initial appearance in our survey in 2011.

What types of fraud have your organisation experienced in the last two years?



Bribery and corruption increased from 56% in 2016 to 73% in 2018. Globally, only 25% of respondents reported that their organisations experienced bribery and corruption, which is almost three times less than Ukrainian ones. Our study results also show that this year every third respondent (33%) reported that their organisation had been asked to pay a bribe in the last two years. It is even more concerning to note that respondents to this year survey in Ukraine reported that there is a 23% likelihood that bribery and corruption will be the most disruptive in terms of impact on their organisations in the next two years.

By contrast, **asset misappropriation**, the perennial leader in this category, showed a decrease from 62% in 2016 to 46% in 2018. The drop in the reported rates of this particular economic crime from Ukrainian respondents could be a result of tightening organisational controls and investments in prevention that are starting to show a return on investment. On the other hand, we believe the inclusion of two new fraud categories (fraud committed by the consumer (17%) and business misconduct (17%)) is partially responsible for the decrease in the wider category of asset misappropriation.

The 2018 survey revealed that 33% of respondents in Ukraine experienced **procurement fraud** in their organisations, which is 11% higher than the global findings. The prevalence of **procurement fraud** may be due to poor due diligence of vendors' integrity and absence of conflict of interest, as well as due to lack of controls over vendors' selection, contracting and remuneration processes.

HR fraud was ranked fourth among the most reported types of fraud in Ukrainian organisations, compared with the 8th place given by global respondents. We have also seen a huge rise in the reported rates of this particular economic crime from Ukrainian respondents: 33% in 2018 up from 4% in 2016. Increase of awareness of HR fraud and perception of it as an actual fraud and not as "business optimisation" is definitely a positive trend, as this type of fraud can significantly decrease employees' morale and loyalty to organisations they are working for.

Cybercrime is steadily growing from year to year and represents high risk for businesses and public authorities. The results of the 2018 survey show a 7% increase in the number of cybercrime incidents in Ukrainian organisations since 2016. The rise of technology has exposed organisations to a number of threats, including malware, phishing, network scanning and brute force attacks. And with 16% of respondents believing that it is likely that their organisation will experience cybercrime in the next two years, organisations in Ukraine should definitely pay close attention to this type of economic crime.

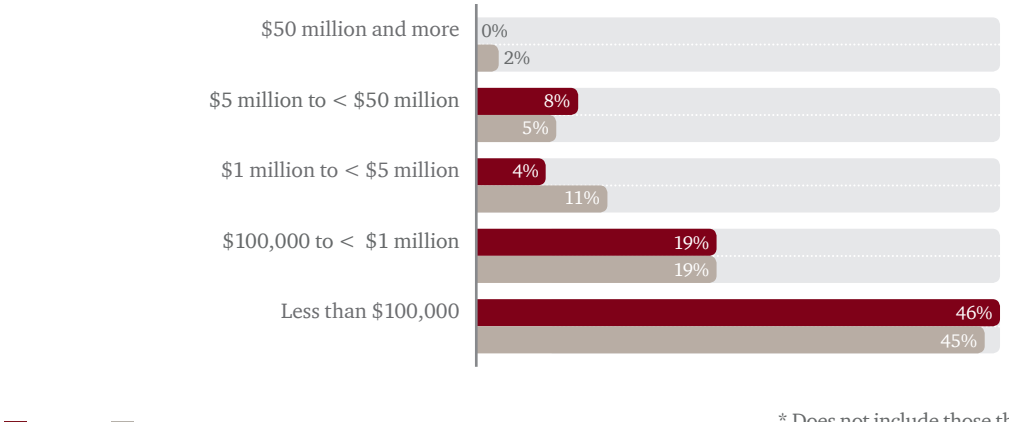
Fraud is hitting the wallets of organisations

Our survey shows that the direct financial impact of fraud can be substantial for Ukrainian organisations, with 31% of respondents reporting losses of over $100 thousand from the most disruptive fraud and **12% among them pointed the losses of between $1 million and $50 million.**

With an eye on the scale of losses that can occur, it is no surprise that Ukrainian organisations are adjusting the amount they are spending on combatting fraud to the global level.

34% of Ukrainian organisations have seen an increase spending on combatting fraud over the past two years (vs 42% globally), and 37% expect it to increase in the next two years (vs 44% globally).

In financial terms, approximately how much do you think your organisation may have directly lost through the most disruptive economic crime over the last two years?



