www.pwc.com/crimesurvey

Cybercrime: protecting against the growing threat

Global Economic Crime Survey

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

November 2011

pwc

Contents

Forewords

Cybercrime: a new and serious threat

It's been ten years since we did our first survey into economic crime. And what an eventful decade it has been.

We have seen multi-billion dollar accounting fraud cases hit the headlines. We have witnessed the start of the worst economic crisis since the 1930s. And we have seen technology transform the way we do business – and live our lives.

We have covered economic crime in the downturn and accounting fraud in previous surveys. Now we look at how our increasing dependence on technology is leaving us open to a new threat: cybercrime.

Ten years ago, our survey showed that hardly anyone knew what it was. But this year's report ranks it as one of the top four economic crimes – just behind asset misappropriation, accounting fraud, and bribery and corruption.

Businesses face serious threats from cyber criminals from within as well as outside. And it's clear that senior management need to take these risks more seriously: worryingly, four in ten respondents say their organisation doesn't have the capability to prevent and detect cybercrime.

Fraud is on the rise

What about fraud more broadly? Two years ago, almost half of our respondents thought fraud was on the rise. They told us there were more opportunities to commit fraud, and more pressure to do so. They were right: our 2011 survey shows that more organisations are saying they have been victims of fraud. And this year's respondents think the trend is going to continue.

So, ten years down the line, economic crime is still as big a threat as ever. We hope our report will give you some ammunition to fight back.

Tony Parton
Partner, Forensic Services, PwC UK

Fighting cybercrime from the top

Businesses and governments the world over are reaping the rewards of the cyber world, from social networking to cloud computing. The problem is that many of them have not yet got a handle on the risks – particularly at the most senior level.

Traditionally, leaders have pigeonholed cyber security as an IT problem. But that's a risk approach that could leave them open to attack.

It's not just about IT. It's about HR making sure employees understand the security policies, and recruiting people with the specialist skills to protect the organisation from cyber attacks. It's about legal and compliance making sure laws and regulations are respected. It's about physical security protecting sites and IT equipment. It's about marketing thinking about cyber security when they launch new products.

If organisations don't look at cyber security from all angles, they are missing a trick. And it's therefore a broad conversation that needs to happen at Board level. CEOs need to fully understand the risks to be able to deal with them.

CEOs need to take action

So what should CEOs do? They need to:

- define clearly who is responsible for what when it comes to cyber security
- keep updating their knowledge: cybercrime moves fast, and new risks are emerging all the time
- make sure their organisation is equipped to track risks and deal with incidents quickly.

Our respondents think cybercrime is on the rise. Organisations need to make sure they have got the right defences in place. And that is something that needs to come from the top.

William Beer
Director, Cyber Security Services, PwC UK

A note from our academic partner

I have welcomed the opportunity to advise PwC[1] on the development of their sixth Global Economic Crime Survey. Both the business and academic communities depend on reliable, unbiased information to advance the study of this topic.

This survey gains its value in the following ways: it is based on the perceptions of nearly 4,000 well-informed individuals world wide. We took great care in the framing of the questions and in how each would appear in the web-based questionnaire, including ensuring that at every point the reader was reminded of the definitions we wanted them to work to. Finally, we went through an extensive process of reviewing responses.

There are several significant problems in assessing cybercrime risks. There is no generally agreed definition; the same event might be 'industrial espionage', 'IP theft' as well as 'cybercrime'. When it comes to assessing costs, do you limit yourself to proven losses through fraud, or include remedial costs or extend that to reputational damage – and if so how do you measure it?

It is now essential for senior management to truly understand the risks and opportunities of the cyber world.

This global survey provides invaluable insights into the actualities of cybercrime risk.

Peter Sommer
Visiting Professor in the Department of Management (Information Systems and Innovation Group) at the London School of Economics and Political Science, and a Visiting Reader, Faculty of Mathematics, Computing and Technology, Open University

1. "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.

Executive summary

Economic crime does not discriminate. It is truly global. No industry or organisation is immune. We have seen a 13% rise since our last survey and organisations see more fraud ahead.

The fallout isn't just the direct costs: 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 are building – and keeping – public trust.

A decade on and the fraud risk continues to rise

Our sixth Global Economic Crime Survey turns the spotlight on the growing threat of cybercrime. Today, most people and businesses rely on the internet and other technologies. As a result, they are potentially opening themselves up to attacks from criminals anywhere in the world. Against a 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.

This year's global report is divided into two sections:

- Cybercrime – its impact on organisations, their awareness of the crime and what they are doing to combat the risks.
- Fraud, the fraudster and the defrauded – the types of economic crime committed, how they are detected, who is committing them and what the repercussions are.

The highlights

Cybercrime

- Cybercrime now ranks as one of the top four economic crimes.
- Reputational damage is the biggest fear for 40% of respondents.
- 60% said their organisation doesn't keep an eye on social media sites.
- 2 in 5 respondents had not received any cyber security training.
- A quarter of respondents said there is no regular formal review of cybercrime threats by the CEO and the Board.
- The majority of respondents do not have, or are not aware of having, a cyber crisis response plan in place.

Fraud, the fraudster and the defrauded

- 34% of respondents experienced economic crime in the last 12 months (up from 30% reported in 2009).
- Almost 1 in 10 who reported fraud suffered losses of more than US$5 million.
- Senior executives made up almost half of the respondents who didn't know if their organisation had suffered a fraud.
- 56% of respondents said the most serious fraud was an 'inside job'.
- Suspicious transaction monitoring has emerged as the most effective fraud detection method (up from 5% in 2009 to 18% in 2011).
- Organisations that have performed fraud risk assessments have detected and reported more frauds.

5 ways to protect your organisation against economic crime

1. Know who you are dealing with – staff, suppliers, partners and agents.
2. Align IT, Internal Audit and the Board in the fight against economic crime.
3. Conduct regular fraud risk assessments.
4. Leadership by a Cyber-Savvy CEO, who instils a cyber risk-aware culture.
5. Implement a cyber crisis response plan.

Cybercrime in the spotlight

For our survey questionnaire, we defined cybercrime as:

'an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one.'[2]

This is a fairly standard definition of cybercrime, but it seems many people interpret it in different ways.

For example, a sales executive who steals confidential sales and marketing data by copying it onto a USB stick or emails it to himself before joining a competitor might have committed a number of crimes. It could be intellectual property theft or a cybercrime or both.

There is currently no globally accepted definition of cybercrime. Therefore, organisations don't know about the danger, which means it's harder to detect and fight it. Essentially, if the 'concept of the enemy' is blurred, any efforts to fight it might prove futile.

So is cybercrime simply a means by which a fraudster commits the 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 survey takes a closer look at these issues.

In our view*, there are five main types of cyber attack, each with its own distinct – though sometimes overlapping – methods and objectives.

They are:

1. ***Economic crime*** – this involves criminals, often highly organised and well-funded, hacking into systems and using technology as a tool to commit fraud.
2. ***Espionage*** – today, an organisation's valuable intellectual property ('IP') includes electronic communications and files as well as traditional IP like research and development ('R&D'). IP theft is a persistent threat, and the victims might not even know it's happened – that is until counterfeit products suddenly appear on the market, or another company registers a patent based on their R&D.
3. ***Activism*** – the attacks are carried out by supporters of an idealistic cause, most recently the supporters of WikiLeaks.
4. ***Terrorism***[3] – terrorist groups might attack either state or private assets, often critical national infrastructure ('CNI') like power, telecoms and financial systems.
5. ***Warfare***[3] – this involves states attacking state or private sector organisations.

*See PwC's 'Delusions of Safety?' – The Cyber Savvy CEO Report, 2011

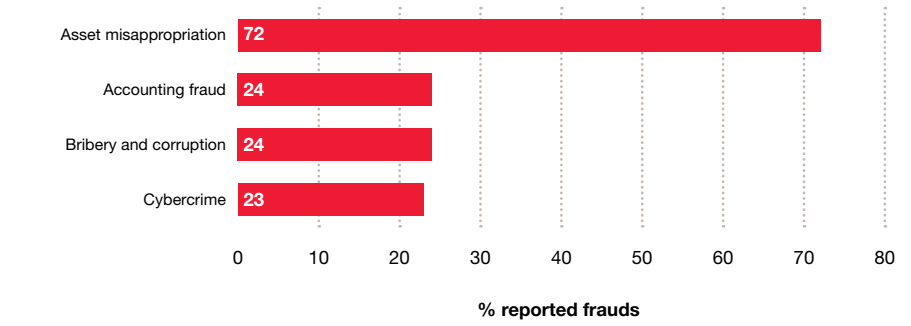
2. As defined in the Global Economic Crime Survey 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer.
3. Terrorism and warfare are types of cyber attacks that have been included for completeness, but they fall outside the definition and scope of the survey which focuses on economic crime.

'Individuals, businesses and governments all face a wide range of cyber security risks to their own interests'

'Future Global Shocks' Project, OECD[4] , 2011

4. OECD is the Organisation for Economic Co-operation and Development

Figure 1: Top four types of economic crime reported



% respondents who experienced economic crime in the last 12 months

Cybercrime: the next wave

In our survey, cybercrime ranks as one of the top four economic crimes.

In our previous economic crime surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. As a result, we combined the results with 'other types of fraud'.

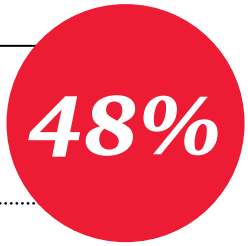
We focused on cybercrime this year and reintroduced it in the 'types of fraud' question, asking respondents if they had experienced cybercrime in the last 12 months. Of those respondents who said they had experienced some form of economic crime, almost 1 in 4 said they had suffered one or more cybercrime incidents in the last 12 months (see figure 1).

So how and why has cybercrime emerged as one of the top types of fraud? We believe that:

- because of media attention around recent cybercrime cases, organisations are more aware of this type of fraud and might have put extra controls in place to detect and report it
- because there is ambiguity around the definition of cybercrime and what it constitutes, respondents might have re-classified some of the more traditional economic crimes as cybercrime because someone used a computer, electronic devices or the internet to carry them out
- regulators are focusing on it more
- advancements in technology make it easier to commit cybercrimes.

