www.pwc.com/crimesurvey

Safeguarding organisations in India against Cyber crime

Global economic crime survey

India Report

Assess the impact of emerging cyber threats and other white collar crimes.

December 2011

pwc

Contents

Foreword

The world of business has undergone a sea change in the manner in which it is conducted and most important, where and how it is conducted. In tandem with the change in nature, form and complexity of business, the risk of economic crime or fraud has also undergone a change in the form in which fraud manifests itself and the key tools that organisations will need to identify and proactively address fraud risks.

With this background, we are delighted to present our sixth Global Economic Crime Survey India, 2011. 3,877 respondents globally and 106 respondents from India participated to complete our web based survey.

Emerging risk of cyber crime

This year, our focus was on the emerging risk of cyber crime. A shift from "brick and mortar", localised environment to an "online", globalised environment implies that cyber crime is increasingly being regarded as a significant area of vulnerability for organisations. Internet penetration in India is at an all time high and while burgeoning growth in the use of internet and social media provides multiple options to cyber citizens in all possible spheres–from entertainment to education to banking and trading, it has also given rise to cyber crime. These new breeds of tech-savvy fraudsters pose an entirely new set of challenges. In today's cyber age, economic crimes can be perpetrated by a flip of a switch and can take on gigantic proportions. Detection is time sensitive and needs to be supported by the right set of forensic technology tools. Organisations cannot afford to be complacent or act in a reactive manner to deal with the emerging threat of cyber crime.

Economic crimes, may demonstrate a predictable pattern of motives and ***modus operandi*** and hence, one can argue that prevention and proactive fraud risk management are useful tools. Questions such as which department is most vulnerable to the risk of fraud, who are the typical fraud perpetrators and what is the change in the types of fraud experienced over the years need to be addressed.

The intention of the survey has been to provide a collective snapshot of the economic crimes and their possible perpetrators. More than anything else, the focus is on making organisations aware of where such crimes are originating and creating an environment where organisations expect and know that they do not need to be "case studies" – rather learn from them!

As always, we hope that you find this survey and associated analysis useful and look forward to your views and comments.

Vidya Rajarao
Leader
Forensic Services
Bangalore, India

Kunal Gupta
Associate Director
Forensic Services
Gurgaon, India

Executive summary

Growing threat of cyber crime

Economic crime does not discriminate. It is truly global. No industry or organisation is immune. We have seen that despite fraud being a serious business issue, 10% of the respondents in 2011 as compared to 6% in 2009 were not aware if their organisation has been a victim to economic crime in the last 12 months. The reason for awareness levels being low can be attributed, to an extent, to the frequency of performing fraud risk assessment. One third of the respondents to the survey do not perform fraud risk assessment due to a perceived lack of value. This trend is exposing more organisations to the risk of fraud.

The fallout isn't just the direct costs: economic crime can seriously damage employee morale, brands or tarnish 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.

Our sixth Global Economic Crime Survey turns the spotlight on the growing threat of cyber crime. 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 report is divided into two sections:

- ***Cyber crime***
  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

Cyber crime

- *Cyber crime ranks as one of the top four types of economic crime.*
- *More than half (58%) perceive Information Technology department as a high risk department with respect to committing cyber crime.*
- *96% said that their organisations monitor internal and external electronic traffic and web-based activity.*
- *About 80% of Indian respondents reported that cyber crime threat originates within India or through a combination of in and outside the country.*
- *About 2/3rd of respondents did not have access to forensic technology tools that are useful in combating cyber crime.*
- *35% of respondents did not have any cyber security training in the last 12 months.*

Fraud, the fraudster and the defrauded

- *Asset misappropriation has not only been the most common type of economic crime but also shown a remarkable increase - 20% in 2007 to 68% in 2011.*
- *Nearly two-thirds of the respondents found that the perpetrators were among their own staff.*
- *In most cases, perpetrators of fraud were male, between the ages of 31 and 40, and educated to degree level or higher.*
- *80% of respondents said their organisation terminated the individual who committed the fraud and more than half of the respondents ceased to conduct business with outsiders who engaged in fraudulent conduct.*
- *Despite the growing confidence that organisations surveyed have in their risk management systems most fraud (35 %) is still detected by chance (e.g., through tip-offs).*

Cyber crime
The new kid on the block

For our survey questionnaire, we defined cyber crime 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 cyber crime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one.'[1]

This is a fairly standard definition of cyber crime, 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 cyber crime or both. There is currently no globally accepted definition of cyber crime. 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 cyber crime 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***[2] – terrorist groups might attack either state or private assets, often critical national infrastructure ("CNI")like power, telecoms and financial systems.
5. ***Warfare***[2] – this involves states attacking state or private sector organisations.

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

1. As defined in the Global Economic Crime Survey 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer.
2. 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.

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

- National Research Council, 'Computers at Risk'

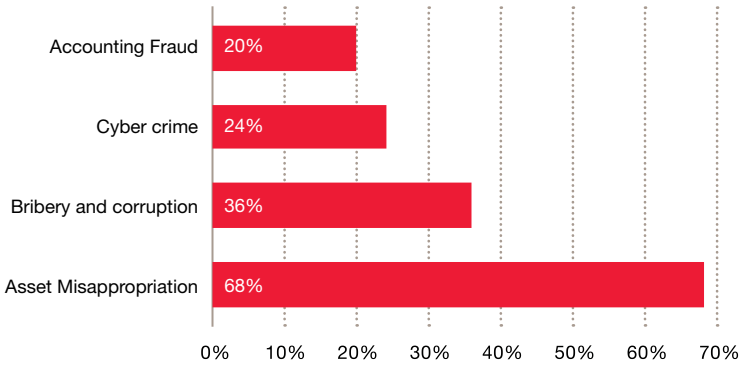
The use of the internet in India is growing rapidly. According to a recent Telecom Regulatory Authority of India (TRAI) survey, we currently have 20.33 million internet subscribers.[4]

While burgeoning growth in the use of internet provides multiple options to cyber citizens in all possible spheres– from entertainment to education, it has also given rise to cyber crime. This new breed of tech-savvy fraudsters pose a new set of challenges.

24% of the respondents who reported economic crime, have experienced cyber crime in the last 12 months. We believe that this data alone shows how serious the risk of cyber crime is to organisations.

In the background of the recent incidents of cyber crime on muti-national companies and financial institutions, we believe that a greater number of organisations are becoming victims of cyber crime. One potential reason that may explain this sudden rise in cyber crime is the rise in the volume of e-business, greater penetration of internet and e-commerce.