* Does not include those that reported "amount is immeasurable" and "do not know"

58%

of Ukrainian respondents described employee morale as being damaged by the most serious fraud

Damage from fraud goes far beyond financial losses

Regardless your organisation has been hit with a one-off incident or is dealing with a systemic fraud – public outreach may damage organisation's reputation.

That is because, in the era of radical transparency, organisations often do not get to decide when an issue becomes a crisis. Rather, that is down to the count of public opinion.

Ukrainian organisations reported that reputation/ brand strength (50%), business relations (42%) and relations with regulators (38%) suffered significantly from economic crime.

And the fallout does not stop there. When an organisation's reputation takes a hit, so do its people. 58% of Ukrainian respondents described employee morale as being damaged by the most serious fraud.

55%

of reported internal fraud in Ukrainian organisations was committed by senior management

67%

of external actors committing the fraud are 'frenemies' of the organisation – agents, vendors and customers

Whose job is it anyway?

At present, many organisations treat compliance, ethics and enterprise risk management as separate functions and they rarely add up to a strategic whole.

When that happens, operational gaps can emerge and fraud can easily be brushed under the carpet or seen as someone else's problem – to the harm of the overall effectiveness of fraud prevention, financial performance and regulatory outcomes.

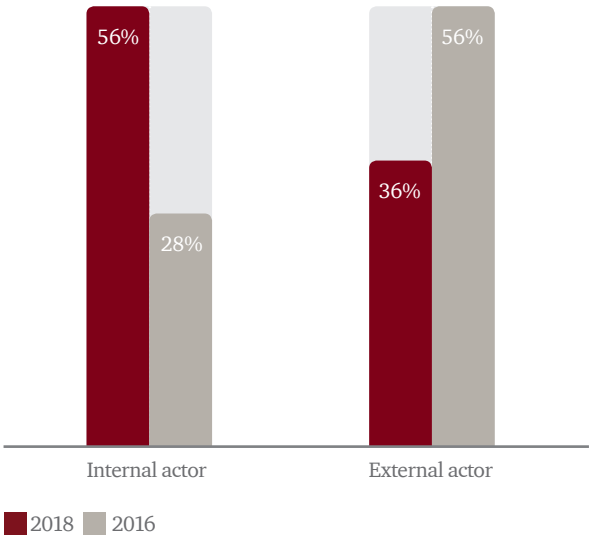
Developing and implementing a mechanism for collaboration or coordination among the parts of a business that investigate fraud, the parts that manage the risk, and the parts that report to the board or regulators can enable an organisation to measure and manage compliance, ethics and risk management better horizontally and embed them in its strategic decision-making process. This is an important step in breaking down the silos between key anti-fraud functions – and pulling fraud out of the shadows.

Who is committing economic crime?

Our survey revealed a significant increase in the share of economic crime **committed by internal actors** (from 28% in 2016 to 56% in 2018) and a dramatic increase in the proportion of those fraud attributed to **senior management** (from 27% in 2016 to 55% in 2018). Internal actors were twice more likely to be the perpetrators of the most disruptive fraud than external actors in the last two years.

However, one of organisation's biggest fraud blind spots – and biggest threats – has often nothing to do with its employees, but rather the people with whom it does business. These are the third parties with whom organisations have regular and profitable relationships: agents, vendors 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 organisation. It seems, therefore, that there is room for organisations in Ukraine to step up their efforts in the area of third party risk management (corporate intelligence / background checks of external parties) as a key fraud prevention measure.

Who was the main perpetrator of the most disruptive crime over the last two years?



Technology: vulnerability or opportunity?