Also, almost half (48%) of those who had experienced economic crime in the last 12 months said they perceive the risk of cybercrime to be on the rise. Only 4% perceive the risk to be falling and the rest think it will stay the same. These statistics clearly show that cybercrime is a growing threat.

48% of those who had experienced economic crime in the last 12 months said they perceive the risk of cybercrime to be on the rise



'Cyber security issues now top the list of risks to watch, ahead of weapons of mass destruction and resource security.'

World Economic Forum Global Risks 2011 report

Low risks and high rewards of cybercrime

We studied the attractions of cybercrime compared with other conventional crimes. Cybercrime presents different risks and rewards to those conventional crimes.

Take, for example, a cybercrime where an 'outside' fraudster infiltrates a banking system remotely to steal money or personal information. There are fewer risks when compared with physically stealing assets from an organisation:

- The fraudster is not present at the location in person, so there is less chance of getting caught in the act.
- There is less chance of law enforcement being able to identify the perpetrator or find out where they were based when they committed the crime. More often than not, the perpetrator is located in a different jurisdiction. This makes it harder to identify, arrest and prosecute them by traditional means. Current laws are not mature enough to prosecute cyber criminals with any impact. Technological advancements are fast-paced, which means the development of cybercrime is too. Organisations need to be up to date on the latest legislation and corporate policies to make sure they keep up.
- Given all these obstacles, the perpetrator can carry on returning to the scene of the crime with minimal fear of being caught.

Organisations can put preventative measures in place to reduce the risk of traditional economic crimes like asset misappropriation, accounting fraud, or bribery and corruption, but with cybercrime, it's much harder.

'Cyber security must be pursued with the same intensity as efforts to eradicate global poverty or tackle climate change'

William Hague, UK Foreign Secretary, November 2011

Is it just an external threat?

Since the rise of the internet, people have perceived cybercrime, traditionally, as an external threat. 46% of our respondents have a similar perception. But our survey results suggest that the perception of cybercrime is changing, and that organisations are now recognising the risk of cybercrime coming from inside.

Figure 2: Greatest risk of cybercrime threats comes from:

External fraudsters	46%
Both internal and external perpetrators	29%
Inside the organisation	13%
Don't know	12%

% all respondents

53% of the respondents who said the cybercrime threat was an internal one believe that there is a risk from the information technology ('IT') department. It's not surprising that many respondents think this, because they expect IT personnel to have the necessary skills and opportunity to commit these crimes. In particular, IT personnel might have 'super user' access, which gives them extra administrative rights to access systems and the ability to delete audit trails, making it harder to detect their wrongdoing.

But it is interesting to see that respondents realise other departments, like operations (39%), sales and marketing (34%) and finance (32%), also pose risks.

Respondents believe the risk of cybercrime is least likely to come from the human resources ('HR') (14%) and legal (8%) departments. But organisations shouldn't ignore these departments, as cybercrime can happen anywhere – for example, a malicious employee with access to confidential HR data or legal documents.

As well as direct financial costs, there are other commercial consequences, such as reputational/brand damage, poor employee morale or service disruption. We've given some examples of potential cybercrimes below. Some of them contain elements of other forms of economic crime as well:

- A disgruntled employee gets hold of confidential information they shouldn't have, like pay, bonuses and other rewards, and uses this information to their advantage.
- An employee gets hold of information from the accounts payable department, sets up dummy supplier information, and extracts money from the company in this way.
- An employee shares some sensitive information with their 'friends' or connections on social media and it leaks out into the public domain.
- An employee accesses a colleague's email account and sends malicious emails from it, bullying other members of staff ('cyber-bullying'). Although this might not result in direct financial losses, it could certainly affect the organisation's reputation, disrupt operations, or result in big legal bills.

Are these strictly cybercrimes or are they forms of economic crime where a computer and the internet are just a means to an end? It doesn't really matter about the definition of cybercrime and what it constitutes – it's clear from the results of our survey and the examples that the threat doesn't just come from the IT department but from all departments in the organisation.

But if it is an external threat, 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 abroad. The countries most mentioned by those respondents who said the threat came from outside their country[5] were Hong Kong (and China), India, Nigeria, Russia and USA. These countries were perceived to be the most likely origins for perpetrating cybercrime. We believe that this is only a perception, as cyber attacks can be initiated from anywhere in the world and attribution is extremely difficult.

5. This question was asked to all respondents who indicated the cybercrime risk was coming from outside their country or from both within and outside their country of operation.

For example, there is no evidence to suggest that Nigeria is a hi-tech crime hub, but people might consider email-based scams, like those asking for payments in advance (so-called '419' frauds), as a form of cybercrime. The high ranking of the US and India suggests people think countries with IT-savvy populations and where online shopping has taken off are higher risk.

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

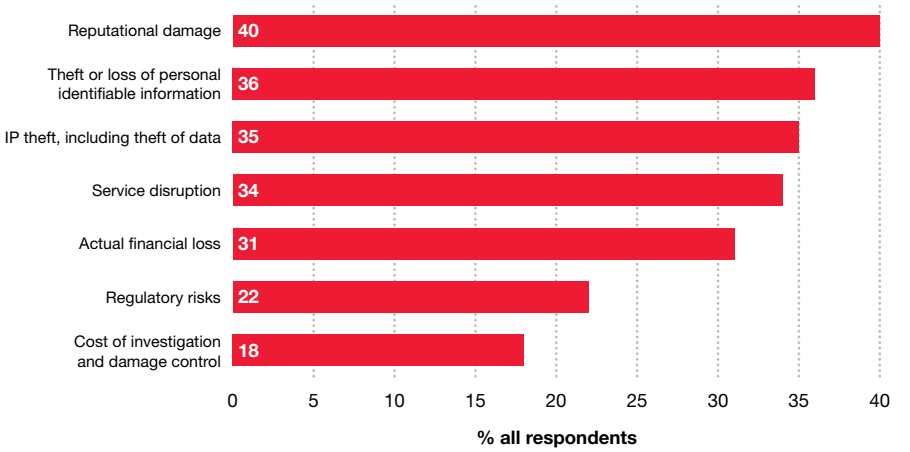
Just as black markets exist for consumer goods, criminal exchange websites, like Dark Market, are emerging, where stolen credit card details are sold for as little as a few cents. There is also the new form of political activism, 'hacktivism', with the Anonymous group as the leading perpetrators. They recently hacked into major credit card companies because those companies withdrew support from WikiLeaks, and threatened to expose members of a Mexican drug cartel for kidnapping one of the Anonymous hackers[6].

What are organisations really worried about?

We asked organisations what aspects of cybercrime they were most concerned about. 40% of respondents mentioned reputational damage. Other high-ranking risks were the theft or loss of personal data, IP theft and service disruption (see figure 3).

Because organisations are very concerned, particularly about reputational damage, it is important for them to show they are the most secure business in the market if they want to gain competitive advantage.

Figure 3: Concerns about cybercrime



Do organisations know what's out there?

As we saw earlier, nearly half of respondents who'd experienced economic crime in the last 12 months said they perceive the risk of cybercrime to be growing. Although they are aware of the risks, organisations are doing little about it, and continue to be reactive rather than proactive in fighting cybercrime.

- 61% said they don't have, or are not aware of having, access to forensic technology investigators
- 60% said they don't have, or are not aware of having, the in-house capability to investigate cybercrime
- 56% said they don't have, or are not aware of having, a media and public relations plan in place
- 46% said they don't have, or are not aware of having, controlled emergency network shutdown procedures
- 40% said they don't have, or are not aware of having, the in-house capability to prevent and detect cybercrime.

Keeping an eye on social media sites

60% of respondents said their organisation doesn't monitor the use of social media sites, or they are not aware of any monitoring policies. This is startling, given these sites can present significant security risks if employees and hackers abuse them.

Social media sites like Facebook, Twitter and LinkedIn might not be the real source of cybercrime, but criminals can use them to social-engineer cybercrime more effectively (phishing attacks). For example, they can use them to collect information on a target (also known as 'spear phishing'), research members of staff, or install malware on the target's computer, all very easily.

Of those respondents who said their organisation is taking measures to prevent the risks, 85% said they monitor internal and external electronic traffic including web pages. 62% said their employee contracts cover how to use information and documents properly, and 37% said they run training programmes.

6. http://www.bbc.co.uk/news/technology-15520912
http://www.guardian.co.uk/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal?INTCMP=ILCNETTXT3487

This suggests that those who are taking steps are doing it right, but the majority are exposed to threats like reputational damage and the loss of sensitive information by not having the right controls in place.

Our survey results suggest that the typical internal cybercrime fraudster is:

- a junior employee or a middle manager (84%)
- less than 40 years old (65%)
- employed with the organisation for less than five years (51%).

The younger generation typically uses social media a lot, and there is considerable peer and social pressure to share information with others. So not monitoring these sites might create potential cybercrime issues for organisations. But we should remember that this generation grew up with social media sites – sharing personal information has become the norm for them and they might have a very different understanding of the risks these sites pose. As a result, organisations need to make their staff aware of the risks that cybercrime presents.

Reducing the risks

Given that people think cybercrime is on the rise, it's worrying to learn that 42% of respondents had not had any cyber security training in the last 12 months – which would suggest that they're potentially unaware of the risks that cybercrime presents to their organisation.

We asked people what training, if any, they had received. Only 1 in 4 respondents had received face-to-face training. 22% had received computer-based training, and 40% had just received emails or seen posters (see figure 4).

It's not surprising there is so little face-to-face training, as it is generally time consuming and more costly to run. Most organisations have made cutbacks over the last 12 months, and training budgets are likely to have fallen victim. But 60% of respondents said face-to-face training is the most effective form when it comes to cybercrime awareness (see figure 5).