Figure 1: [5]
Types of economic crime experienced by respondents in the last 12 months



% respondents who experienced economic crime in the last 12 months. Respondents were able to select multiple responses.

3. http://www.crime-research.org/analytics/702/

4. http://www.trai.gov.in

5. Percentages have been rounded to the nearest number in the report.

Reasons for cyber crime emerging as one of the top four types of fraud in India

- *The increased media attention around recent cyber crime cases, leading to a heightened awareness about this type of fraud . Organisations may have installed extra controls in place to detect and therefore report more of such economic crime; or*
- *Due to ambiguity around the definition of cyber crime and what it constitutes; or*
- *The respondents may have re-classified some of the more traditional economic crimes as cyber crime because these were committed by using a computer, electronic devices or the internet; or*
- *Increased focus from the regulators; or*
- *Advancements in technology could have made it easier to commit cyber crimes.*

Respondents (24%) in India, reported cyber crime to be among the top four economic crimes. This highlights the need to analyse the impact of cyber crime and invest in preventive and diagnostic measures.

Also, almost half of the respondents said they perceive the risk of cyber crime to be on the rise. Only 8% were optimistic about its decline and the rest thought it will stay the same. This data can be interpreted in the backdrop of greater media involvement in exposing or broadcasting an exposé - more so an economic exposé that could impact several unsuspecting third parties.

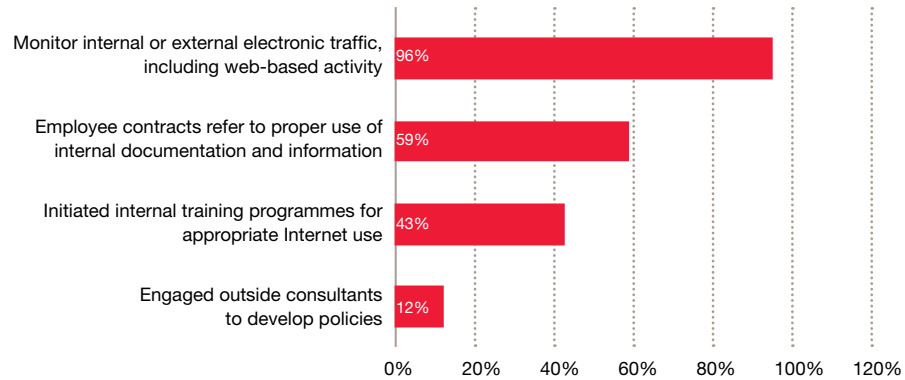
The use of the internet on handheld devices has enabled everyone to have access to real time information, for e.g. news, cricket scores, stock prices, etc., and also to carry out functions like online trading, shopping and banking. These new devices have opened up new ways for criminals to commit cyber crime, be it on a micro scale by just targeting individual, or on a macro scale by targeting large networks. This has made consumers and organisations at large to be vulnerable to cyber crime risks.

Moreover with extensive use of social media sites like facebook, twitter and the like, employees are unwittingly sharing confidential information. Organisations need to be aware that the employees might have a very different understanding of the risks such sites pose and hence need to be educated accordingly.

Combating social media risks

As seen in *Figure 2*, 96% of the respondents said they monitor internal and external electronic traffic including web pages, around 59% said their employee contracts cover how to use information and documents properly, and 43% said they conducted training programmes. It is critical to note that in the absence of appropriate guidelines on use of internal information and documents in employee contracts, it will make it difficult to take action against employees.

Figure 2:
Action taken to combat the risks of social media



Respondents were able to select multiple responses.

Is it just an external threat?

47% (i.e. 15 % internal and 32% combination of internal and external) respondents feel that cyber crime is an internal threat.

What is hiding in your IT and Marketing and Sales Department?

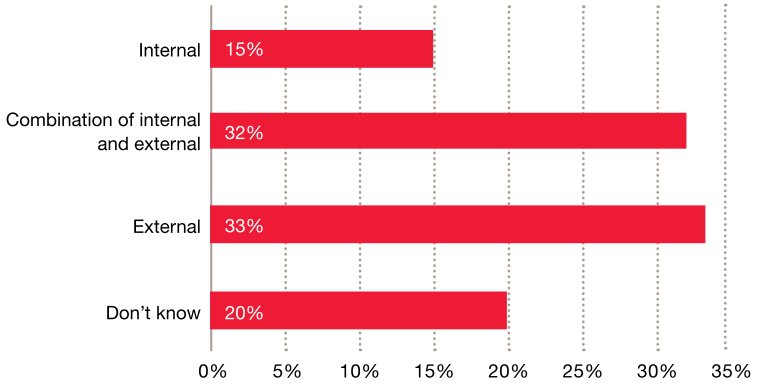
Figure 4 reveals that 58% of the respondents in India felt the IT department in the organisation was a high risk target for cyber crime. This was followed by marketing and sales (50%). Only 4% found the legal department to be at high risk.

One of the potential reasons why IT is perceived as a high-risk department is because its personnel have "super user" access. This presents an opportunity to misuse additional administrative rights to access systems and the ability to delete audit trails. This makes it hard to detect wrongdoing.

The marketing and sales department ranks second on the list. In the past few years the volume of online transactions in India has increased rapidly.

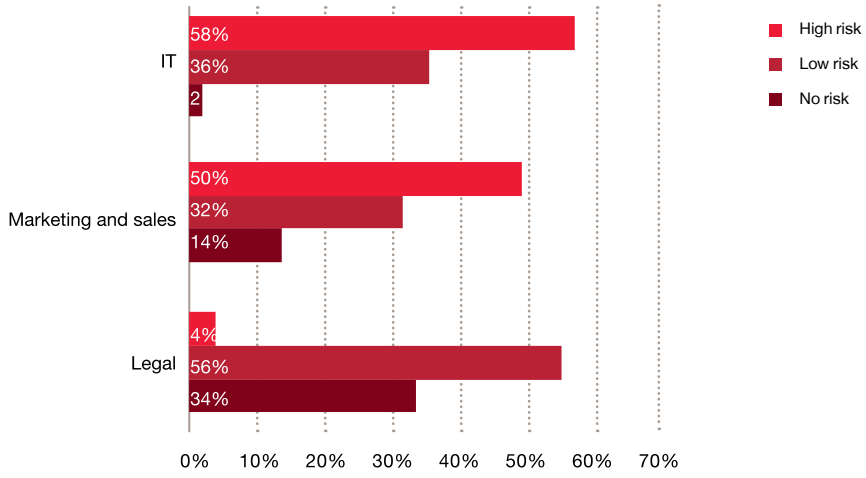
Additionally, marketing and sales teams have far greater contact with third-parties such as resellers, agents, intermediaries, online gateways, hosting sites, server companies and consumers. In India, around 44% of the respondents felt that after customers, agents and intermediaries are the main perpetrators of fraud. This underscores the need for regular internal audits to check cyber crime risks and to ensure compliance of the company's internal security regulations.