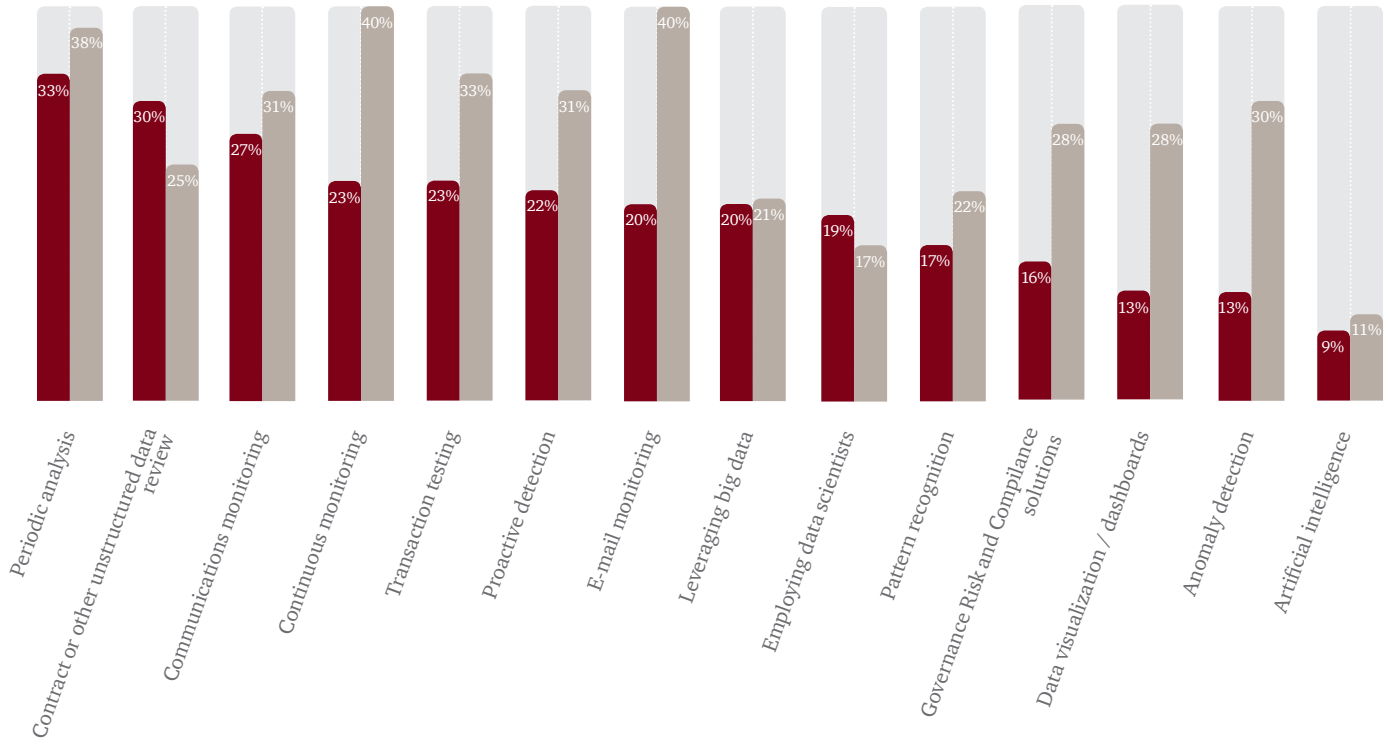
Find the right technology in your fight with fraud

Digital technology continues to develop and it is worth mentioning that it is a double-edged sword: both as threat and protector for organisations. Like every part of an organisation, economic crime and fraud have gone digital. As a result, we can perceive the existence of a vicious circle: year after year technology becomes more advanced and fraudulent activities are subsequently growing. Organisations now must brace themselves to deal with increasingly sophisticated kinds of fraud.

When technology is used well, it can help to protect organisations. **49% of organisations in Ukraine reported that technology tools enable them to carry out real-time monitoring** and **51% stated it provided them with actionable insights.**

The wheels of progress never stop turning and on the fraud defence front, organisations today have a wealth of innovative and sophisticated technologies available. When it comes to using more advanced techniques to combat fraud, Ukrainian organisations seem to be lagging behind the rest of the world.

To what degree is your organisation using or considering the following alternative/disruptive technologies in your control environment to help combat economic crime and/or fraud?



Respondents who answered "using and finding value"

Fraud is becoming more and more digital

Every day levels of online business activity are increasing. People and organisations have greater dependency on IT than ever before. The growth of the internet, and more sophisticated every-day electronic items made fraud more sharper and ingenious.

Industry 4.0 (the "Fourth Industrial Revolution", the "Industrial Internet" or the "Digital Factory") is focused on the on the end-to-end digitisation of all physical assets and processes as well as integration into digital ecosystems with value chain partners. The established way of doing business – increasingly frequently we hear about new intelligent devices such as smart phones, smart TVs, smart cars. Innovative solutions enable machines to communicate and make decisions, whilst artificial intelligence, robots, drones and 3D printing transform the way products are made and how people perform their everyday work. IT solutions have already become a basis of many businesses while modern IT organisations are expanding to other sectors such as retail, financial sector, automotive. Moreover, these solutions create new markets and services replacing work traditionally performed by humans. Interaction is changing as well: online platforms and e-services for B2C, smart contracts for B2B, e-government for B2G.

