www.pwc.com/ua

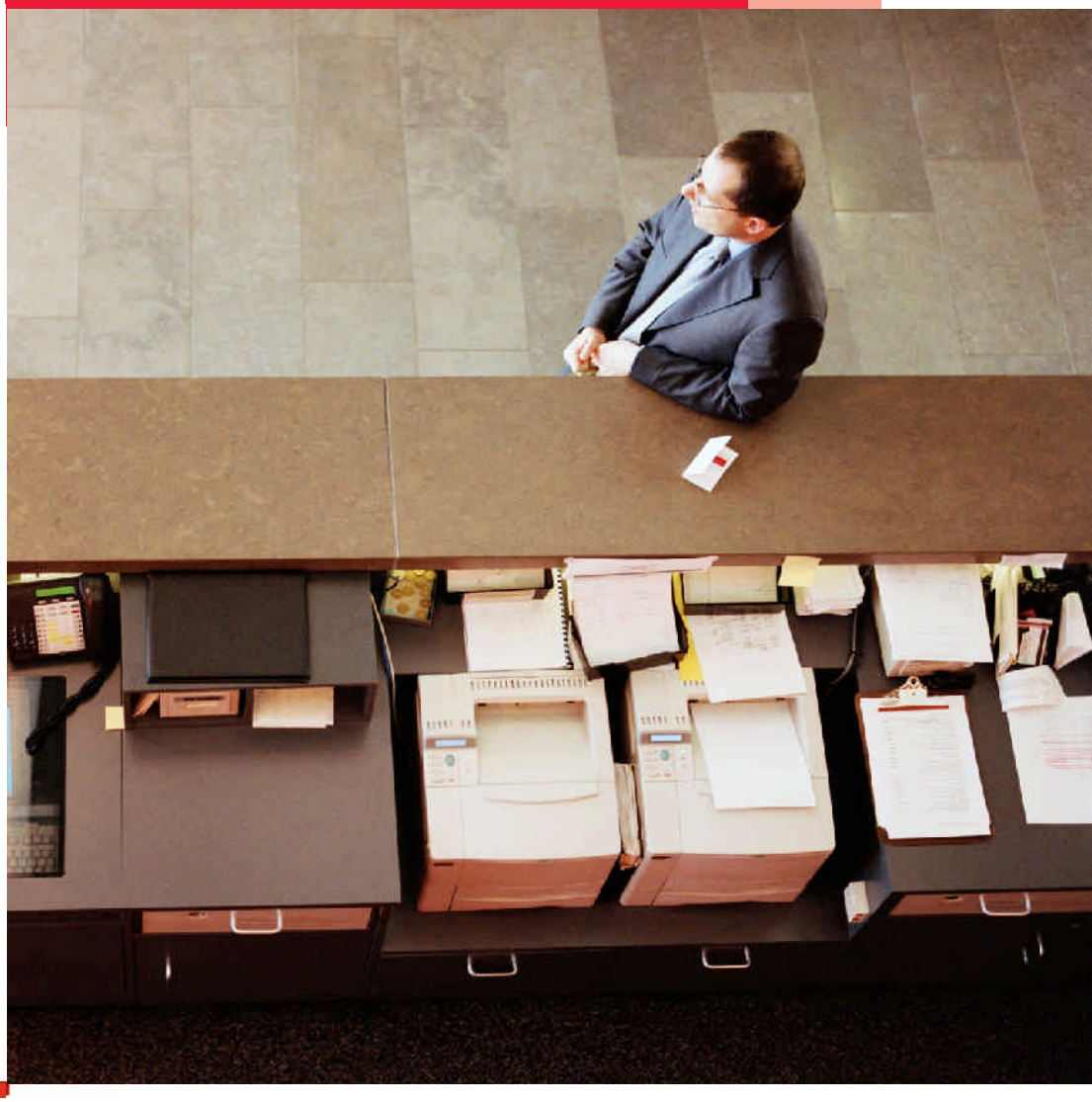
Ukraine

Global Economic Crime Survey

Cybercrime in the spotlight

3, 877 respondents from organisations in 78 countries provide a global picture of economic crime

December 2011



pwc

Contents

Executive summary

Economic crime does not discriminate. It affects organisations all over the world, and no industry or organisation is immune. The fallout cannot be measured simply by the direct costs, as economic crime can seriously damage brands or tarnish a reputation, leading organisations to lose market share. As society becomes less tolerant of unethical behaviour, businesses need to make sure they're building – and keeping – the public's trust.

This year's Economic Crime Survey turns the spotlight on to the growing threat of cybercrime. Today, most people and businesses rely on technology, including the Internet. In doing so, they are opening themselves up to potential attacks from criminals anywhere in the world. Against the backdrop of data losses and theft, computer viruses and hacking - our survey looks at the significance and impact of this new type of economic crime and how it affects businesses worldwide.

The survey was designed to seek the respondents' views on economic crime in general, and to spot long-term trends and questions specifically related to cybercrime, the threats posed by cybercrime, and how organisations work to counter any cyber attacks.

This year's report is divided into two sections:

1. Cybercrime – its impact on organisations, their awareness of the crime, and what they are doing to combat the risks.
2. Fraud, the fraudster and the defrauded – types of frauds committed, how fraud is detected, who commits fraud, and the repercussions for those who are caught.