Figure 3:
Source of greatest risk of cyber crime



% of respondents who monitor social media sites

Figure 4:
Departments susceptible to cyber crime threat



% of respondents who feel that threat of cyber crime lies within the organisation

On the other hand, the legal department is more or less localised and the risk may pertain to the leakage of sensitive information. Although the probability of the legal department being the source of cyber crime is low, the potential impact can be extremely high.

e.g. the leakage of a share purchase agreement in an ongoing mergers and acquisitions transaction could result in financial and reputational loss for the organisation.

What makes cyber crime different?

We found that cyber crime offers low risks and high rewards as compared to traditional crimes.

For example, in an externally perpetrated cyber crime, a fraudster infiltrates a banking system, remotely, to steal money or personal information. The fraudster is at a lesser risk when compared to someone who physically steals assets from an organisation.

There are fewer risks when committing cyber crime:

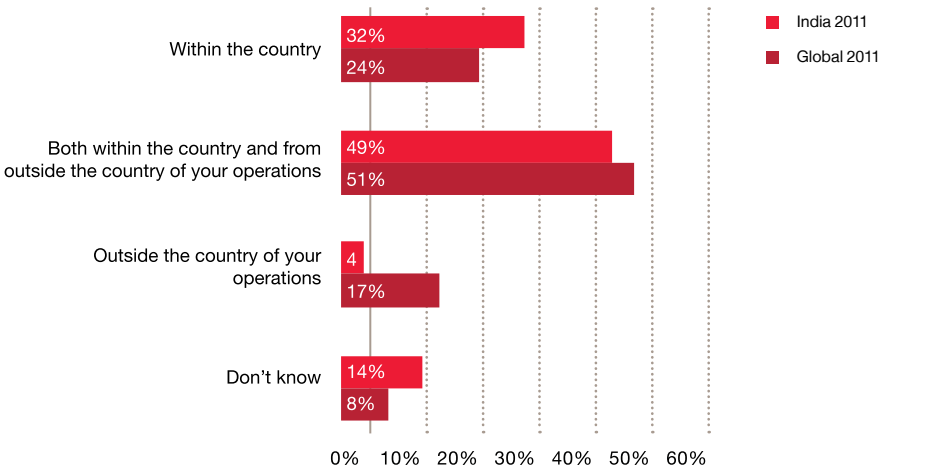
- *The fraudster is not present at the location, hence the chances of getting caught are less.*
- *Difficulties for law enforcement agencies to follow traditional investigative steps to prosecute the perpetrator owing to the different location and jurisdiction of the perpetrator.*
- *The perpetrators can return to the scene of the crime with relatively minimal fear of detection.*

External perpetrators of cyber crime

Out of the total number of respondents who chose cyber crime as an external threat, 81% (i.e. 32% within the country and 49% both within and outside the country) of the Indian respondents felt the threat comes from both within and outside the country. However, only 4% of the respondents identified the threat as external as opposed to 17% of global respondents.

This indicates that organisations in India feel that the greatest threat of cyber crime is localised and at home than outside the country of operations where they draw a lot of comfort, perhaps due to advanced regulations and enforcement systems dealing with cyber crime. This argument gains more momentum if one were to see the profile of Indian respondents- 34% of Indian respondents are working in organisations which have offices in more than 20 countries. In the Indian context, with the recent wave of outbound investments, many organisations in India have acquired operations UK, USA, Western Europe, Africa and Latin America and their perception of a greater cyber crime threat at home underscores the need for implementing cyber security programmes at home.

Figure 5:
Source of external cyber crime threat



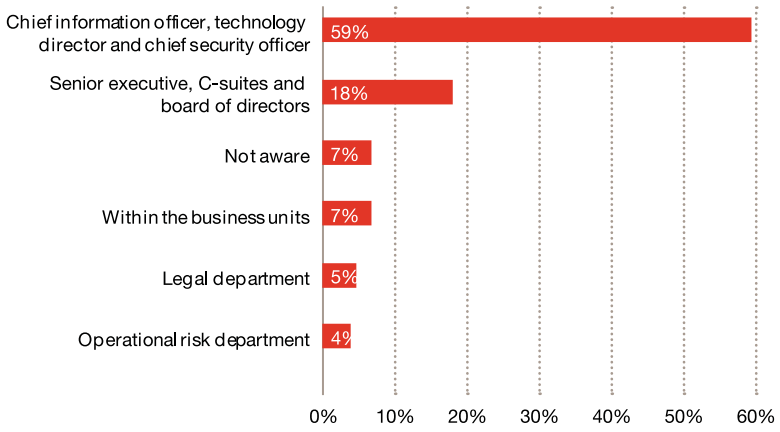
% of respondents who feel that threat of cyber crime is external to the organisation

Who is responsible?

In the past, cyber security was classified as an IT issue, creating a communication gap between business managers and security professionals. Today, cyber security is considered not just a technical issue, but a core business imperative. PwC's Global State of Information Security Survey 2011 confirms that executive recognition of security's strategic value is now more closely aligned with business than with IT. The most common reporting channel for chief information security officers (CISOs) is now the chief executive officer (CEO) rather than the chief information officer (CIO).

Figure 6 reveals that 59% of the respondents placed responsibility of dealing with cyber crime threats on the CIO or technology director. Only 18% placed responsibility on the CEO or the board. Although the CIO is usually responsible for IT security risks, the CEO and the board should understand and probe into the risk of cyber crime.

Figure 6:
Ownership and responsibility of preventing cyber crime

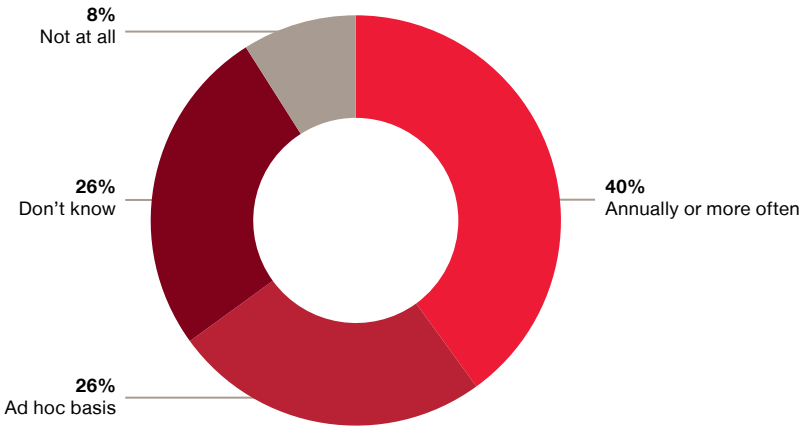


Are cyber crime risks being reviewed by your Management?