Figure 4: Cybercrime training received in the last 12 months

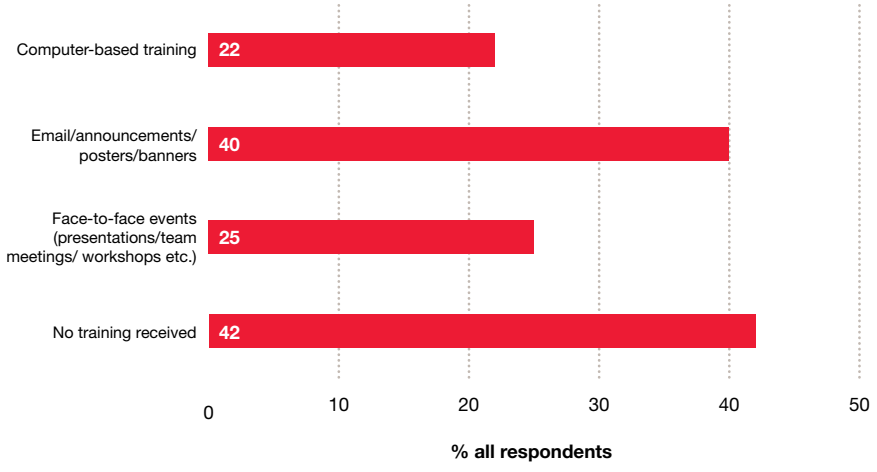
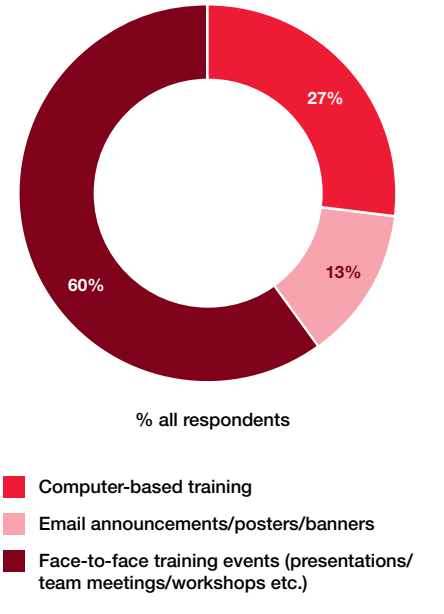


Figure 5: Most effective type of cybercrime training perceived



A quarter of respondents said there is no regular formal review of cybercrime threats by the CEO and the Board

Who is ultimately responsible for dealing with cybercrime inside an organisation?

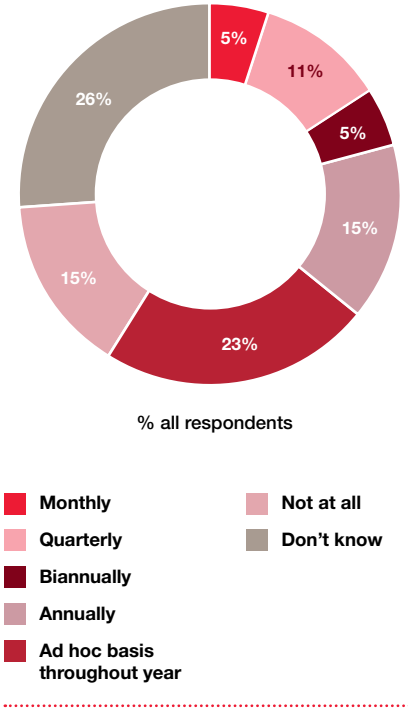
People continue to pigeonhole cyber security as an IT issue, which means there is little communication between business managers and security professionals. Awareness is now growing that cyber security is actually a core business issue. Information security's strategic value is now more closely aligned with the business than with IT[7], – more Chief Information Security Officers ('CISO's) now report to the Chief Executive Officer ('CEO') than to the Chief Information Officer ('CIO').

We asked organisations who should ultimately be responsible for dealing with cybercrime threats. 54% of respondents named the CIO or Technology Director but only 21% went for the CEO or the Board. Whilst it is clear that the CIO is usually responsible for IT security risks, we believe it is essential that the CEO and the Board understand cybercrime risks and probe into them on a regular basis.

So it is not surprising that, according to our survey, the CEO and the Board do not routinely review the cybercrime threats to their organisation – which we think they should do. Only 36% of respondents said the CEO and the Board review these risks at least once a year, and almost a quarter said they only review them on an ad hoc basis (see figure 6).

The statistics show that the most senior people in organisations are not placing enough emphasis on the importance of managing the cybercrime threat. We believe the CEO needs to get to grips with these threats – to become cyber-savvy. We think having a CEO who truly understands the risks and opportunities of the cyber world will be a defining characteristic of organisations, whether public or private sector, in the future.

Figure 6: Review of cybercrime risks by the CEO and the Board



7. See PwC's Global State of Information Security Survey 2011

What actions should organisations take to defend themselves against cyber security attacks?

- Get the CEO involved – the CEO and the Board need to be aware of the risks and opportunities of the cyber world.
- Look at how prepared the organisation is for cybercrime – unlike traditional economic crime, cybercrime is fast-paced and new risks emerge all the time, which means the organisation needs to adapt its procedures continually to reflect these.
- Be aware of the current and emerging cyber environment (Situational Awareness) – only then can the organisation make well-informed decisions and do the right things at the right times.
- Set up a cyber incident response team that can act and adapt quickly – the organisation can then track, risk-assess and deal with an incident as soon as it is spotted anywhere in the business.
- Recruit people with the relevant skills and experience – they can pass this knowledge on to everyone else, helping to create a 'cyber-aware' organisation that can protect itself better.
- Take a tougher and clearer stance on cybercrime – the organisation should show it means business by taking legal action against cybercriminals and announcing what it's doing about threats and incidents.

Fraud, the fraudster and the defrauded

Do organisations know what they are facing?

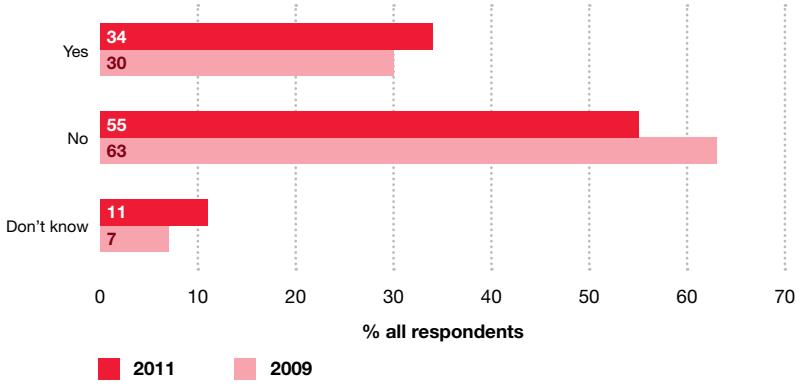
34% of the 3,877 respondents from around the world said they had experienced economic crime in the last 12 months, a 13% rise since our last survey in 2009.

It is interesting to note that 11% of respondents didn't know if their organisation had suffered any type of fraud in the last 12 months. Employees at certain levels within the organisation may not have the information to be able to answer this question. But 44% of respondents who don't know were at Senior Executive level.

While we do not expect executives at this level to know the type, significance or cost of every economic crime their organisation had been a victim of, we at least expect them to know about the more serious ones. And if they don't know, what are they doing or should be doing to find out?

In our experience, one of the best proactive measures an organisation can take is to conduct regular fraud risk assessments to detect actual incidents of economic crime. We hope that the 11% who didn't know are not taking a 'hear no evil, see no evil' approach. Ignoring the issue is really asking for trouble.

Figure 7: Experience of economic crime



What's the global picture?

Figure 8 shows that both developed and growing economies are among those experiencing either high or low levels of reported fraud.

Certain growing markets surprisingly reported low levels of fraud – namely Indonesia, India, Romania and Greece. This might be because their fraud detection methods are ineffective and/or their respondents are reluctant to report fraud.

Figure 8: Reported fraud by territory

Territories that reported high levels of fraud (40% or more)	% respondents 2011	% respondents 2009
Kenya	66%	57%
South Africa	60%	62%
UK	51%	43%
New Zealand	50%	42%
Spain	47%	35%
Australia	47%	40%
Argentina	46%	39%
France	46%	29%
USA	45%	35%
Malaysia	44%	28%
Mexico	40%	51%

Territories that reported low levels of fraud (below 25%)	% respondents 2011	% respondents 2009
Romania	24%	16%
India	24%	18%
Sweden	22%	19%
Slovakia	21%	29%
Turkey	20%	15%
Switzerland	18%	17%
Netherlands	17%	15%
Italy	17%	19%
Greece	17%	23%
Slovenia	17%	(didn't participate in 2009)
Indonesia	16%	18%
Japan	6%	10%

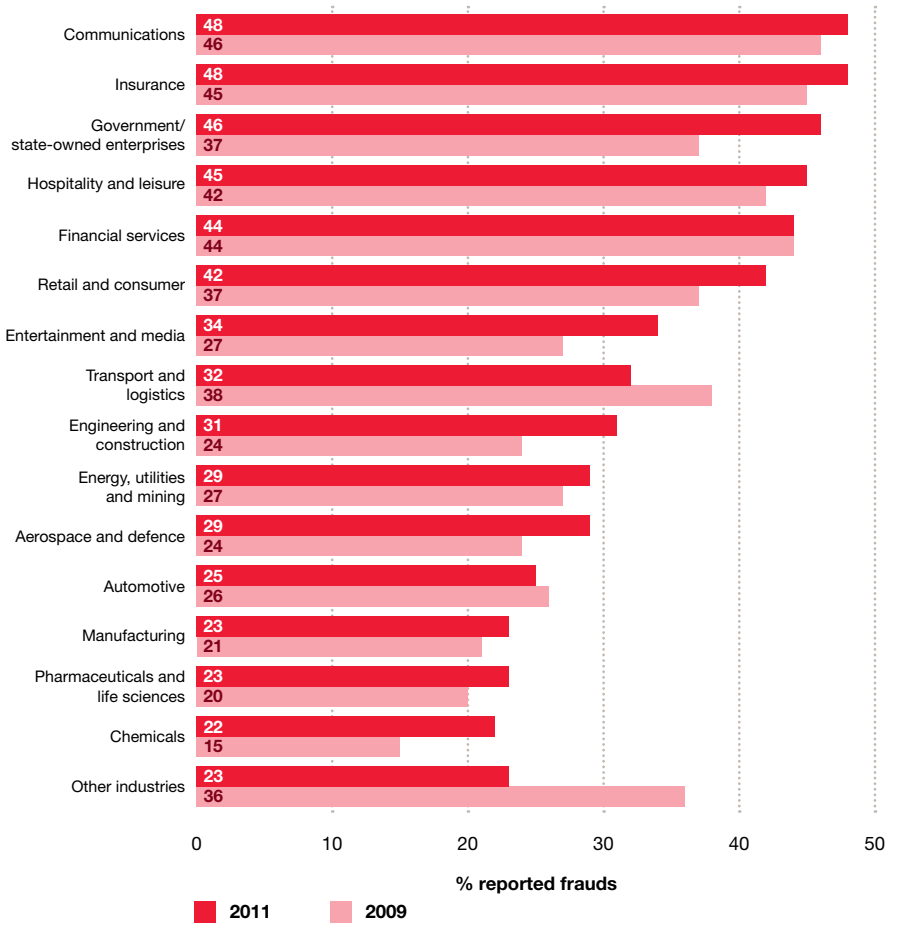
Is any particular sector experiencing high levels of fraud?