This is the sixth time that the Global Economic Crime Survey has been administered globally and the second time in Ukraine.

Almost 4,000 respondents from 78 countries completed it globally. Of the total number of global respondents, 53% were directors or senior executives of their respective organisations, 36% represented listed companies and 38% represented organisations with more than 1,000 employees.

The number of participants from Ukraine increased by 23% in comparison to last survey and included 84 Ukrainian senior executives and managers representing 13 industries.

Key findings

Cybercrime in Ukraine

- Cybercrime has become one of top five economic crimes in Ukraine.
- Every 3rd respondent (37%) believes that the risk of cybercrime has increased over the past 12 months.
- More than 25% of organisations do not have adequate cybercrime incident response mechanisms/policies.
- 46% of respondents have not received any training related to cyber security during the last 12 months.
- 58% of respondents in Ukraine report that their organisations do not monitor the use of social media sites.

Economic crime in Ukraine

- 36% of organisations had experienced economic crime in the past 12 months
- Every 3rd organisation does not perform risk assessments.
- Assets misappropriation (73%), bribery and corruption (60%) remain the most common types of crime in Ukraine.
- The number of internal frauds has increased significantly (by 22%) since 2009.
- The majority of Ukrainian respondents who faced economic crime estimated losses up to $5m.
- 40% of crimes are committed by senior management
- Every 5th organisation that has suffered from economic crime has not taken any actions against an internal perpetrator of fraud.

Due to the ambiguity surrounding the definition of cybercrime and what it constitutes, organisations may not be fully aware of the risks associated with fraud, and find it difficult to detect and combat

Cybercrime in the spotlight

In PwC's view, there are five main types of cyber attacks, each with its own distinct – though sometimes overlapping – methods and objectives. They are:

Financial crime and fraud. This involves criminals – often highly organised and well-funded – using technology as a tool to steal money and other assets.

Espionage. Today, an organisation's valuable intellectual property includes corporate electronic communications and files as well as traditional intellectual property such as research and development outputs. Theft of intellectual property is a persistent threat, and the victims may not even know it has happened – until knock-off products suddenly appear on the market, or a patent based on their research and development is registered by another organisation.

Warfare. This can take place between states, or may involve states attacking private sector organisations, especially critical national infrastructure such as power, telecoms and financial systems.

Terrorism. This threat overlaps with the warfare threat. Attacks are undertaken by terrorist groups (possibly state-backed), again targeting either state or private assets, and often critical national infrastructure.

Activism. This may again overlap with some other categories, but the attacks are undertaken by supporters of an idealistic cause.

There is no globally accepted standard definition of cybercrime available. The implication of not having a clear-cut definition is that if organisations do not know about the dangers, it's harder to detect and combat cybercrime – essentially, if the "concept of the enemy" is blurred, any efforts to fight them might prove futile.

Is cybercrime therefore simply a means by which a criminal commits an illegal act, or is it an economic crime in its own right?

Should organisations take specific measures over and above other fraud prevention and detection methods to manage this risk?

Our 2011 survey takes a closer look at these issues.

For the purposes of our survey questionnaire, Cybercrime was formally defined as follows: "***Cybercrime, also known as computer crime***, *is an economic offence committed using the computer and Internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing, pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by product in order to create the fraud, and only includes such economic crimes where a computer, the Internet or the use of electronic media and devices is the main element and not an incidental one*"[1].

[1] As defined in the Global Economic Crime Survey 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer.

Cybercrime ranked as one of the top 5 frauds in Ukraine

Cybercrime is ranked as one of the top five types of economic crime in Ukraine (see Figure 1). The other four are: asset misappropriation, bribery and corruption, anti-competitive behaviour and accounting fraud.

This year's survey shows that cybercrime represents 23% of frauds reported globally, and 17% in Ukraine. Current information security trends indicate that cybercrime attacks are becoming more sophisticated and harder to detect and prevent, resulting in much greater damage.

Emerging risk or existing and growing fraud?

Not all of the five main types of cyber attack that were previously defined are common in Ukraine, however it is clear that the threat of cybercrime has become a real issue that may impact Ukrainian organisations.

In previous editions of the Global Economic Crime Survey, we asked respondents about their experiences involving cybercrime. Since the reported cybercrime levels were statistically insignificant, the results were not presented separately in our 2009 survey.