Only 40% of the Indian respondents reported that top management reviews these risks at least annually. Almost a quarter (26%) of the respondents stated that the CEO and the board review cyber crime related risks on an ad hoc basis.

The statistics indicate that senior management do not place enough emphasis on managing cyber crime threats and frauds. Keeping in mind future challenges, PwC has introduced a white paper on the cyber-savvy CEO. The paper examines why entering the cyber environment represents a seismic shift in the security landscape for all organisations. It also highlights some of the structures, actions and capabilities that organisations can apply to achieve sustainable success in the cyber age. We believe that a CEO who understands the risks and opportunities of the cyber world will realise the benefits and manage the risks for his/her organisation (both private and public) more effectively.

Figure 7:
Frequency of risk review by senior management

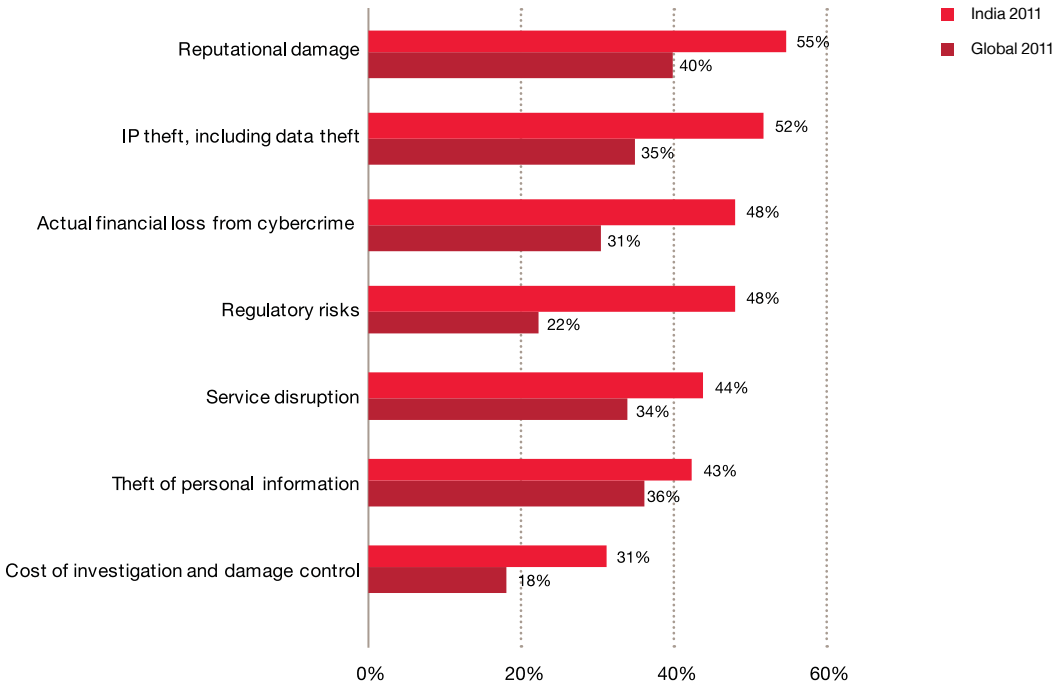


55% are concerned about reputational damage arising out of cyber crime.

Prevention is better than cure

As seen in *Figure 8*, in India, an overwhelming number of respondents (55%) are concerned about reputational damage, IP theft (52%) and actual financial loss (48%) resulting from cyber crime. These figures are higher than the global trend. This emphasises the need for Indian companies to have an adequate response mechanism and policies, and invest in trainings to reduce the risk of cyber crime.

Figure 8:
Areas of major concern



Respondents were able to select multiple responses.

Engagement of external experts in India

More than half of the Indian respondents (51%) do not engage experts until the incident has occurred. If organisations adopt a more proactive approach, it will not only reduce their susceptibility to cyber crime, but will also bring down the response time. In its absence, response time is slow and the investigation becomes less efficient. This trend has been observed globally as well.

Therefore, organisations need to perform cyber crime assessment, design crisis plans and training programmes, and define responsibilities and activities to be carried out at the time of crisis.

Figure 10 explains that only a third had access to forensic technology investigators. In absence of forensic technology investigators, organisations dealing with cyber crime threats will not be able to secure evidence of required nature and standard that can help address the risks of cyber crime.

Figure 9:
Engagement of external experts in India

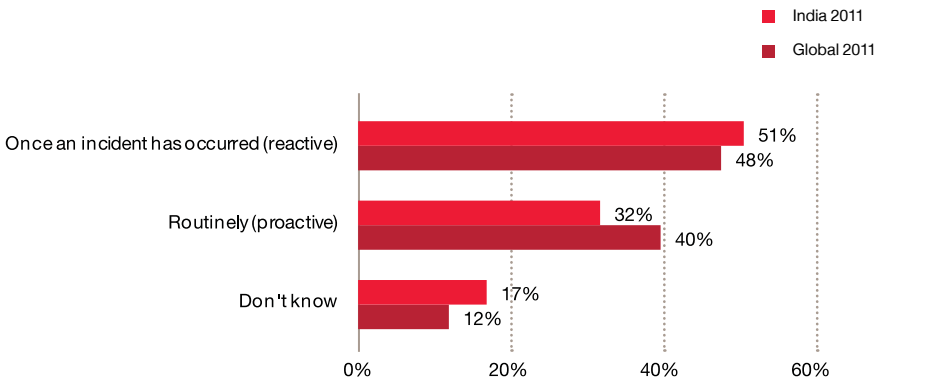
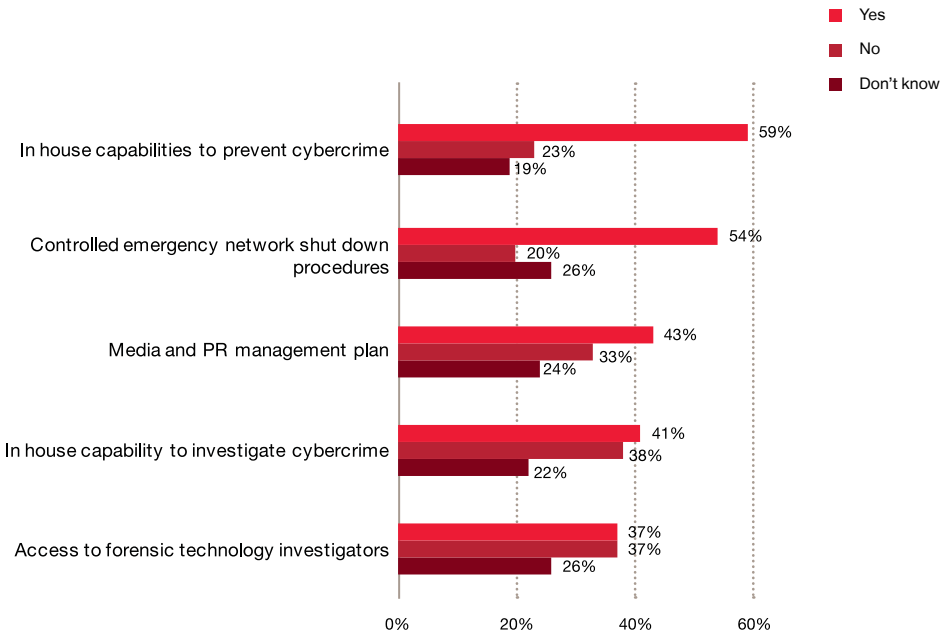