However, Industry 4.0 also creates new threats to organisations such as cyber attacks, espionage, etc. In this respect, information security becomes an integral part of doing business.

Here are some of the characteristics and challenges of today's digital fraud:

- *New digital products are creating new attack surfaces.*

To bring products to market, organisations once followed an established B2B process involving resellers, distributors and retailers. On today's innovative B2C digital platforms, there is a much wider surface for attack — and much more room for fraud to break through. As a result, there are still a lot of people who do not trust online shops due to fear of personal data breaches or leak of trust in online payments.

- *The technical sophistication of external fraudsters continues to grow.*

Digital fraud attacks continue to get more sophisticated, thorough and ruinous. In a recent cyber attack on the Ukrainian power grid, hackers were able to successfully compromise the information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers. Due to the attack, about 230 thousand people were left without electricity for 1-6 hours.

- *Politically motivated cyber attacks are breaking new ground.*

Cyber attacks have been around for several years. Currently, organisations and governments around the world are suffering from a new player – cyber attacks perpetrated by states, politically or ideologically motivated hacktivists and terrorist organisations. These intruders use a cyber attack not to enrich themselves, but to achieve some geopolitical goals: disrupt state activities, steal personal data and intellectual property, collect information about the structure of information systems and software and get data for remote access to critical infrastructure.

31%

Organisations in Ukraine experienced cybercrime

16%

Organisations in Ukraine expect to experience a cyber attack in the next two years

Get cyber ready before it is too late

In our survey, cybercrime ranked as one of the top economic crimes, affecting 31% of organisations in Ukraine.

Cyber attacks slash everything on their path: whether, a private company or a government organisation, whether located in Ukraine or elsewhere in the world.

Organisations in Ukraine continue to cast a wary eye on cybercrime, with 16% of respondents not only expecting to experience a cyber attack in the next two years, but also believing it will be the most disruptive, damaging economic crime they will face.

However, most organisations in Ukraine are still not adequately prepared for – or even aware of the risks they face: **only 1 in 3 organisations (31%) has a Cyber security programme** that is fully operational to deal with cyber attacks. Such a programme should handle current and prospective risks to the business and include a tested cyber incident response plan.

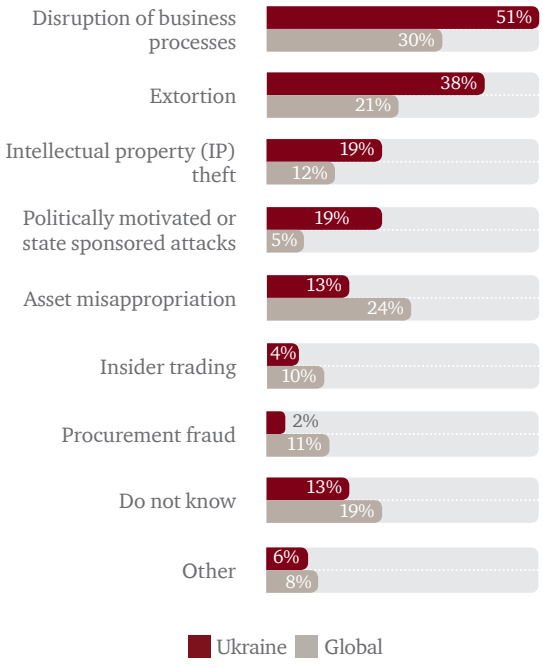
When the cybercrime hits, it is common practice to share this information with the government or law enforcement agencies. However, **28% of organisations in Ukraine are not likely or even unlikely to share this information with the government or law enforcement agencies** (in comparison with 12% of global respondents). More than half of these respondents (54%) stated, that they do not believe that law enforcement agencies have required expertise, while 41% - do not trust law enforcement agencies.

Over a third of all respondents in Ukraine stated that their organisations had been targeted by cyber attacks, using malware.