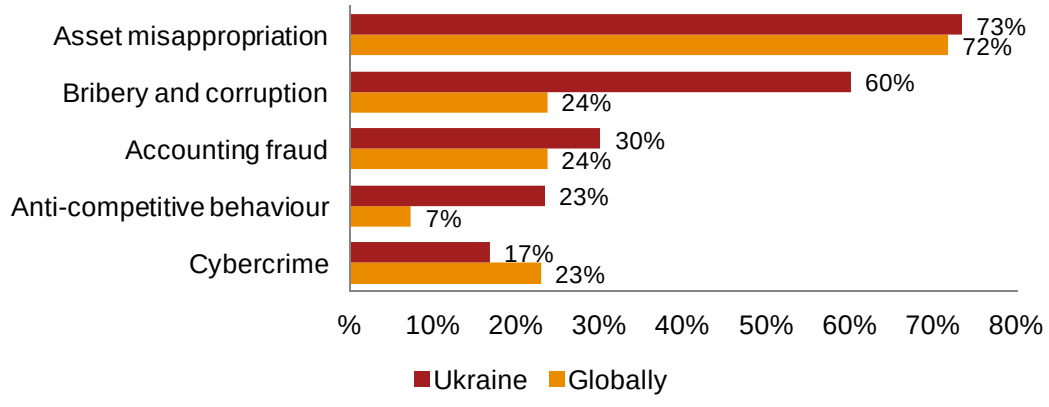
Given the increasing concerns around cybercrime, we focused on this fraud activity in 2011 and reintroduced it in questions regarding the different types of fraud, asking the respondents whether they had experienced cybercrime in the past 12 months.

More than one third (37%) of Ukrainian respondents said they perceive the risk of cybercrime to be on the rise, while only 4% indicated a decrease. The remainder (59%) believe that the situation has not changed.

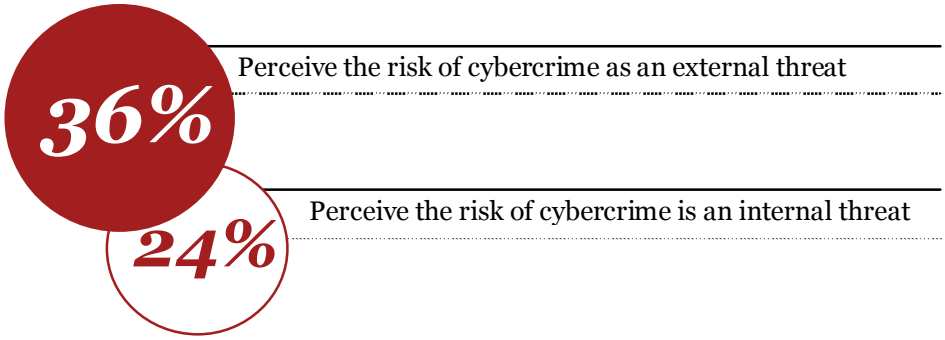
The increasing risk of cybercrime can be explained in the following ways:

- Increased media attention around recent cybercrime cases, leading to a heightened awareness of this type of fraud. Organisations may have put extra controls in place to detect and report such economic crimes;
- Due to the ambiguity around the definition of cybercrime and what it constitutes, the respondents may have re-classified some of the more traditional types of economic crimes as cybercrime because these were committed through the use of a computer, electronic device or the Internet;
- Increased focus from regulators;
- Advancements in technology may have made it easier to commit cybercrimes.

Figure 1: Top five types of economic crime reported in Ukraine and globally in 2011



Respondents who experienced economic crime in the last 12 months



Is cybercrime an external threat?

36% of respondents in Ukraine feel that cybercrime is an external threat, another 34% would treat it as both an internal and external threat, and the 24% state that it is internal.

Such results differ from those reported globally, where 46% of respondents recognise the risk of cybercrime coming mainly from external fraudsters, whereas crimes committed from inside the organisation account for 13% and 29% believe the fraud comes from both internally and externally.

Where does it come from?

We asked organisations if they thought the risk of external cybercrime mainly came from inside their own country or from other nations.

More than half (53%) of respondents in Ukraine mentioned that external cybercrime threats come from within the country. Customers and vendors were commonly reported as key external perpetrators. Still, over 40% of survey participants believe that threats come from both inside and outside the country of their operations.

The top three countries reported in Ukraine as the likely home of cybercrime threats are Hong Kong (and China), Russia and the USA. However, a significant number of Ukrainian organisations consider cybercrime threat comes from Ukraine as well as from other countries.

Globally the statistics are similar to the Ukrainian results, as the following six countries are perceived to be the likely home of cybercrime: Hong Kong (and China), India, Nigeria, Russia, Ukraine and the USA[1].

The reality is that cybercrime is a real global threat that can come from anywhere in the world, and it is not restricted by jurisdictional boundaries like many other conventional crimes

Where does the internal risk reside?

In Ukraine, the Information Technology ("IT") department of an organization is considered to be the most risky in terms of the internal cybercrime threat – according to 67% of respondents. This is not surprising, as they expect that IT personnel have the necessary skills and access to commit these crimes (e.g. extra administrative rights to access systems and the ability to delete audit trails, making it harder to detect their wrongdoing, etc.).

However, it is interesting that respondents also perceive other departments (Finance – 47%, Marketing and Sales – 37%, Legal – 27%, Operations – 22%) as potential sources of cybercrime threats, as well as representatives of the senior executive level (29%). Similar results are observed globally.

Respondents believe that the risk of cybercrime is least likely to come from the Information and Physical Security (16%) and Human Resources (10%) departments – however organisations should not ignore these departments, as cybercrime can happen anywhere.

[1] Countries are listed in alphabetical order

58% of respondents stated that their organisation does not monitor the use of social media sites, or they are not aware of it

Is there any danger in social media sites?

58% of respondents in Ukraine and 60% globally stated their organisation does not monitor the use of social media sites, or that they are not aware of such monitoring. This is startling because these sites can present big security risks if employees abuse them.