Figure 10:
Detection mechanisms for cyber crime incidents



Respondents were able to select multiple responses

In India, despite the implementation of the IT Act, 2000, the state enforcement agencies and the police are generally unprepared to conduct sophisticated investigation and unearth relevant evidence that can be used to prosecute offenders. As a result, organisations are left to deal with the perpetrators. e.g. if an organisation wants to take action against an employee engaged in fraudulent activities, it needs to have access to forensic technology investigators. This will provide evidence to support any inquiry, in the absence of which the company runs the risk of being sued for unjustifiable termination or employee harassment.

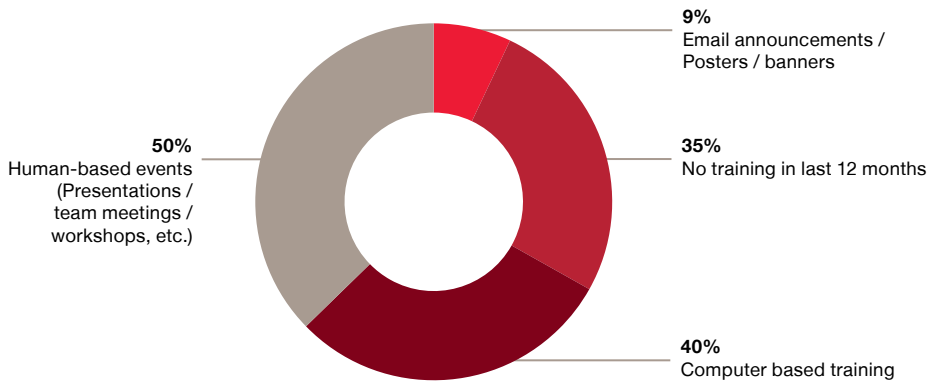
Reducing risks

To help organisations design effective training programmes, we asked our respondents the type of trainings they have received in the past and what according to them will be the ideal cyber security awareness training.

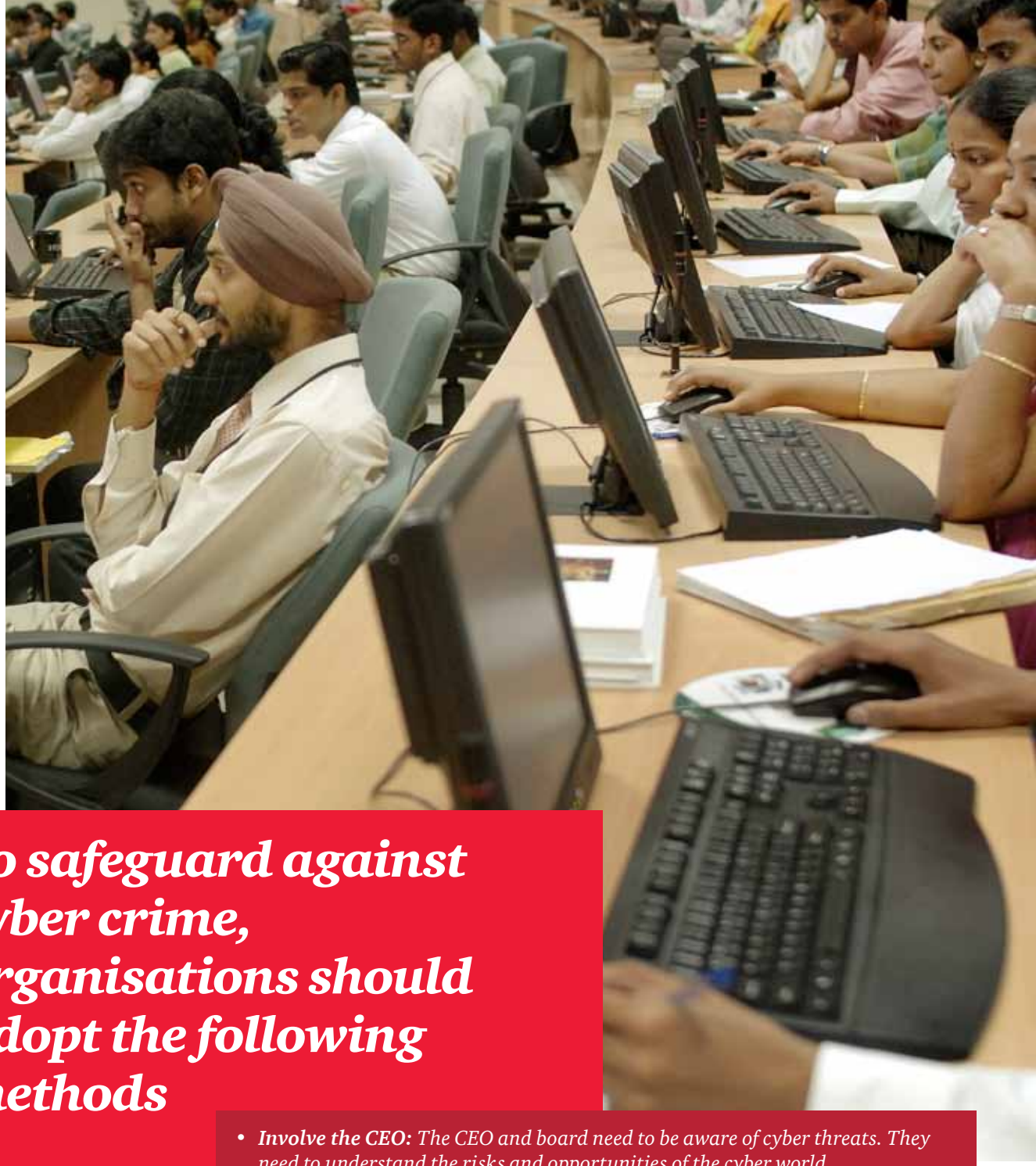
Given that people think cyber crime is on the rise, it is discouraging to learn that 35% of respondents did not have any cyber security training in the last 12 months.