No industry sector is immune to economic crime, but the communications and insurance sectors top the table of reported frauds.

Compared with the 2009 figures, we see that fraud in the government sector has increased by 24%, now making it one of the top five targets for economic crime.

As in our previous surveys, we have found that highly regulated industries, such as financial services, typically report more economic crime. Their procedures and systems require greater levels of transparency, which increase the likelihood of detecting incidents of fraud. Industries such as construction, where there are fewer regulatory pressures, are more prone to economic crime. We have found that control and detection mechanisms are often less sophisticated as well. Furthermore, some industries may accept fraud losses as inevitable and therefore neglect the risks.

Figure 9: Fraud reported by industries



% respondents representing individual industry sectors

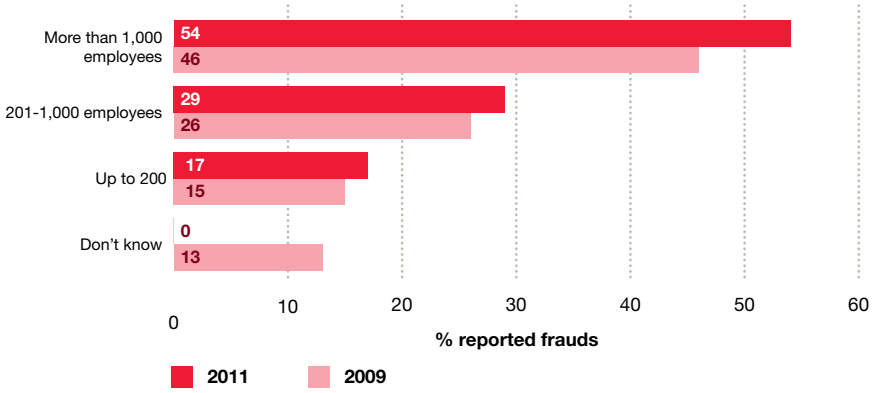
Big or small – any organisation is a target

Which types of organisation are falling victim to fraud?

There is an important correlation between the size of an organisation, measured by how many employees it has, and the likelihood of experiencing economic crime. Figure 10 suggests that there's a trend for larger organisations to experience more fraud. 54% of the respondents who experienced economic crime were from organisations with more than 1,000 employees. But fraud committed against smaller and medium organisations is on the rise as well, suggesting that fraudsters are now targeting these organisations more often.

Larger organisations are more likely to suffer fraud because they have got more employees and more assets, deal with more vendors, and operate in more countries. But they might also be more successful in identifying fraud as they tend to dedicate more resources and staff to detecting and preventing it.

Figure 10: Reported frauds based on the size of organisation



% respondents representing different sizes of organisations

So what types of economic crime are we talking about?

Economic crimes can take on many different forms, with some being more common and more persistent than others. Figure 11 shows the different types of economic crime experienced by those respondents who said they had experienced fraud in the last 12 months.

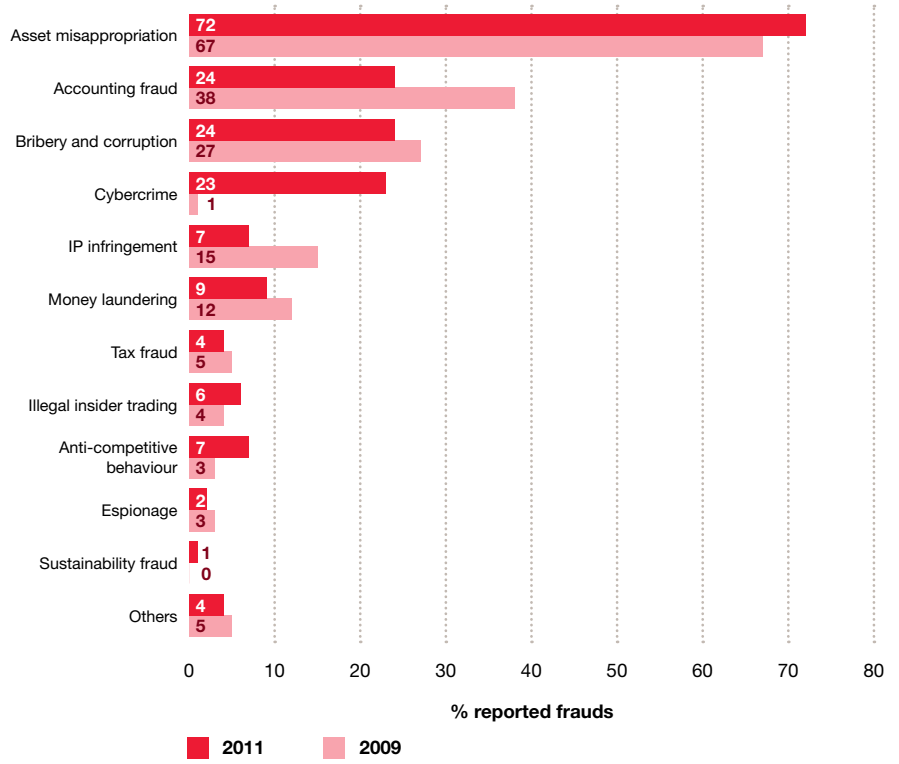
The top three economic crimes were asset misappropriation, accounting fraud and bribery and corruption. Interestingly, the 2011 survey brings us a 'new kid on the block': cybercrime.[8]

Anti-competitive behaviour has more than doubled since 2009, the second largest increase in types of economic crime after cybercrime. This is perhaps owing to the challenging economic environment in which organisations struggle to retain market share. It is therefore surprising that only 1 in 4 organisations engage in the proactive detection of anti-competitive behaviour. "Tone from the top" and a "Risk based competition compliance framework", including: clear policies, whistle-blowing, staff training, review of relationships with competitors and targeted Internal Audit reviews, are key in managing anti-competitive risks.

Another form of economic crime that has emerged this year is sustainability fraud. With increased regulation and public awareness in relation to climate change and sustainability, we anticipate a rise in sustainability fraud over the next two years.

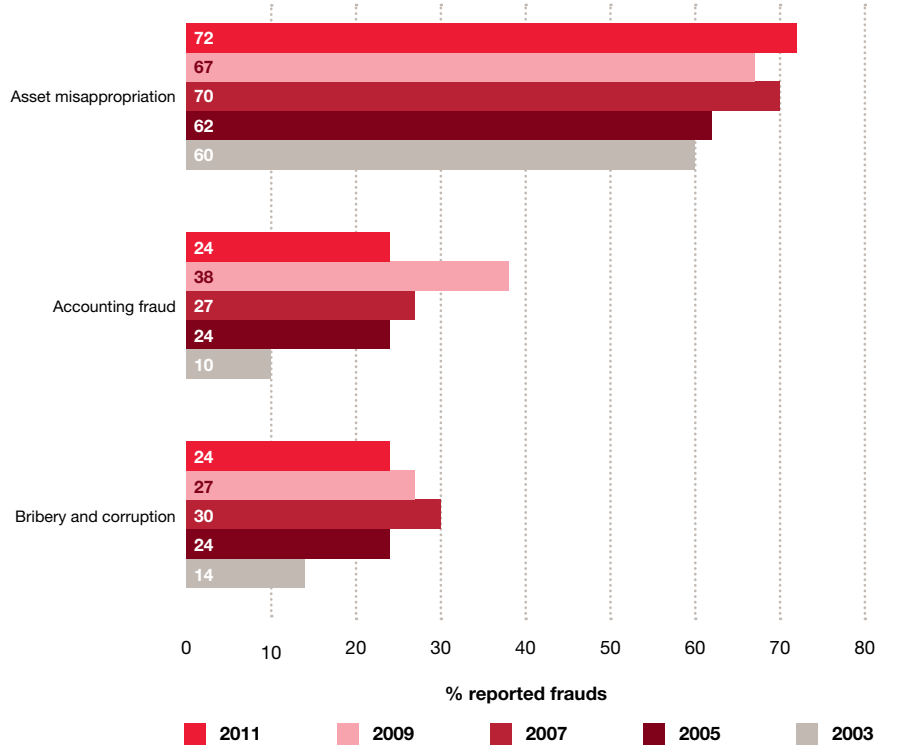
We also see in figure 12 that not only has asset misappropriation been the most common type of economic crime over the years, it has also steadily gone up – a 20% increase since 2003. The sectors reporting the most asset misappropriation were hospitality and leisure (85%), retail and consumer (79%), communications (78%), insurance (76%) and engineering and construction (76%).

Figure 11: Types of economic crime



% respondents who experienced economic crime in the last 12 months

Figure 12: Trends in reported frauds



% respondents who experienced economic crime in the last 12 months for 2011 and 2009; and in the last two years for 2007, 2005 and 2003

8. In our previous economic crime surveys, when we asked respondents if they had experienced cybercrime, the response levels were very low and statistically insignificant. Hence, we combined the results with 'other types of fraud'. Given the increasing concerns around cybercrime, we focussed on cybercrime this year and reintroduced it in the types of fraud question, asking the respondents whether they had experienced cybercrime in the last 12 months. Sustainability fraud has also been included for the first time as a fraud category in this year's survey. Please refer to the terminology section at the end of the report for a definition.