The younger generation typically uses social media extensively, and there is considerable peer and social pressure to share information with others – therefore, not monitoring these sites may create potential issues for organisations from a cybercrime perspective.

However, one needs to add that this generation grew up with social media sites, and sharing personal information has become the norm for the whole generation.

Organisations need to be aware that the younger generation might have a very different understanding of the risks such sites pose, and hence need to be educated accordingly.

How to reduce the risk?

Given that people think that cybercrime is on the rise, it is worrying to learn that 46% of respondents in Ukraine and 42% globally have not performed any cyber security training for their employees in the past 12 months – which would suggest that they are potentially unaware of the risks that cybercrime presents to their organisation.

How efficient are trainings to prevent cybercrime?

We asked people what training, if any, they have had. Only one in six respondents who have had trainings – received them face-to-face. 62% received other kinds of trainings such as e-learnings, email announcements, etc.

It is not surprising that there is so little face-to-face training, as it is generally time consuming and more costly. However 56% of respondents said that face-to-face trainings are the most effective form when it comes to cybercrime awareness.

What if a crime occurs?

The top three reactions of Ukrainian organisations in response to a potential cybercrime would be:

- Consult internally with experienced staff to resolve the matter;
- Consult with experts who are external to the firm; and
- Inform law enforcement.

The most common actions taken against external perpetrators of fraud were informing law enforcement and notifying the relevant regulatory authorities as well as proceeding with civil actions, including recoveries and cessation of the business relationship.

Identified internal perpetrators of fraud were fired in the most cases (73%).

While social media sites may not be the real source of cyber economic crime, they can be used to socially engineer cyber economic crime to be more effective.
This media can make phishing attacks more effective. For example, social media sites can be used to collect information about a targeted individual (also known as spear fishing), to research certain staff members, or to install malware onto the user's computer, making the cybercrime more effective.

Executive recognition of the strategic value of security is now more closely aligned with business than with IT

What are the responses from organisations?

As we saw earlier, nearly half of respondents who had experienced economic crime in the past 12 months said they perceive the risk of cybercrime to be growing.

Based on reported frauds, cybercrime ranks in the top five types of fraud. A large number of Ukrainian organisations (50%) are addressing fraud risks by introducing in-house capabilities to prevent, detect and investigate cybercrime.

Also, organisations based in Ukraine tend to engage with an external consultant once an incident has occurred (57%), compared to only 21% of organisations that prefer to preventatively engage external consultants.

Table 1: Cybercrime incident response mechanisms used by organisations in Ukraine in 2011

In-house capabilities to prevent and detect cybercrime	51%
In-house capabilities to investigate cybercrime	50%
Involvement of Forensic technology investigators	45%
Media & PR management plan	38%

% of all respondents

How to defend?

1. Get the CEO involved – the CEO and the Board need to be aware of the cyber threats. Top management needs to understand the risks of the cyber world.

2. Reassess the security function – unlike traditional 'economic crimes', cybercrime is fast paced with new risks constantly emerging, which means an organisation need to continually adapt its procedures.

3. Awareness – organisations need to have a clear awareness of its current and emerging cyber environment. If this is in place, well-informed and prioritised decisions and actions can be taken

4. Create a cyber incident response team – which needs to act with speed and agility. A well functioning cyber response team means an incident that is spotted anywhere in the business will be tracked, the risk assessed, and the threat negated.

5. Educating all employees – organisations need to embed a 'cyber awareness' culture, through recruiting those with the relevant skills so that this knowledge can be shared with all employees, creating a cyber aware organisation which is better able to protect itself.

6. Take a more active and transparent stance towards cybercrime – respond by pursuing cybercrime perpetrators through legal means, and communicate more publicly regarding the actions that organisation is taking regarding the threats, incidents and responses.

Cybercrime is more than just an IT issue

Traditionally, cyber security has been perceived as an IT issue, creating a communication gap between business managers and security professionals.

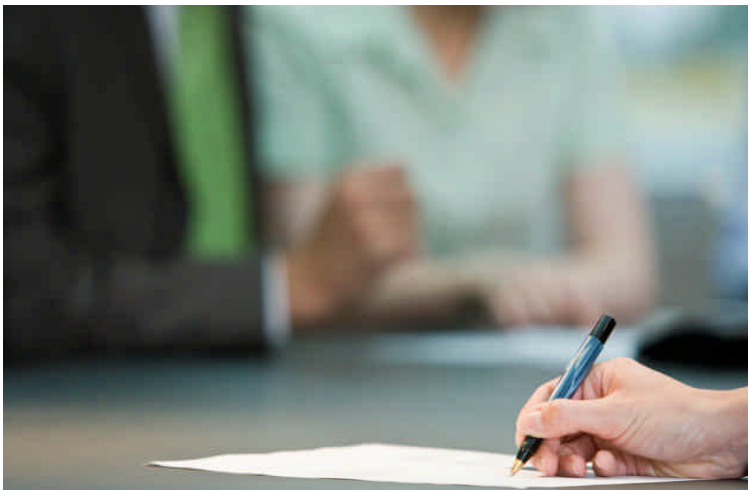
PwC's Global State of Information Security Survey 2011 confirms that cyber security is not only a technical issue, but a core business imperative.