Once employed, the trajectory of the employee and subsequently the organisation's growth depend on the trainings provided. Out of the multiple ways in which cyber crime prevention training sessions are being provided by organisations, about 50% of the respondents find face-to-face trainings to be more effective.

Figure 11:
Types of training received to prevent cyber crime



Respondents were able to select multiple responses



To safeguard against cyber crime, organisations should adopt the following methods

- ***Involve the CEO:*** *The CEO and board need to be aware of cyber threats. They need to understand the risks and opportunities of the cyber world.*
- ***Re-assess the security function:*** *Unlike traditional 'economic crimes', cyber crime is fast paced with new risks emerging which means an organisation needs to continuously revamp its procedures.*
- ***Increase awareness:*** *Organisations need to have a clear understanding of the current and emerging cyber environment. This will facilitate in undertaking well informed and prioritised decisions and actions.*
- ***Create a cyber incident response team:*** *The team needs to act with speed and agility. A well-functioning cyber response team will track and assess risk and escalate it to the top.*
- ***Educating employees:*** *An organisation needs to embed a 'cyber awareness' culture by recruiting personnel with the relevant skills. These personnel can share knowledge with other employees and create 'cyber-awareness' to protect the organisation.*
- ***Take consistent action:*** *An organisation needs to pursue cyber crime perpetrators through legal means and publicly communicate its actions.*

Economic crime
A new high or a new low

In the last one year, the world of economic crime has touched new lows. Fraudsters, criminals, hackers, imposters, etc. have been increasingly active, especially on the economic crime front.

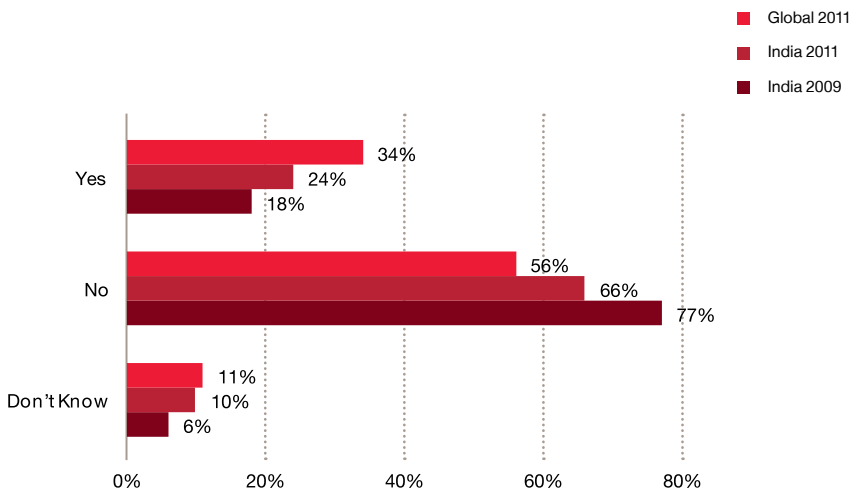
This survey attempts to understand where the risk of economic crime lies within an organisation and how to address it.

The 'new high' of economic crime is reflected in our survey as well where 24% of the Indian respondents reported having been a victim in the last 12 months, compared to 18% in 2009.

Interestingly, 10% of Indian respondents were unaware whether their organisation has experienced economic crime in the last 12 months as compared to 6% in 2009. This is a distressing trend as majority of our respondents were key decision makers.

A look at the profile of the Indian respondents reveals that around 20% belong to organisations with employee strength greater than 1000, whereas for 2009 it was 22%.

Figure 12:
Economic crime experience



% of respondents

Large organisations are more susceptible to fraud despite stringent controls and policies.

A large organisation is more susceptible to economic crime than a smaller one. Such organisations also tend to have a more stringent and efficient policy in place, along with dedicated personnel, to tackle such risks. The increase in reporting of economic crime might indicate that the system is becoming more efficient in tracking perpetrators but not in stopping them. It may also imply that the measures in place are more reactive than proactive.

Globally, 34% of the organisations experienced economic crime in the last 12 months, whereas in India 24% of the organisations were victim of economic crime. Indian organisations are reluctant to report fraud due to the fear of media coverage and the regulatory attention. Some Indian organisations might also have a high tolerance for crimes such as bribery and corruption, as these are perceived to be necessary for survival.

Although, over the years, organisations have made significant investments to control fraud, the level of reported economic crime has risen.

This may, in part, be due to ***'fraud controls paradox'*** – the notion that when controls are implemented in an organisation, the number of frauds detected increases almost immediately. However, their deterrent effect takes time to become visible. Potential fraudsters need to know that there exists a greater likelihood of detection, and those in breach of an organisation's ethical, regulatory and legal guidelines will be suitably punished.

Behind the overall background of an increasing economic crime rate, we asked our respondents what types of fraud they have experienced. The results are similar to what we have noticed in our previous surveys, with the exception of cyber crime – the newest addition to the list of economic crime types.

reported asset misappropriation which is a significant jump from 46% in 2009.

68%

Types of Economic Crime

Asset Misappropriation is on the rise

Economic crime can take many different forms, with some being more common and more persistent than others. Equipped with four years of data (i.e., 2005, 2007, 2009 and 2011), we are able to compare how opinions have changed over this time period.

Most common types of economic crimes experienced in the last 12 months were asset misappropriation, bribery and corruption, cyber crime and accounting fraud.

Around 68% of our Indian respondents reported asset misappropriation cases as opposed to 46% in 2009 and 20% in 2007.

This is most likely driven by the personal financial situation of the fraudster combined with weak controls in an organisation resulting in greater opportunities to commit crime. Asset misappropriation has been prevalent in India since we began our survey in the country and covers a variety of misdemeanors. While this type of fraud is the hardest to prevent, it is arguably the easiest to detect.