Almost 1 in 5 victims of bribery and corruption lost more than US$5m

This year's survey shows there has been a steep drop in accounting frauds since 2009. The number of respondents reporting accounting fraud is 37% less than in 2009 and has returned to 2005 levels. There could be various reasons for this, but some of the things we think could have had an impact are:

- Organisations have put tighter controls in place, which deter the perpetrator.
- More attention from the regulators and tougher punishments like prison sentences appear to be working as a deterrent.
- In our 2009 survey, we saw a sharp rise in accounting frauds. Some statistics suggested that this could have been the result of organisations struggling to survive in difficult times and management feeling the pressure to manipulate financial statements. It may be that there is less incentive and/or pressure prevalent today.
- Organisations might not be detecting economic crime. Headcounts around the world have gone down over the past couple of years. So departments responsible for detecting and preventing economic crime now have fewer resources. For example, if an internal audit department has fewer people, the chances of identifying fraud will be reduced. And if fewer incidents of accounting fraud are detected, fewer are reported.
- Given the focus of our survey on cybercrime this year, some respondents might have classified accounting frauds involving the use of computers and the internet as cybercrimes instead. As we mentioned earlier in the cybercrime section, people interpret the definition of it in different ways.

A quarter of those who said they had experienced economic crime suffered from bribery and corruption. The most affected sectors were energy, utilities and mining (40%), engineering and construction (35%) and communications (34%).

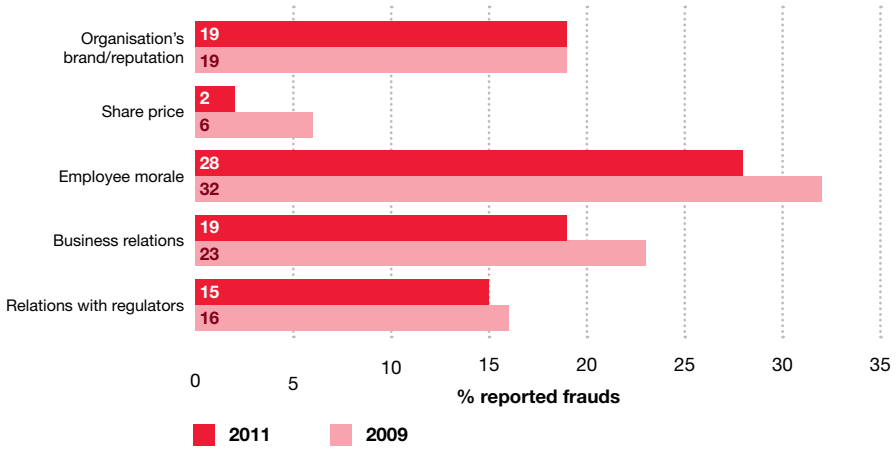
Despite the increase in anti-bribery laws and regulations globally, organisations are still falling victim to this type of economic crime. Business integrity is fundamental to the success of any organisation. Around the world, organisations are increasingly being held to account not only for what they achieve, both technically and financially, but also for how they achieve it. Bribery, wherever it occurs, can fatally undermine that achievement, creating huge financial and regulatory risk for the organisations involved. Organisations must understand and document the bribery risks they face and take appropriate steps to address them.

How much does fraud cost, and what's the collateral damage?

Almost 1 in 10 of those respondents who said they had experienced economic crime in the last 12 months reported losses of more than US$5 million. The direct cost reported by those who had been victims of bribery and corruption was much higher – almost 1 in 5 of them lost more than US$5 million on average.

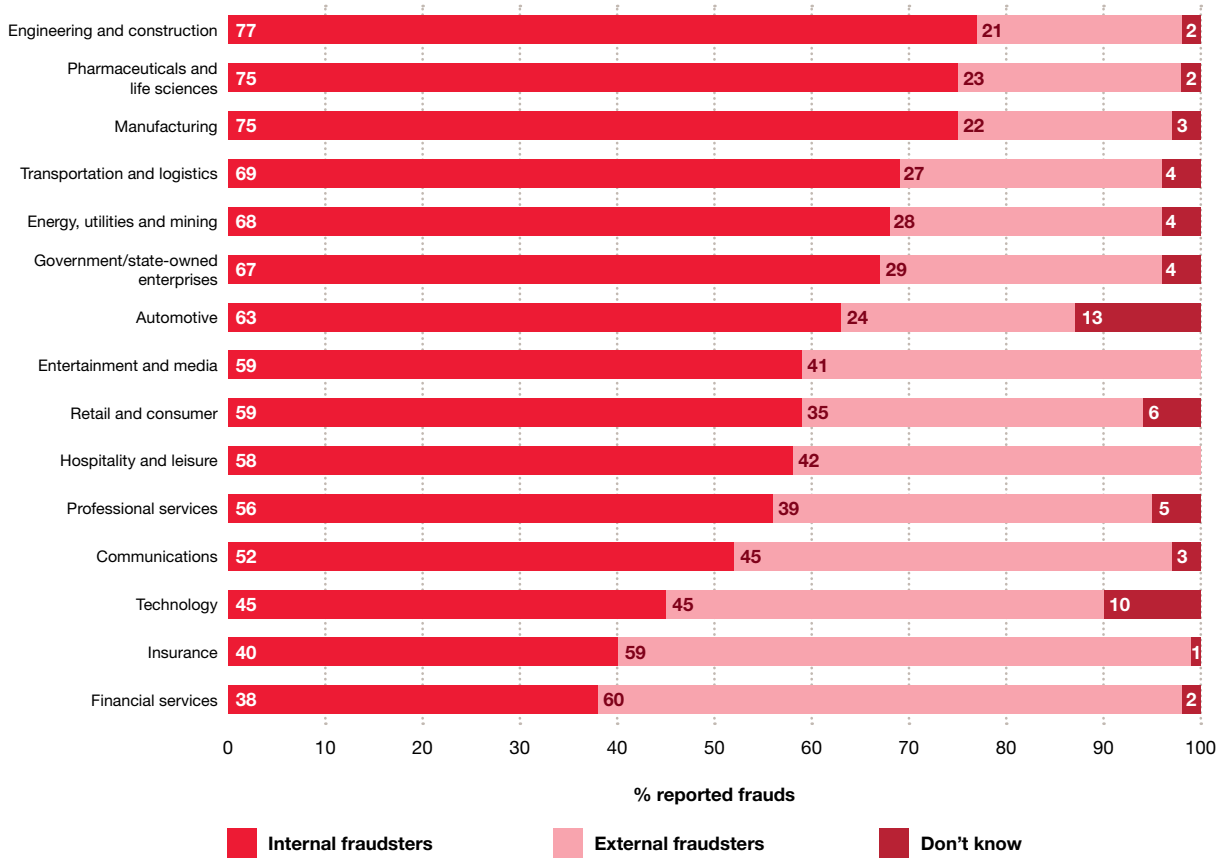
We also asked organisations about the collateral damage they had suffered and what impact economic crime had had on their reputation/brand, share price, employee morale, business relations, and relations with regulators (see figure 13). Of those who had experienced economic crime, 28% reported damage to employee morale, 19% damage to reputation/brand and another 19% to business relations.

Figure 13: Collateral damage



% respondents who experienced economic crime in the last 12 months

Figure 14: Perpetrators of fraud – by industry



% respondents representing individual industry sectors

Who's committing this fraud?

As the amount of fraud increases, organisations can no longer just fight it reactively. They need to be more proactive when it comes to protecting themselves.

One aspect of this is gathering as much information as possible about the perpetrators. Knowing who they are and where they come from is essential for finding out where the weaknesses are in an organisation's response mechanisms and internal controls.

We asked those respondents who said they had experienced economic crime in the last 12 months to profile the main perpetrator of the most serious fraud. 56% said it was an internal fraudster, and 40% said it was an external fraudster.

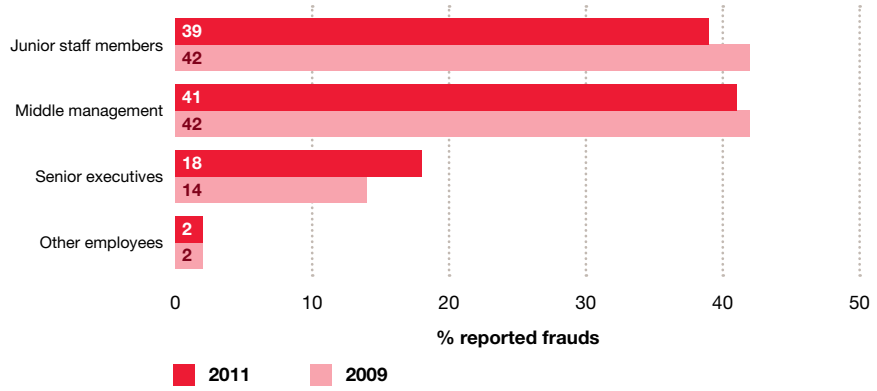
But the financial services and insurance sectors stood out, with the main perpetrator usually coming from outside the organisation. This is typical in the financial services and insurance sectors, so it wasn't a surprise here.

The profile of the internal fraudster

Given there are more 'inside jobs' than 'outside jobs', organisations need to improve internal controls and be more aware of fraudster profiles so they can do something about it. This is clear from the fact that 1 in 10 respondents who had been the victim of an economic crime carried out by an internal fraudster didn't know how long the perpetrator had been working in the organisation.

Figure 15 shows the profile of the internal fraudster, according to our survey.

Figure 15: Profile of internal fraudsters



% respondents who reported that an internal employee was the main perpetrator of fraud

The profile of the external fraudster

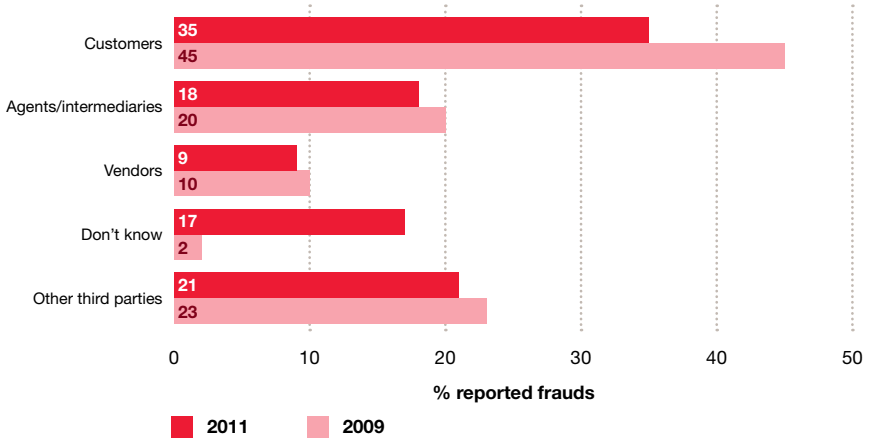
The number of frauds carried out by customers has dropped significantly and there has been a sharp rise in the number of 'don't knows' (see figure 16).