We asked organisations who should ultimately be responsible for dealing with cybercrime threats. More than half of the respondents (67%) pointed to the Chief Information Officer (CIO) or Technology Director; only 13% suggested the Chief Executive Officer (CEO) or the Board. This suggests that, whether or not the CIO sits on the Board, they do not share ultimate responsibility with the CEO or the board as a whole.

Only 20% of respondents said that the CEO and the Board review these risks at least once a year, and more than quarter (32%) said that they only review them on an ad hoc basis compared to 25%, who do not perform assessments at all.

We would expect the CEO and the Board to understand and investigate cybercrime risk related matters on a regular basis.

36% of organisations in Ukraine have experienced economic crime in the past 12 months



Overview of fraud in Ukraine

36% of respondents in Ukraine report that they have experienced at least one instance of economic crime in the past 12 months. This is higher than figures reported globally (34%), but lower than indicators reported in 2009 (45%).

We may assume that the results of the 2009 survey were affected by the economic recession, which was followed by increased instances of fraudulent activity.

We believe that the decrease reported by Ukrainian organisations for fraud in 2011 is explained by a low detection rate rather than an actual decrease of fraud cases.

To determine this, we compared the level of reported fraud by organisations which perform regular risk assessments with those that do not assess fraud risks regularly.

As a result, the organisations performing regular risk assessments report more fraud with a higher frequency of its occurrence.

However, we expect executives to know about these crimes. Happily, in 2011 executives are better informed about fraud instances in their organisations than in 2009: only 10% of respondents who did not know if their organisations faced fraud risks were senior executives, compared to 55% in 2009.

In order to ensure that a business operates efficiently, organisations need to pay more attention to anti-fraud and risk management procedures.

Organisations performing regular risk assessments, report more fraud and a higher frequency of its occurrence

Fraud by ownership type

The majority of survey participants in Ukraine represent private organisations (69%) and publicly listed organisations (24%).

Governmental, state-owned and non-profit organisations, which represent 7% of the survey participants, confirmed that they either have not experienced economic crime during past 12 months, or are not aware of such instances.

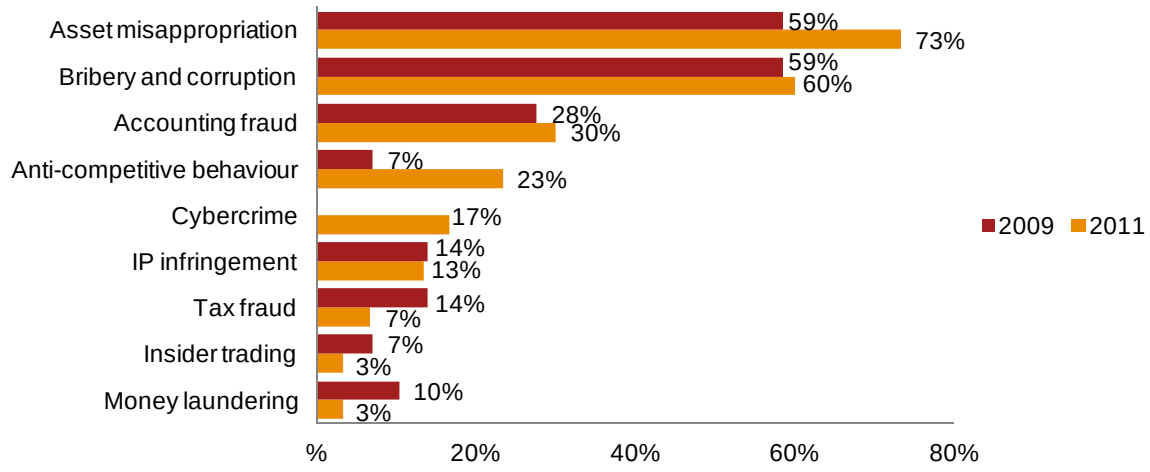
However, private organisations are almost 3 times more likely to face economic crime than publicly listed organizations. The most common types of fraud with private organisations are:

- Assets misappropriation (31%),
- Bribery and corruption (29%), and
- Accounting fraud (14%).

Publicly listed organisations are primarily affected by:

- Assets misappropriation (37%),
- Bribery and corruption (21%), and
- Cybercrime (16%).

Figure 2: Types of fraud incidents in 2009 and 2011



% respondents who experienced economic crime in 2009 and 2011

What types of fraud are organisations facing in Ukraine?

Economic crimes can take on many different forms, with some being more common and more persistent than others. In 2011, the most widespread type of crime in Ukraine was assets misappropriation (73%), followed by bribery and corruption (60%), and accounting fraud (30%).

Survey results indicate that Ukrainian organisations suffer much more from "bribery and corruption" and "anti-competitive behaviour" than other countries in Central and Eastern Europe and globally (see Table 2).

Table 2: Types of fraud in Ukraine which significantly differ from CEE and globally in 2011

	Bribery and corruption	Anti-competitive behavior
Ukraine	60%	23%
CEE	36%	12%
Globally	24%	7%

% respondents who experienced economic crime in the last 12 months

Such a significant number of reported fraud instances may also mean that these are not only the most popular types of fraud, but also that this type of fraud is easier to detect than the other types.