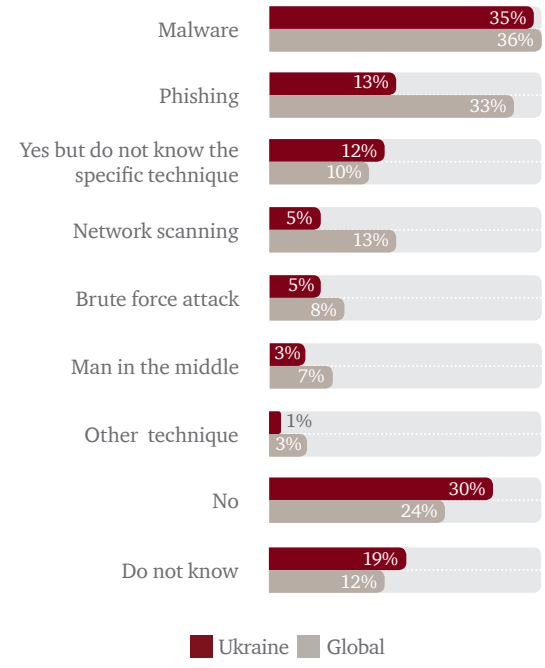
Most of these attacks, which can severely **disrupt business processes (51%),** also led to substantive losses to organisations: **38% of respondents were digitally extorted.**

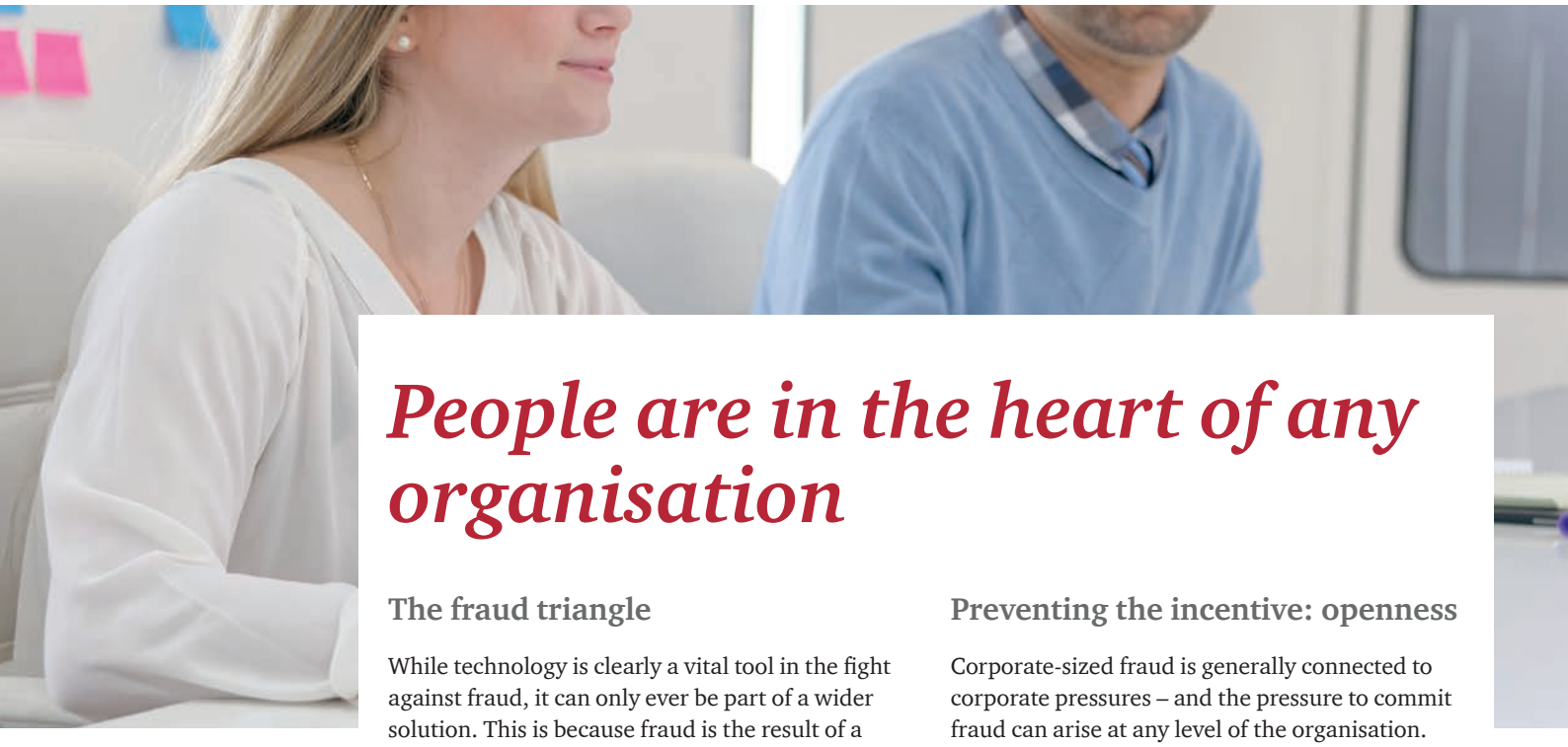
Recent major ransomware cyber attack affected large private companies, entrepreneurs and public institutions in Ukraine as well as globally. This case has demonstrated that everyone is under risk. To be prepared or not – that is the question which everyone should ask oneself.