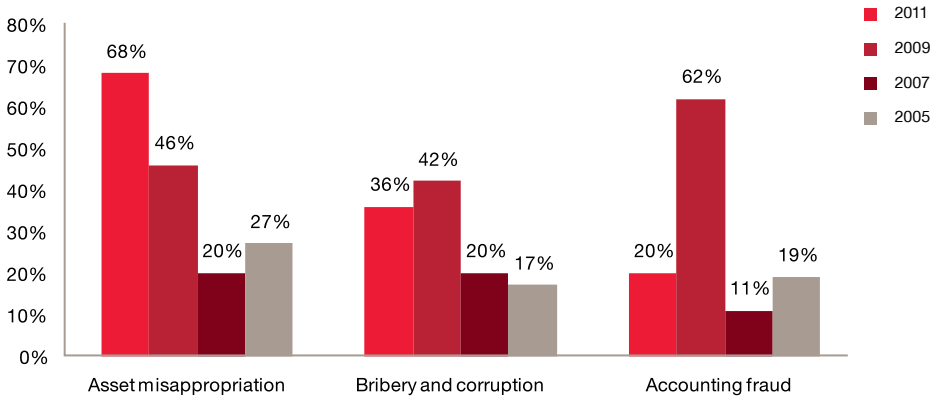
It involves theft of an entity's resources. The primary examples of asset misappropriation are fraudulent disbursements such as billing schemes, payroll schemes, expense reimbursement schemes, cheque tampering and cash register disbursement schemes. Sometimes, employees may collude with others to perpetrate frauds such as aiding vendors to short change the organisation.

Among the several new economic crimes registered in our survey, asset misappropriation as a category has registered a continuous increase since 2005 (barring 2007).

The sharp rise in organisations who have experienced asset misappropriation, indicates that the controls designed to detect and prevent it have not proven to be uniformly effective. Further, it indicates that controls to check such crimes are more reactive than proactive in nature.

Organisations that have established controls in this area, must consider the inherent delayed deterrent effect of such controls. The perceived effectiveness of controls is significantly impacted by the 'fraud controls paradox' and the fact that fraudsters will always try to find ways to circumvent the most rigorous controls.

Figure 13:
Trends in reported frauds



% reported frauds . Respondents were able to select multiple responses

Hence it is our proposition that the value of controls lies in ensuring that

- *Controls are continually upgraded and adapted to thwart the fraudster;*
- *Controls reflect the culture of the firm and its ethical guidelines (which incorporate the explicit norms of criminal law); and,*
- *Cases of fraud that are detected trigger an immediate, appropriate and consistent punitive response, no matter what the position of the perpetrator inside or outside the firm.*

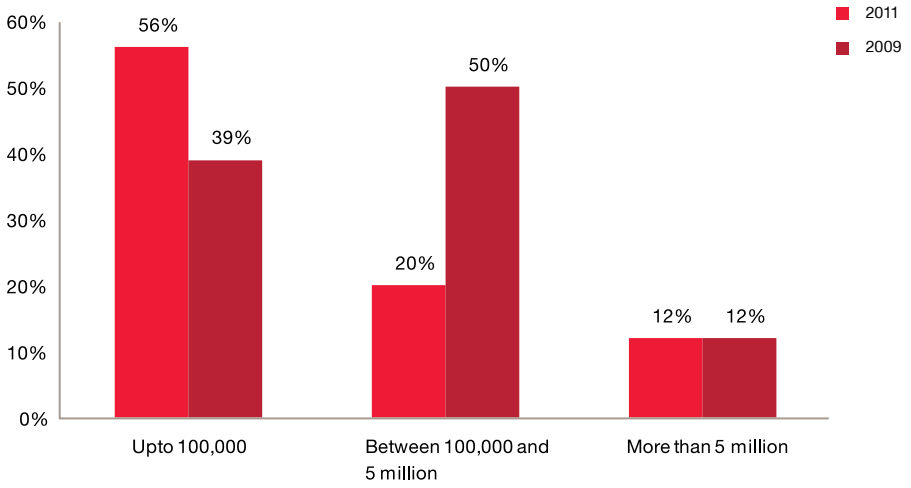
Why is it important to address fraud risks?

The financial damage from 'tangible frauds'

Of the total respondents that reported incidents of fraud over the last 12 months, approximately 32% said that the direct financial impact of this exposure was more than US$ 100,000 (approximately INR 50 lakh).

Yet the consequences faced by organisations due to fraud are not just financial in nature as they also suffer significant collateral damage. If a financial loss of more than US$ 100,000 (approximately INR 50 lakh) seems insignificant, consider the collateral damage from fraud, for it is here that one sees the potentially crippling impact of economic crime.

Figure 14:
Financial loss due to economic crime in US$



% respondents who experienced economic crime in the last 12 months.

In money laundering cases, there are no immediate financial costs to the organisation as it only attempts to legitimise the proceeds of a crime. Similarly, corruption and bribery involve payment of cash or gifts to secure a contract or favour but may not be considered as losses to the organisation.

Collateral damage

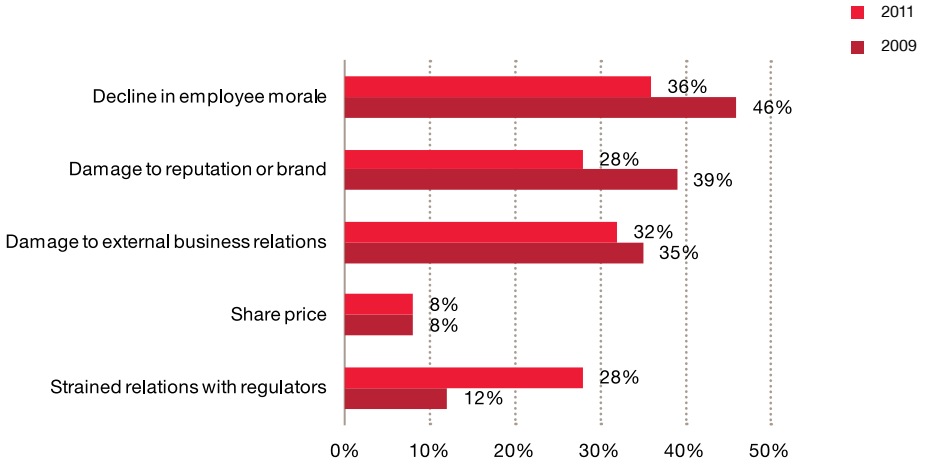
Beyond financial consequences

While quantifying the financial damage of fraud is hard, it is even more difficult to estimate the collateral damage. Following are the collateral damages as reported by respondents who experienced fraud:

- Decline in employee morale (36%)
- Damage to external business relations (32%)
- Damage to reputation or brand image in the marketplace (28%)
- Damage to relations with regulators (28%)

Managing stakeholders, employees and also increased global co-operation among regulators and growing local enforcement add to the complexity/success factors of any business and can be undermined by the occurrence or even the perception of fraud.