Instances of "assets misappropriation" and "anti-competitive behaviour" increased almost by 15% compared to 2009. Meanwhile, "bribery and corruption" and "accounting fraud" stayed at the same level.

These changes force those who wish to commit fraud to develop new and more sophisticated ways to commit their crimes and remain undetected. Nowadays, these individuals are well equipped technically, while internal investigators are only starting to develop in-house mechanisms for prevention and investigation. The economic slowdown makes organisations reluctant to spend funds on in-house services such as audit or internal forensics.

Does the size of the organisation matter?

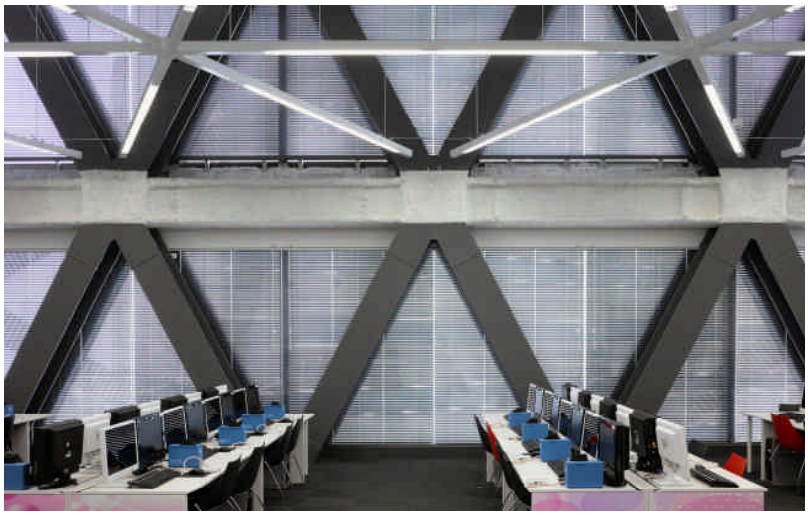
This year's results show that all Ukrainian organisations (no matter their size) suffer equally from economic crimes.

Table 3: Fraud indicated in 2011 by the size of organisations in Ukraine

Up to 200 employees	27%
201 to 1,000 employees	30%
1,001 to 5,000 employees	23%
More than 5,000 employees	20%

% respondents who experienced economic crime in the last 12 months

More than 40% of respondents in Ukraine expect incidents of bribery and corruption within the next year



What industries are the most affected?

This year's survey represents views of representatives from more than 13 different industries. Financial services, retail and consumer, manufacturing and professional services represent more half (63%) of all survey participants both in Ukraine and worldwide.

Every 2nd respondent working in financial services, energy, utilities and mining experienced economic crime during the last 12 months.

Comparing incidents of crime by industries, we note an increase in fraud in the retail and consumer industry by 6%, and 5% in the financial services in 2011.

Future expectations

Despite a decrease of 9% in the levels of bribery and corruption reported, more than 40% of Ukrainian respondents are expecting its occurrence within the next 12 months. Two other leading types of fraud are expected to be Intellectual Property infringement (36%) and assets misappropriation (35%).

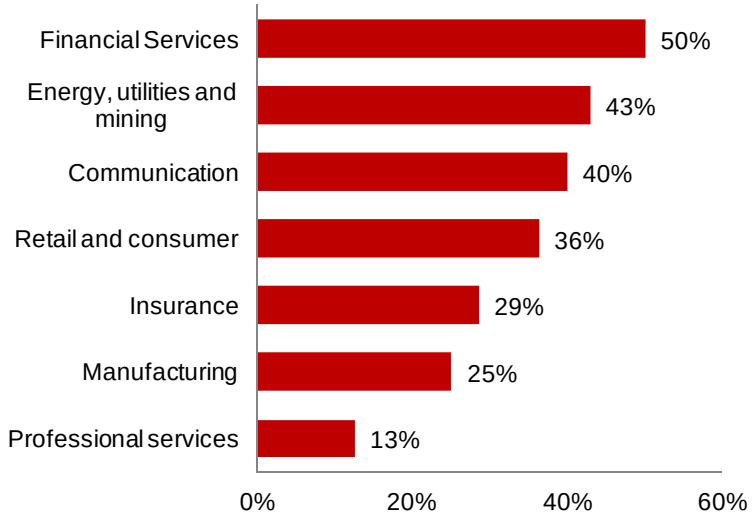
Organisations globally expect an increase in asset misappropriation (34%), cybercrime (26%) and bribery and corruption (23%).

Table 4: Types of fraud Ukrainian organisations anticipate will occur in the future

Bribery and corruption	42%
IP infringement	36%
Assets misappropriation	35%
Accounting fraud	25%
Cybercrime	25%
Anti-competitive behavior	24%
Money laundering	17%
Tax fraud	14%
Insider trading	12%
Espionage	10%

% all respondents

Figure 3: Fraud reported by industry segment in Ukraine in 2011



% respondents from particular industry who experienced fraud in the last 12 months

40% of crimes in Ukraine are committed by senior management

A very typical perpetrator of fraud worldwide is the so-called 'white-collar criminal'.

A white-collar criminal is a 30+ years old male individual, with a postgraduate education, having good psychological health and a stable family situation.