Which of the following types of economic crime and/or fraud was your organisation victim through a cyber attack?



In the last two years, has your organisation been targeted by a cyber attack using any of the following techniques?





People are in the heart of any organisation

The fraud triangle

While technology is clearly a vital tool in the fight against fraud, it can only ever be part of a wider solution. This is because fraud is the result of a complex mix of conditions and human motivations. There is a powerful method for understanding and preventing the three principal drivers of internal fraud – the fraud triangle.

The fraud triangle starts with an incentive (generally a pressure to perform from within the organisation) followed by an opportunity (possibilities caused by lack of internal controls), and finally a process of internal rationalisation (justification of actions). Since all three of these drivers must be present for an act of fraud to occur, each of them should be addressed individually through advocating for openness at all levels of organisation, implementation of effective controls and establishment of positive spirit of corporate culture.

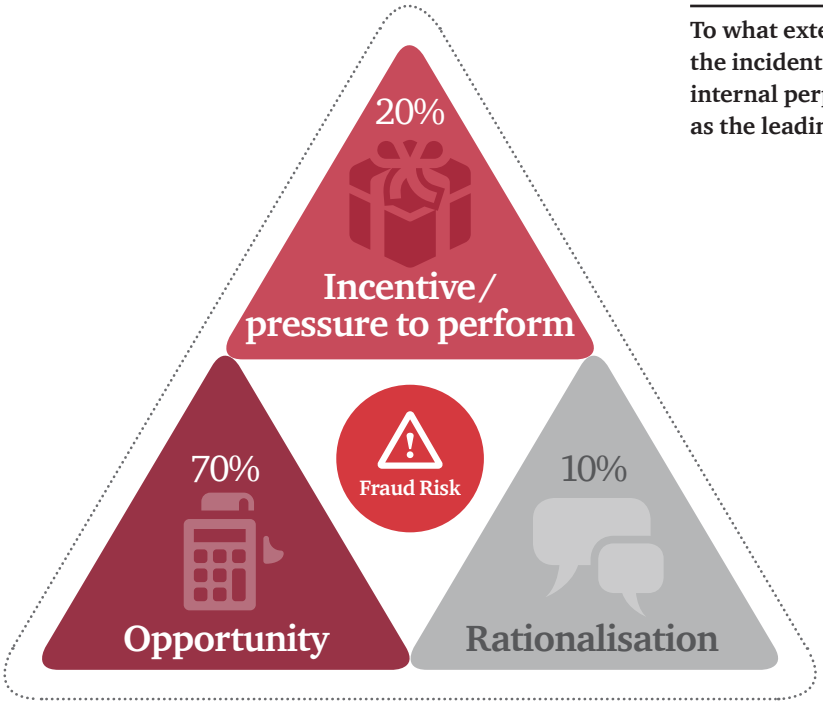
Preventing the incentive: openness

Corporate-sized fraud is generally connected to corporate pressures – and the pressure to commit fraud can arise at any level of the organisation. Our survey shows that **17% of organisations in Ukraine that experienced fraud in the last two years suffered business conduct/misconduct fraud (incentive abuse).**

It is important not to over-emphasise financial incentives when considering what drives a person to commit fraud. Fear and embarrassment about making a mistake may be equally important.

In addition, short-term bespoke controls can serve as useful checks on whether aggressive sales programmes are leading to fraudulent behaviour. A well-publicised open-door or hotline policy can also provide a valuable early-warning system of potential problems in an organisation.

To what extent did each of the following factors contribute to the incident of economic crime and/or fraud committed by internal perpetrator? (% of respondents who ranked the factor as the leading contributing factor to internal fraud)



Number of organisations in Ukraine that indicated they have a formal business ethics and compliance programme had dropped from

75% to 59%

Preventing the opportunity: controls

31% of survey respondents in Ukraine said that their organisations put effort into building up business processes, such as internal controls, that target opportunities to commit fraud. Organisations are putting the same effort into measures to counteract incentives and rationalisation, of 31% and 30% respectively.