Whilst it may be difficult to collect information on an external fraudster, those organisations who conduct a thorough investigation stand a better chance of identifying the perpetrator.

The most common economic crimes carried out by an unknown party were cybercrime, asset misappropriation and accounting fraud. The perpetrators of cybercrime could be ingenious organised criminals who can protect their identity, however the fact that organisations don't know who carried out so much accounting fraud and asset misappropriation suggests that detection controls are not working, in particular when dealing with external perpetrators.

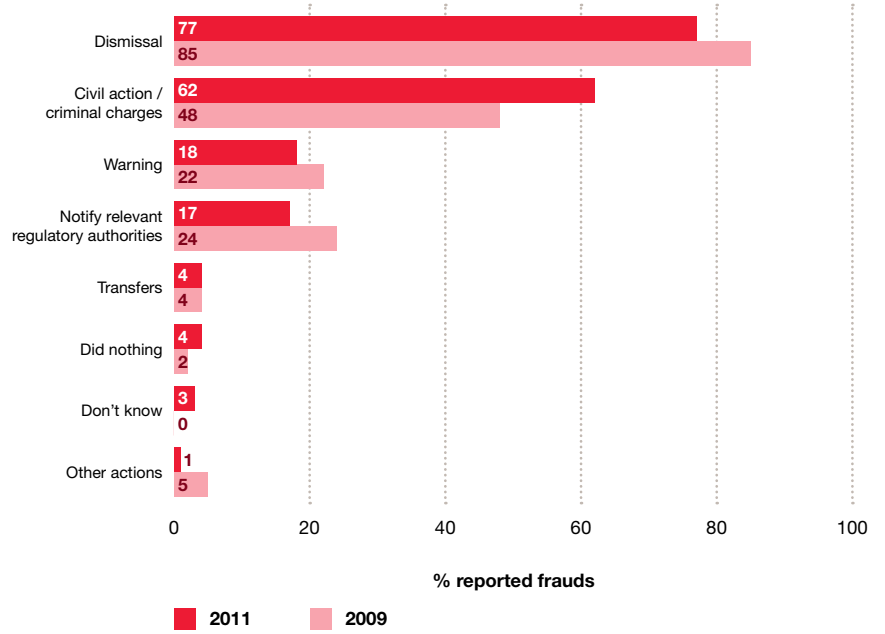
One of the best ways to prevent fraud is to know who you are doing business with – your customers, your vendors, your agents. It has long been recognised that 'fraud flees from sunlight', so transparency programmes, such as 'know your business associates' remain one of the more effective preventative tools available to organisations.

Figure 16: Profile of external fraudsters



% respondents who reported that an external party was the main perpetrator of fraud

Figure 17: Actions brought against internal fraudsters



% respondents who experienced economic crime in the last 12 months

61% of respondents said their organisation still has a business relationship with the fraudster

61%

What do organisations do with the fraudster?

If an organisation catches the perpetrator, they can deal with them in several ways.

For an 'inside job', 77% of respondents said their organisation fired the individual, 44% said they told the police, and 40% said they took civil action[9]. These are obviously hard line approaches.

But it's perhaps worrying that, for the most serious fraud carried out by an employee, 4% said their organisation did nothing, 4% said it moved the individual to somewhere else in the organisation, and 18% said it just gave them a warning.

So in some organisations there seems to be complacency or a wish to deal with fraud in a low-key way. We question this. Is it right to keep the fraudster in the organisation and run the risk that they might do it again?

We think organisations should show 'zero tolerance' towards fraud and set the right tone, by dealing with the fraudster officially and by involving outside authorities.

For an 'outside job', 63% of respondents said their organisation told the police, 43% said they took civil action, and 40% said they told the relevant regulatory authorities.

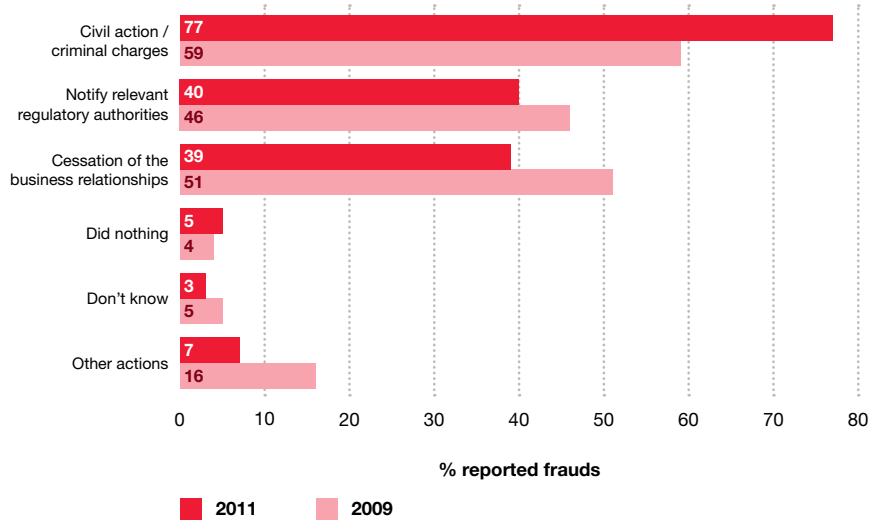
Although many organisations took a firm approach, 61% said their organisation still has a business relationship with the fraudster – this is worrying, and perhaps highlights some fundamental concerns about the culture of these organisations. Of course, the victim might have 'worked it out' with the fraudster and been able to carry on the relationship. And if the crime was hacking the network, there isn't a relationship to end in any case.

How do organisations detect economic crime?

Organisations use many methods to find out if a fraud has been committed. These methods fall into one of three groups:

- 'corporate controls' like internal auditing, fraud risk management, electronic and automated suspicious transaction monitoring, corporate security and moving people around
- 'corporate culture' like internal tip-offs, external tip-offs and whistle-blowing
- 'beyond the influence of management' – finding out by accident or through the media, for example.

Figure 18: Actions brought against external fraudsters



% respondents who experienced economic crime in the last 12 months

9. For this question, respondents were able to select more than one action taken against the perpetrator.

Figure 19 shows that the effectiveness of internal audits to detect fraud has steadily gone down since 2005. Only 14% of respondents said frauds were detected by internal audit. Likewise, fraud risk management didn't prove as effective as in 2009, slipping from 14% to 10%.

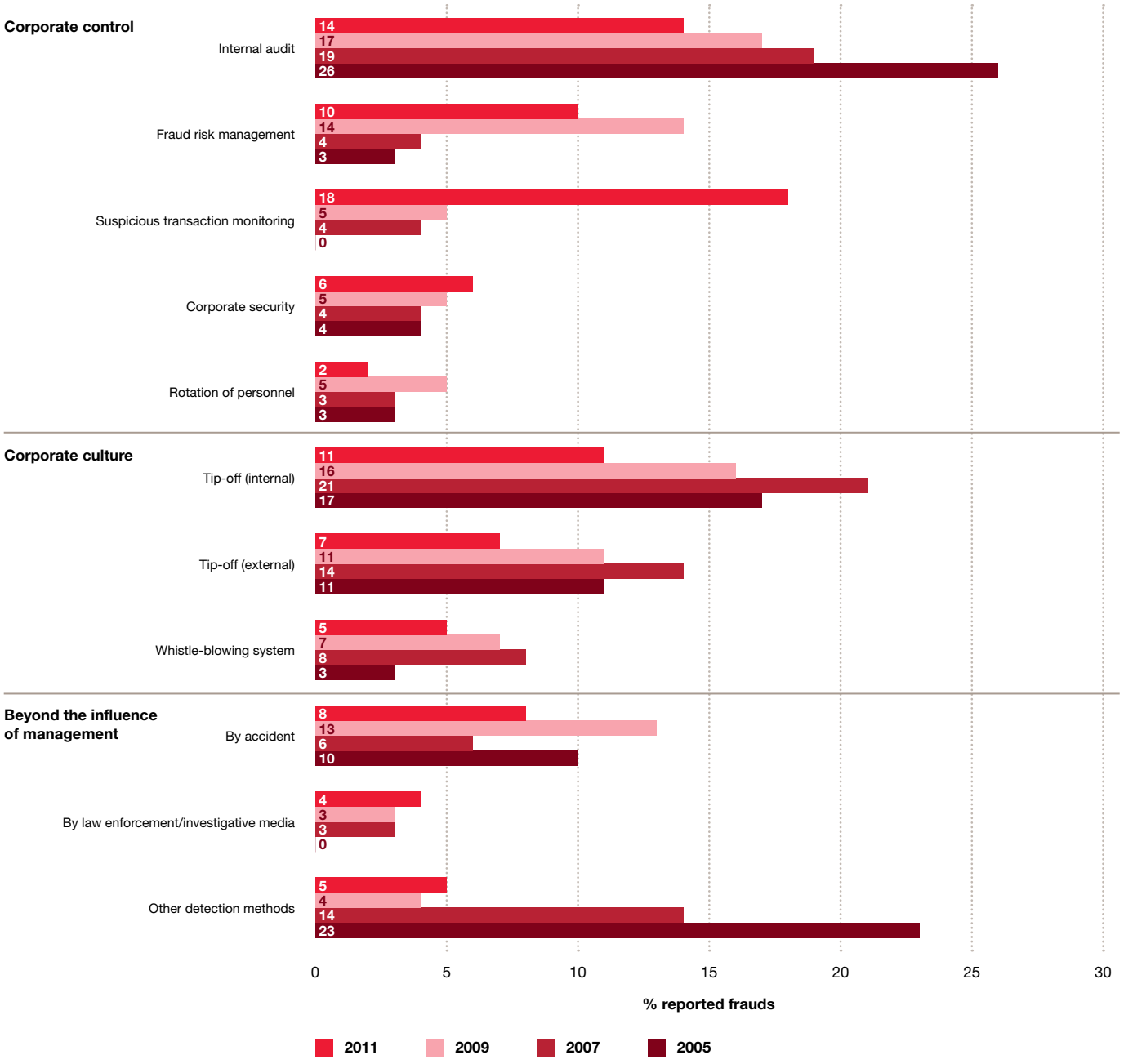
It is interesting that the effectiveness of 'corporate culture' methods has also been on the decline since 2007. External and internal tip-offs have fallen markedly from a peak in 2007 as shown in Figure 19, suggesting either that people are less willing to inform on their colleagues and customers, or that the different business units are not talking to each other or acting on the information they get. It must be the case that there has been more reliance on suspicious transaction monitoring.