Portrait of a Fraudster

This year, organisations equally suffer from both internal and external fraudsters, though since 2009, the number of serious economic crimes committed by internal offenders increased by 22%.

Table 5: Perpetrators of fraud

	2011	2009
Internal fraudsters	56%	28%
External fraudsters	40%	72%
Don't know	3%	0%

% respondents who experienced economic crime

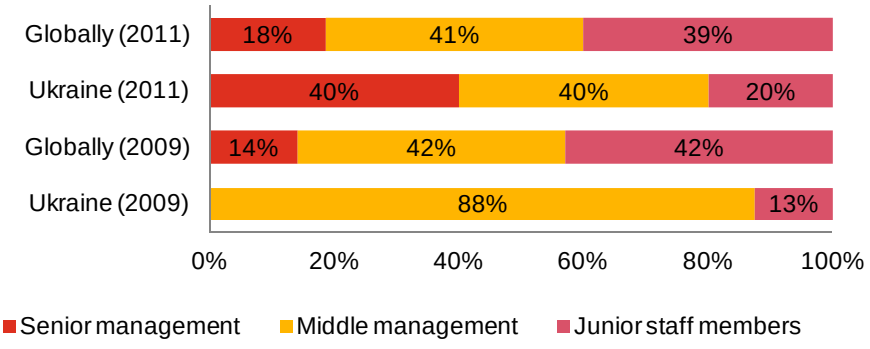
The majority of internal fraudsters in Ukraine are representatives of senior (40%) and middle management (40%). To compare, 60% of internal crimes globally are performed by middle management and junior staff.

The average perpetrator of internal fraud in Ukraine is male, degree university graduate, 31-50 years old, who has been employed with the organisation for a period of 3 to 10 years.

Both in Ukraine and globally, the main perpetrator of external fraud is a customer (43% for Ukraine and 35% globally). Other external fraudsters include agents and intermediaries (14%) and vendors (14%).

One of the key fraud prevention techniques is to know who you are doing business with. Thus, know your customer, vendor, and agent due diligences are becoming more recognised as a critical element of any risk reduction program.

Figure 4: Main perpetrators of internal fraud in Ukraine and globally



Respondents who experienced economic crime in 2009 and 2011

The majority of Ukrainian respondents that experienced an economic crime in the last 12 months estimated losses up to $5m

How much does fraud cost organisations?

The majority of those respondents who said they had experienced economic crime in the last 12 months reported losses up to $5m. The top three most expensive types of fraud were also the most common types, including assets misappropriation, bribery and corruption and accounting fraud. Comparing 2011 with 2009, there is a noticeable increase in both the frequency and cost of these types of fraud.

Cases of fraud committed by employees are usually more expensive for organisations than frauds committed by external parties i.e. customers, vendors or agents.

The cost of crime increases with the fraudsters' age. For example, the more expensive crimes (between $5m and $100m) were committed by individuals older than 50 years old.

Cost of collateral damage

The financial losses are just one aspect of the damage that organisations face from fraudulent activities, and might be far from the most important. The collateral damage suffered, and its impact on the reputation/brand, share price, employee morale, business relations, and relations can be a significant cost to any business.

Of those who had experienced economic crime as a result of fraud this year, 23% reported damage to employee morale, 17% noticed damage to the organisation's brand, 13% to relations with regulators and another 13% to business relations.

Even though these figures are consistent with similar results reported by organisations globally, collateral damage is significantly lower in 2011 compared to 2009, when employee morale damage accounted for 34%, damage to relations with a regulator for 34%, 28% for damaged business relations, and 14% for damage to a brand.

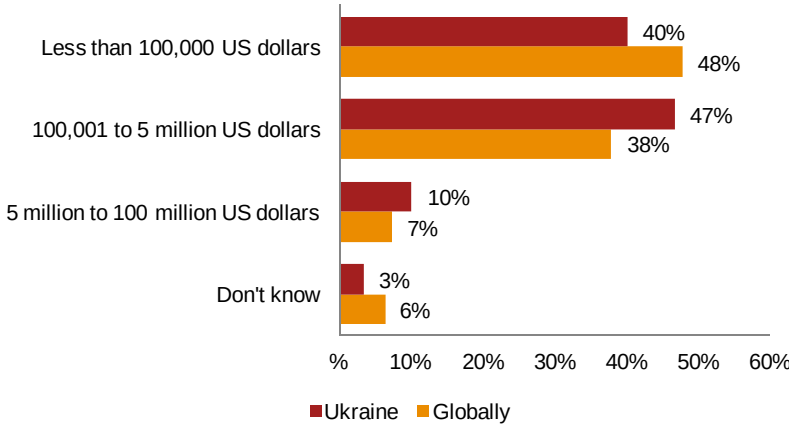
Table 6: Comparison of collateral damage in Ukraine in 2009 and 2011

	2011	2009
Relations with regulators	13%	34%
Employee morale	23%	34%
Business relations	13%	28%
Reputation/brand	17%	14%
Share price	7%	1%

% respondents who experienced economic crime

The low indicators of collateral damage in 2011 are surprising. Fraud is become to be viewed as an inherent feature of doing business in Ukraine, which leads organisations down a worrying path where the organisations themselves provide a rational for potential fraudsters, and therefore increase the probability of fraud.