However, organisations should pay more attention to and focus their anti-fraud efforts on reducing the opportunities for fraudulent acts.

There is a belief that internal technology-driven controls alone can catch fraud and it is assumed that management will always behave ethically. In fact, experience shows that virtually every significant internal fraud is the result of management circumventing or overriding those controls. Our survey demonstrated that the share of reported serious internal fraud committed by senior management has risen dramatically from 27% of respondents in Ukraine in 2016 to 55% in 2018. To overcome this pervasive problem, organisations need to create controls that actually account for management override or collusion in targeted areas.

Fraud is the result of the intersection of human choices with system failures, hence it is important to be wary of the false sense of security.

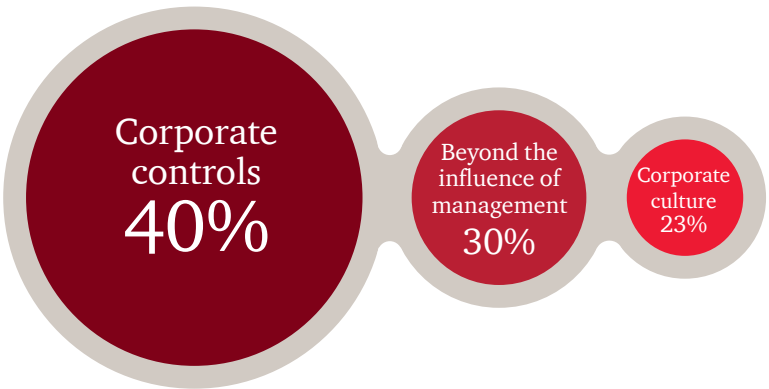
Preventing rationalisation: culture

One of the peculiarities of internal fraud is that those who commit it often see it as a victimless crime and cannot visualise those people who will be directly harmed by their actions.

The first step in preventing rationalisation is to focus on the environment that governs employee behaviour – the organisational culture. Surveys, focus groups and in-depth interviews should therefore be used to assess the strengths and weaknesses of that culture. Consistent training and capacity building are also pivotal. If people clearly understand what constitutes an unacceptable action and why – rationalising fraudulent activity will be harder.

Our survey found a decreasing number of organisations in Ukraine are investing in ethics and compliance. The percentage of respondents who indicated they have a formal business ethics and compliance programme had dropped from 75% to 59% since the last survey in 2016. And only 40% of organisations with such programme indicated that it includes specific policies for tackling general fraud.

How was the most disruptive economic crime and/or fraud initially detected?



Includes

Suspicious activity monitoring	14%
Corporate security	8%
Internal audit (routine)	6%
Fraud risk	6%
Data analytics	3%
Rotation of personnel	3%