The only detection method for which effectiveness has increased is 'suspicious transaction monitoring', up from 5% in 2009 to 18% in 2011. This electronic method automatically detects irregularities and suspicious transactions, and is commonly used in the financial services sector.

Because the number of economic crimes detected by computers is going up, but the number detected by people is going down, we fear more fraud overall will go undetected, as headcounts fall in control functions across the different industries.

It is surprising to learn that in this year's survey 10% of respondents didn't know how their most serious fraud was detected. This further highlights the need for Senior executives to be fully aware of the fraud risks and their organisation's detection and prevention measures.

Figure 19: Detection methods



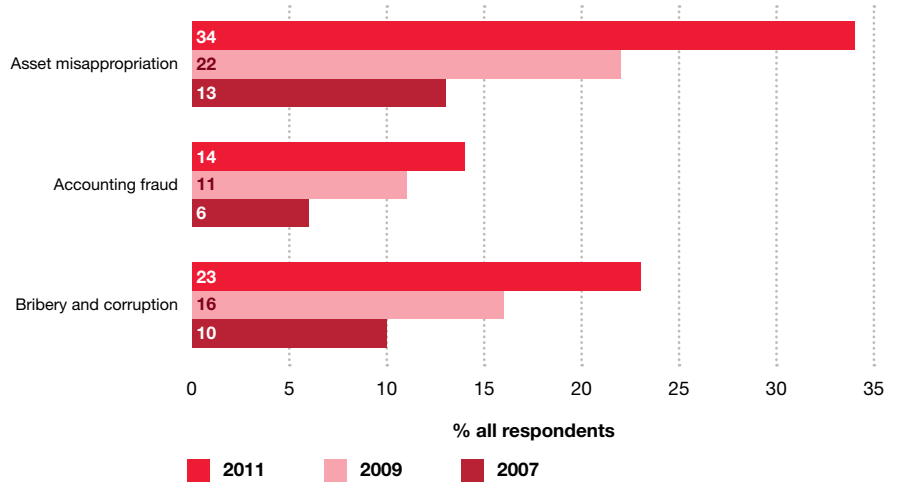
% respondents who experienced economic crime in the last 12 months for 2011 and 2009; and in the last two years for 2007 and 2005.

And organisations see more fraud ahead

People perceive the three most common types of fraud to be on the increase: 34% of all respondents believe their organisation is likely to fall victim to asset misappropriation in the next 12 months, 14% believe their organisation may suffer accounting fraud, and 23% bribery and corruption (see figure 20). This is consistent with the overall greater level of fraud risk.

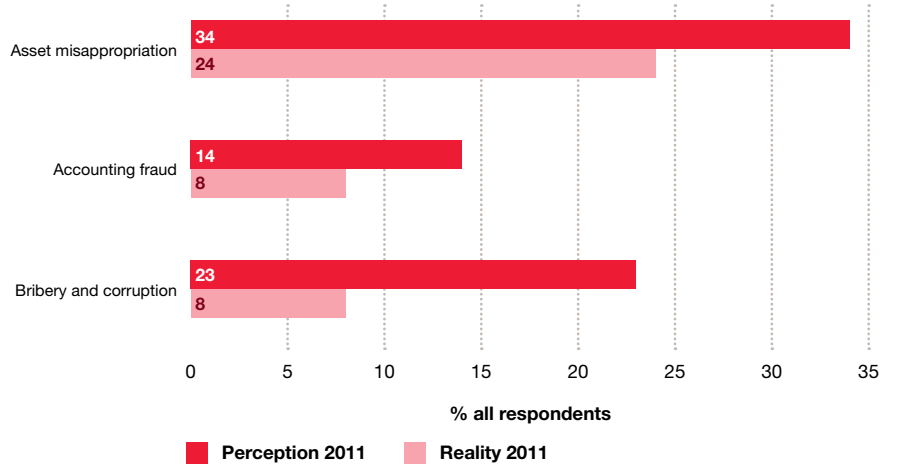
When we look at actual occurrence of fraud versus perception of economic crime in the future, our respondents expect to see more frauds in the next 12 months. In figure 21 we can see that if the perception is accurate then we expect to see more respondents suffering from economic crime in the future.

Figure 20: Trends in fraud perception



% all respondents' perception over the next 12 months for 2011 and 2009; and over the next two years in the 2007 survey

Figure 21: Perception versus reality



% all respondents' perception over the next 12 months; and % types of economic crime reported over all respondents

How fraud risk assessments can really help organisations

The best way to fight fraud is to know how to assess and identify the risks. Organisations can find this out by doing regular fraud risk assessments. Our survey finds that there is a clear correlation between how often these assessments are done and how many frauds are reported. The fewer fraud risk assessments organisations carry out, the less fraud they are likely to detect.

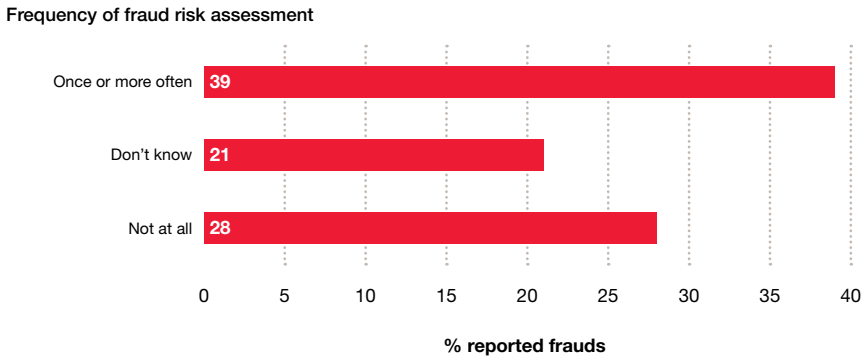
For example, more than three-quarters of the organisations that said they don't do any fraud risk assessments reported less than ten incidents of fraud. These figures confirm the dictum of 'seek and you shall find'.

Figure 22 indicates that of the total number of respondents who had performed a fraud risk assessment once or more often in the last 12 months 39% identified fraud. In comparison, of those respondents who had not performed a fraud risk assessment in the last 12 months, 28% identified fraud.

41% of respondents said either they don't do fraud risk assessments or didn't know if they do. Of those who said they don't do them, 1 in 2 said they don't know what one is or what it involves.

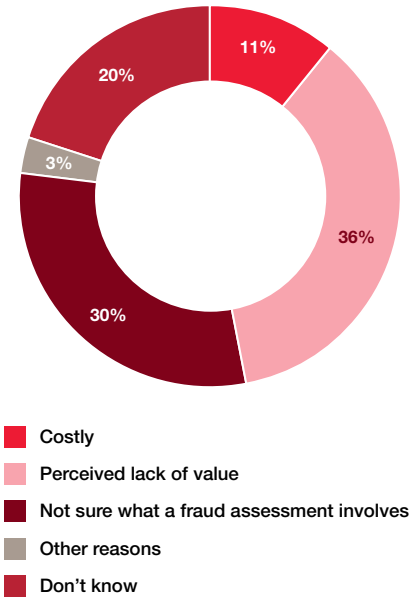
Figure 23 suggests that there is an awareness problem. Organisations need to understand the benefits of doing regular fraud risk assessments and how important they are in the fight against fraud.

Figure 22: Percentage of reported frauds in the last 12 months in relation to the frequency of fraud risk assessments



% respondents who experienced economic crime in the last 12 months

Figure 23: Reasons for not carrying out fraud risk assessments



Conclusion

It's time for everyone to rise to the challenge

Our survey results show that fraud is persistent, and that organisations need to be vigilant and proactive when fighting economic crime.

'Traditional' frauds like asset misappropriation, accounting fraud and bribery and corruption remain the top three that our respondents fell victim to in the last 12 months. But 'new' types of fraud are emerging – cybercrime in particular. With new ways of doing business, new technologies and changing work environments, come new risks and new ways for fraudsters to carry out crimes. Organisations need to be aware of these changes and adapt their response mechanisms and detection methods accordingly.

This is even more true when it comes to new technologies. Smart phones and tablet devices, social media and cloud computing all offer a wealth of attractive business solutions and opportunities, but they can also be a Pandora's box of risks and dangers. Having a smart phone or a tablet device means carrying around your organisation's sensitive and confidential data in your pocket which without precautions in place, anyone might be able to access sensitive and confidential information and cause considerable harm, both financial and collateral.

A decade on and the fraud risk continues to rise. Despite the effectiveness of risk management systems being deployed, there are always individuals or groups of individuals who are able to spot an opportunity and circumvent or override controls. This is especially true when it comes to cyber security. As headcounts fall in control functions across the globe, we fear more fraud will go undetected.

Advances in technology are fast-paced, as are fraudsters, however organisations are often far behind. It is now essential to ensure that cyber and information security issues have the standing they warrant on an organisation's risk register. Those organisations ready to understand and embrace the risks and opportunities of the cyber world, will be the ones to gain competitive advantage in today's technology driven environment. Establishing the right "tone at the top" is key in the fight against economic crime.

Methodology and acknowledgments

We carried out our sixth Global Economic Crime Survey between June 2011 and November 2011. The survey had three sections:

- *general profiling questions*
- *comparative questions looking at what economic crime organisations had experienced*
- *this year's special topic, cybercrime.*

About the survey

The 2011 Global Economic Crime Survey was completed by 3,877 respondents (compared to 3,037 respondents in 2009) from 78 countries (compared to 54 countries in 2009). Of the total number of respondents, 52% were Senior executives of their respective organisations, 36% represented listed companies and 38% represented organisations with more than 1,000 employees.

We used the following research techniques:

1. Survey of executives in the organisation. The findings in this survey come from executives' reports of their experiences of economic crimes in their organisations. We obtained information from them on the different types of economic crime, their impact on the organisation (both the financial loss and any collateral damage), the perpetrator of these crimes, what action the organisation took and how they responded to the crime.
2. Questions relating to cybercrime. This survey takes a detailed look at the growing threat of cybercrime, and how vulnerable organisations are to it. This focus enables us understand what cybercrime really means for organisations.
3. Analysis of trends over time. Since we started doing these surveys in 2001, we have asked a number of core questions, and extra ones that are relevant from time to time, dealing with issues likely to have an impact on organisations around the world. With this historical data to hand, we can see current themes, chart developments, and find trends.