Figure 5: Financial losses from economic crimes in Ukraine and globally in 2011



% respondents who experienced economic crime in the last 12 months

How do organisations detect fraud?

Fraud detection refers to all methods employed by organisations to find out if an economic crime has been committed. In 2011, Ukrainian respondents indicate that the following methods are the most effective for revealing fraud.

In Ukraine the majority of crimes are detected with the help of Corporate Security. Only 6% of frauds are identified by Internal Audit. The global results show a completely opposite situation.

It is also worth mentioning that 27% of respondents were not aware of the way fraud was initially detected, compared to 10% globally. This means that organisations in other countries maintain a higher level of awareness about anti-fraud programs.

More than half of survey participants (54%) do not use a whistle-blowing system. However, 82% of those who employed such a system consider it to be effective.

What actions are taken by organisations against the fraudsters?

73% of perpetrators of internal fraud were dismissal and faced civil actions, including recoveries. Notably, organisations have taken no action in 20% of incidents. In 2009, this figure was only 3%, so the increase represents a worrying statistic.

In some organisations there seems to be complacency or a wish to deal with fraud in a low-key way. We question this approach. Is it right to keep the fraudster in the organisation and to run the risk that they might do it again? We think organisations should show 'zero tolerance' towards fraud, and to set the right tone by dealing with the fraudster officially, and by involving outside authorities.

The following actions have been taken by Ukrainian organisations against external fraudsters:

- Informing law inforcement (71%);
- Civil actions, including recoveries (64%);
- Cessation of the business relationship (57%); and
- Notification of the relevant regulatory authorities (43%).

These figures coincide with the global statistics, as well as with the results of the 2009 survey.

It is worrying that 43% said their organisation still has a business relationship with a fraudster– perhaps highlighting some fundamental concerns regarding the culture of the organisation.

Figure 6: Fraud detection methods used in Ukraine and globally in 2011

% respondents who experienced economic crime in the last 12 months

Terminology

Due to the diverse descriptions of individual types of economic crime in the legal statutes of different countries, we developed the following categories for the purpose of this survey. These descriptions were defined in the web survey to assist respondents in completing the survey.

Accounting fraud

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

Anti-competitive behaviour

Includes practices that prevent or reduce competition in a market such as cartel behaviour involving collusion with competitors (for example, price fixing, bid rigging or market sharing) and abusing a dominant position.

Assets misappropriation (including embezzlement/deception by employees)

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

Corruption and bribery (including racketeering and extortion)

The unlawful use of an official position to gain an advantage in contravention of a duty. This can involve the promise of an economic benefit or other favour, or the use of intimidation or blackmail. It can also refer to the acceptance of such inducements.

Cybercrime incident response mechanism

This would typically include in-house technical capabilities to prevent, detect and investigate cybercrime, access to forensic technology investigators, media and PR management plan, controlled emergency network shut down procedures, etc.

Economic crime or fraud

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

Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information or using technology to act on your behalf as a spy.

Fraud risk assessment

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

(i) The fraud risks to which operations are exposed;

(ii) An assessment of the most threatening risks (i.e. evaluate risks for significance and the likelihood of occurrence);

(iii) Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;

(iv) Assessment of the general antifraud programmes and controls in an organisation; and

(v) Actions to remedy any gaps in the controls.

Insider trading

Insider trading refers generally to buying or selling of a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non public information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

Intellectual Property infringement (including trademarks, patents, counterfeit products and services)

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

Money laundering

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

Senior executive

The senior executive (for example the CEO, Managing Director or Executive Director) is the main decision maker in the organisation.

Sustainability activities

Includes activities such as carbon credit trading (buying and selling carbon credits), or engaging in projects which create carbon emissions offsets.

Sustainability fraud

Fraud in relation to sustainability activities (refer to sustainability activities) such as carbon trading markets, environmental claims or statutory declarations.

Contacts

PwC provides industry-focused assurance, tax and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 169,000 people in 158 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice. You can find out more information by visiting www.pwc.com.

Forensic services

With the largest network of forensic services practices in the world, spanning 63 countries and employing over 1,400 advisors, PwC firms can draw on a vast experience of dealing with difficult situations across a broad spectrum of industries in many jurisdictions.

Our fast-growing Forensic services practice in CEE employs over 70 professionals, including accountants, economists and IT professionals.

Our services include:

- Investigations
- Fraud risk management
- Commercial disputes
- International arbitration
- Transaction and shareholder disputes & investigations
- Forensic technology solutions
- Intellectual property services
- Licensing management services
- Insurance claims services
- Anti-money laundering services
- Capital project services
- U.S. regulatory investigations and securities litigation

Forensic services team

Rafal Krasnodebski
Partner
Advisory services
rafal.krasnodebski@ua.pwc.com

Irina Novikova
Partner
Forensic services in Russia
irina.n.novikova@ru.pwc.com

Gennadiy Chuprykov
Senior Manager
Forensic services leader for Ukraine
gennadiy.chuprykov@ua.pwc.com

Victoriya Tsytsak
Manager
Forensic services in Ukraine
victoriya.tsytsak@ua.pwc.com