Includes

By accident	14%
By law enforcement	8%
Investigative media	8%

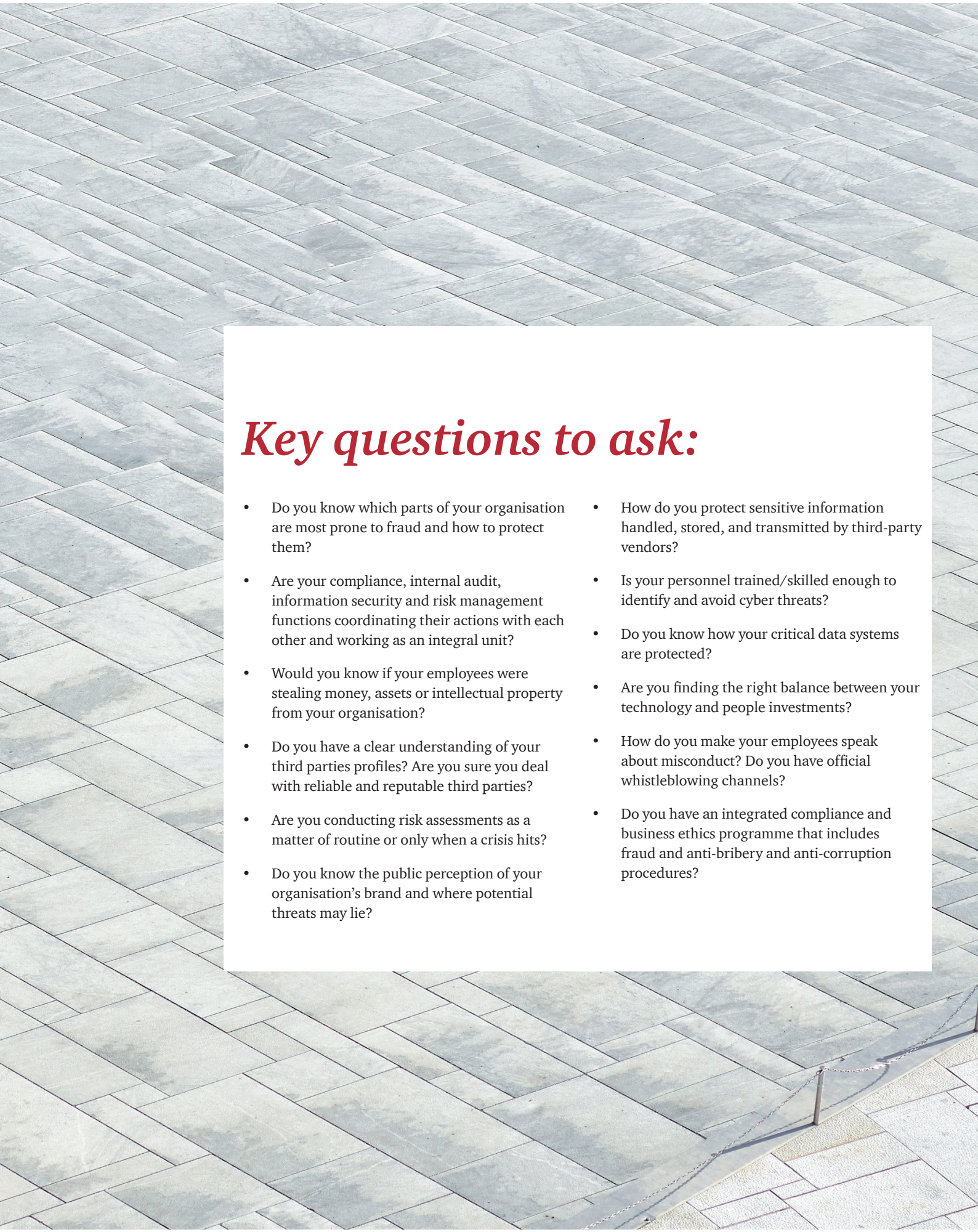
Includes

Tip off (internal)	14%
Tip off (external)	6%
Whistleblowing hotline	3%

Summary

Our survey shows that many organisations are still under-prepared to face fraud, both from internal and external perpetrators. The task of detecting and preventing economic crime or fraud is undoubtedly a complex and onerous one. It means finding the right blend of technological and people-focused measures, guided by a clear understanding of the motivations behind fraudulent acts and the circumstances in which they occur.

Organisations need not resign themselves to the belief that technology is the only solution, or that a certain amount of fraud is simply part of the cost of doing business. Rather, by establishing a culture of honesty and openness from the top down, they can imbue their organisations with a spirit of open accountability – and pull fraud out of the shadows.



Key questions to ask:

- Do you know which parts of your organisation are most prone to fraud and how to protect them?
- Are your compliance, internal audit, information security and risk management functions coordinating their actions with each other and working as an integral unit?
- Would you know if your employees were stealing money, assets or intellectual property from your organisation?
- Do you have a clear understanding of your third parties profiles? Are you sure you deal with reliable and reputable third parties?
- Are you conducting risk assessments as a matter of routine or only when a crisis hits?
- Do you know the public perception of your organisation's brand and where potential threats may lie?
- How do you protect sensitive information handled, stored, and transmitted by third-party vendors?
- Is your personnel trained/skilled enough to identify and avoid cyber threats?
- Do you know how your critical data systems are protected?
- Are you finding the right balance between your technology and people investments?
- How do you make your employees speak about misconduct? Do you have official whistleblowing channels?
- Do you have an integrated compliance and business ethics programme that includes fraud and anti-bribery and anti-corruption procedures?

Contacts

Want to know more about what you can do in the fight against fraud? Contact one of our subject matter experts

Marcin Klimczak
Partner
Forensic Services Leader – Poland, Ukraine & the Baltics
marcin.klimczak@pwc.com

Gennadiy Chuprykov
Director
Forensic Services, PwC Ukraine
gennadiy.chuprykov@pwc.com

Rafal Turczyn
Director
Forensic Services, PwC Ukraine
rafal.turczyn@pwc.com