Figure 25: Participating territory counts

	2011	2009
Asia Pacific	**796**	**652**
Australia	79	75
Hong Kong (and China)	22	67
India	106	145
Indonesia	84	50
Japan	73	73
Malaysia	93	65
Middle East Countries*	127	14
New Zealand	93	85
Papua New Guinea	1	0
Philippines	0	1
Singapore	18	51
South Korea	0	1
Taiwan	2	0
Thailand	79	25
Vietnam	19	0

	2011	2009
Africa	**260**	**145**
Angola	1	0
Botswana	1	0
Ghana	29	27
Kenya	91	53
Liberia	5	0
Namibia	2	1
Nigeria	3	0
Sierra Leone	0	1
South Africa	123	63
Sudan	1	0
Swaziland	1	0
Tunisia	2	0
Zambia	1	0

	2011	2009
South and Central America	**483**	**275**
Argentina	77	39
Bolivia	3	0
Brazil	115	62
Chile	1	76
Colombia	1	0
Dominican Republic	0	1
Ecuador	11	1
Mexico	174	94
Peru	17	1
Venezuela	84	1

	2011	2009
North America	**209**	**123**
Canada	53	52
USA	156	71

	2011	2009
Western Europe	**1,317**	**1,243**
Andorra	1	0
Austria	8	34
Belgium	84	62
Cyprus	5	1
Denmark	116	105
Finland	61	52
France	112	52
Germany	38	17
Greece	92	96
Ireland	80	91
Italy	127	90
Luxembourg	3	0
Netherlands	41	76
Norway	67	75
Portugal	0	1
Spain	85	55
Sweden	79	78
Switzerland	140	129
UK	178	229

	2011	2009
Central and Eastern Europe	**804**	**589**
Bulgaria	58	59
Croatia	1	0
Czech Republic	84	83
Estonia	1	0
Hungary	85	53
Lithuania	7	0
Moldavia	1	0
Montenegro	1	0
Poland	79	63
Romania	76	55
Russia	126	86
Serbia	14	4
Slovakia	84	69
Slovenia	48	0
Turkey	55	52
Ukraine	84	65

No primary country specified	**8**	**10**

TOTAL	**3,877**	**3,037**

*Middle East countries included participants from Jordan, Kingdom of Saudi Arabia, United Arab Emirates, Lebanon, Iraq, Kuwait, Bahrain, Qatar and Sultanate of Oman.

Figure 26: Participating industry groups

	% respondents	
	2011	2009
Aerospace and defence	1%	1%
Automotive	4%	4%
Chemicals	2%	2%
Communications	3%	2%
Education	1%	0%
Energy, utilities and mining	7%	7%
Engineering and construction	5%	7%
Entertainment and media	3%	3%
Financial services	18%	16%
Food related	1%	0%
Government/state-owned enterprises	5%	6%
Health and care	1%	0%
Hospitality and leisure	2%	2%
Insurance	5%	5%
Manufacturing	12%	14%
Pharmaceuticals and life sciences	5%	5%
Professional services	6%	6%
Property	1%	0%
Retail and consumer	8%	9%
Technology	5%	5%
Transportation and logistics	4%	5%
Other industries	1%	1%

Figure 27: Organisation types participating

	% respondents	
	2011	2009
Private	51%	42%
Listed on a stock exchange	36%	43%
Government/state-owned enterprises	10%	10%
Others including cooperative/ non-profit organisations	3%	5%

Figure 28: Size of participating organisations

	% respondents	
	2011	2009
Up to 200 employees	32%	32%
201 to 1,000 employees	29%	33%
More than 1,000 employees	38%	34%
Don't know	1%	1%

Figure 29: Function (main responsibility) of participants in the organisation

	% respondents	
	2011	2009
Executive management or finance	46%	58%
Audit	16%	12%
Risk management	6%	5%
Compliance	5%	4%
Security	4%	4%
Legal	4%	3%
Information technology	4%	0%
Advisory/consultancy	3%	3%
Operations and production	3%	3%
Marketing and sales	2%	0%
Human resources	1%	0%
Tax	1%	0%
Customer service	1%	0%
Research and Development	1%	0%
Procurement	1%	0%
Others	2%	8%

Figure 30: Job title of participants in the organisation

	% respondents	
	2011	2009
Senior executives	**52%**	**52%**
Chief Executive Officer/President/ Managing Director	10%	12%
Chief Financial Officer/Treasurer	23%	30%
Chief Operating Officer	2%	2%
Chief Information Officer/ Technology Director/ Chief Security Officer	3%	1%
Other Senior executives	10%	4%
Board member	4%	3%
Non-senior executives	**48%**	**48%**
Senior Vice President/ Vice President/Director	8%	8%
Head of Business Unit	7%	3%
Head of Department	15%	15%
Manager	17%	15%
Others	1%	7%

Terminology

Due to the diverse descriptions of individual types of economic crime in countries' legal statutes, we developed the following categories for the purpose of this survey. These descriptions were defined as such in our web survey questionnaire.

Accounting fraud

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

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.

Asset misappropriation (including embezzlement/ deception by employees)

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

Corruption and bribery (including racketeering and extortion)

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

Cybercrime

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

Cybercrime incident response

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.

Financial losses

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

Financial performance

This can be defined as measuring the results of an organisation's policies and operations in monetary terms. These results are reflected in return on investment, return on assets and value added; typically, in the private sector, returns will be measured in terms of revenue; in the government/state-owned enterprises, returns will be measured in terms of service delivery.

Fraud risk assessment

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

i. The fraud risks to which operations are exposed.

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

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

iv. Assessment of the general anti-fraud programmes and controls in an organisation.

v. Actions to remedy any gaps in the controls.

Hacking

This refers to unauthorized attempts to bypass the security mechanisms of an information system or network.

Hacktivism

Hacktivism is the act of hacking into an information system or network for a politically or socially motivated purpose.

Insider trading

Insider trading refers generally to buying or selling 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.

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

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

Money laundering

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

Pharming

Pharming refers to the redirection of website traffic by hackers, with the aim of obtaining personal and financial information.

Phishing

This is an email fraud method in which the fraudster sends out legitimate-looking emails in an attempt to gather personal and financial information.

Senior Executive

The Senior Executive (for example the CEO, Managing Director or Executive Director) is a key decision maker in the organisation.

Situational Awareness

A term drawn from military strategy which means knowing the landscape surrounding your own position, including actual and potential threats.

Social Media

Communication channels or tools used to store, share, discuss, or deliver information within online communities.

Sustainability activities

Includes activities such as carbon credit trading (buying and selling carbon credits), 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.

Acknowledgements

The 2011 Global Economic Crime Survey team consisted of the following individuals:

Survey Leadership Team

Tony Parton, Partner, United Kingdom

Vidya Rajarao, Partner, India

Steven Skalak, Partner, USA

Wayne Anthony, Director, United Kingdom

Survey Management Team

Faisal Ahmed, Global Project Manager, United Kingdom

Zina Hunt, Global Marketing Manager, United Kingdom

Rhona Foy, Manager, United Kingdom

Editorial Team Members

William Beer, Director, United Kingdom

Mona Clayton, Partner, Brazil

Dyan Decker, Partner, USA

John Donker, Partner, Hong Kong

Peter Forwood, Senior Manager, Australia

Ed Gibson, Director, USA

Jon Hayton, Director, United Kingdom

Tom Lewis, Partner, United Kingdom

Malcolm Shackell, Partner, Australia

Louis Strydom, Partner, South Africa

Peter Vakof, Partner, Canada

John Wilkinson, Partner, Russia

Survey Academic Partner

Peter Sommer
Visiting Professor in the Department of Management (Information Systems and Innovation Group) at the London School of Economics and Political Science and a Visiting Reader, Faculty of Mathematics, Computing and Technology, Open University

www.pmsommer.net

Information Security Forum

Michael de Crespigny
Chief Executive Officer, Information Security Forum

www.securityforum.org

Particular thanks in compiling this report are also due to the following individuals at PwC: Mike Ascolese, Jonti Campbell, Arjit Chakraborti, Sarah Craig, Matthew Curry, Bonnie Fagan, Gary Fairman, Anjali Fehon, Freddy Fobian, Ayse Francis, Jack Gray, Kunal Gupta, Harry Holdstock, Jonathan Holmes, Fran Marwood, Noel McCarthy, Kim McCourt, Derek Nash, Richard Nugent, Kathrin Prietzel, Mayukh Ray, Aida Roslan, Keith Smith, Rick Stevenson, Josh Williams and Neal Ysart.

Contacts

Survey Leadership Team

Tony Parton
Partner, United Kingdom
+44 (0) 20 721 34068
tony.d.parton@uk.pwc.com

Steven Skalak
Partner, Peoples Republic of China
+86 (10) 6533 2630
steve.l.skalak@cn.pwc.com

Vidya Rajarao
Partner, India
+91 (0) 80 4079 7002
vidya.rajarao@in.pwc.com

Wayne Anthony
Director, United Kingdom
+44 (0) 20 721 26582
wayne.g.anthony@uk.pwc.com

Survey Management Team

Faisal Ahmed
Global Project Manager, United Kingdom
+44 (0) 20 780 46128
faisal.a.ahmed@uk.pwc.com

Zina Hunt
Global Marketing Manager, United Kingdom
+44 (0) 20 780 44031
zina.hunt@uk.pwc.com

Forensic Services Leaders

Chris Barbee
Partner, USA, Global Leader
+1 (267) 330 3020
chris.barbee@us.pwc.com

Andrew Palmer
Partner, United Kingdom, Central Cluster Leader
+44 (0) 20 7212 8656
andrew.palmer@uk.pwc.com

John Donker
Partner, Hong Kong, East Cluster Leader
+852 2289 2411
john.donker@hk.pwc.com

Erik Skramstad
Partner, USA, West Cluster Leader
+1 (617) 530 6156
erik.skramstad@us.pwc.com

Forensic Services

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

Design & Media – The Studio 20731 (11/11)