Figure 15:
Collateral damage of fraud



% respondents who experienced economic crime in the last 12 months. Respondents were able to select multiple responses.

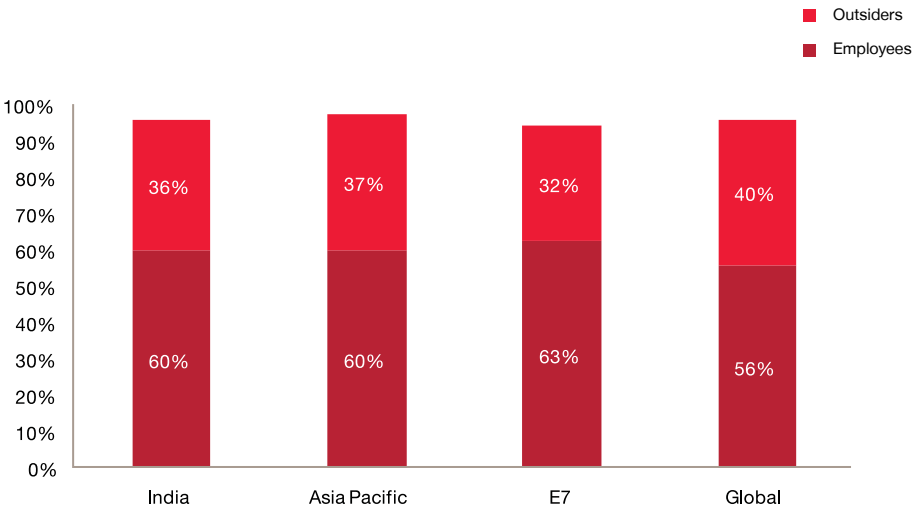
Who is committing the fraud?

As instances of fraud increase, organisations need to diligently protect themselves.

An effective way of combating fraud is by gathering relevant information about the perpetrators. This helps detect loopholes in an organisation's response mechanisms and internal controls.

Our survey asked respondents who had experienced economic crime in the last 12 months to profile the main perpetrator of the most serious fraud. 60% organisations said it was employees while only 36% pointed to outsiders. The remaining 4% said they did not know.

Figure 16:
Perpetrators of fraud



% respondents who experienced economic crime in the last 12 months.

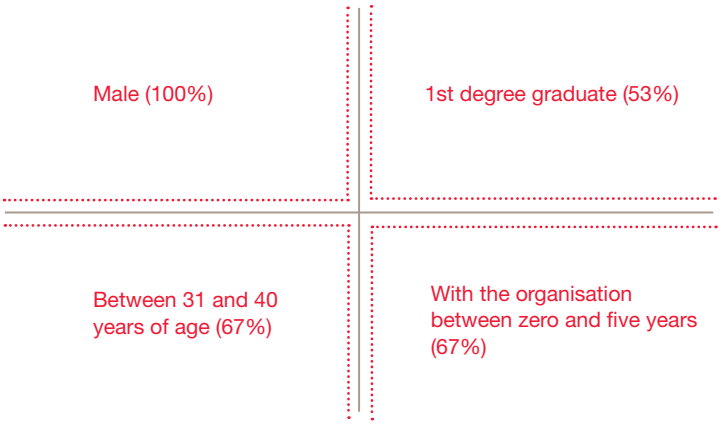
Note: Percentages do not add up to 100 for India, Asia Pacific, E7 and global since some of these respondents indicated that they did not know if the fraudster was an outsider or an employee.

Profile of an internal fraudster

Nearly two-thirds of the respondents (60%) found that the perpetrators were among their own staff. This is not surprising as internal fraudsters have a strong understanding of the organisation, including the strengths and weaknesses of the internal controls that prevent fraud.

Based on our survey, the figure alongside shows the typical characteristics of the internal fraudster

Figure 17:
Profile of an internal fraudster



Respondents were able to select multiple responses

Dealing with employees

An important step in creating a corporate culture that does not tolerate fraud is consistent action when an economic crime is detected. When staff understand the probable, personal and legal consequences of fraud, and realises that detection is likely due to the effective nature of risk management systems and internal controls, it serves to deter many criminals-in-the-making.

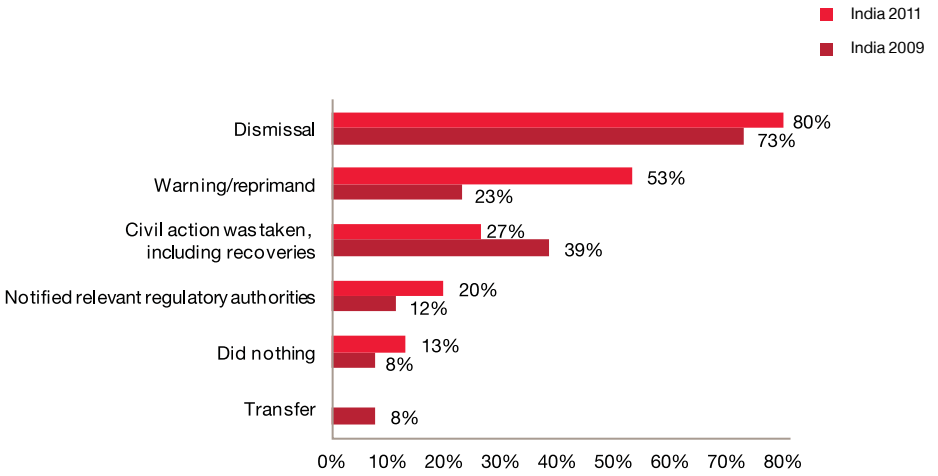
For an 'inside job', 80% of respondents said their organisation terminated the individual, more than half warned or reprimanded and quarter took civil action and around 20% informed relevant regulatory authorities.

Some organisations display complacency in dealing with fraud. Is it right to keep a fraudster in the organisation and run the risk that he/she might do it again?

In our experience, while dealing with fraudsters, maintaining independence, having a process and consistency in process is critical for it to be a deterent.

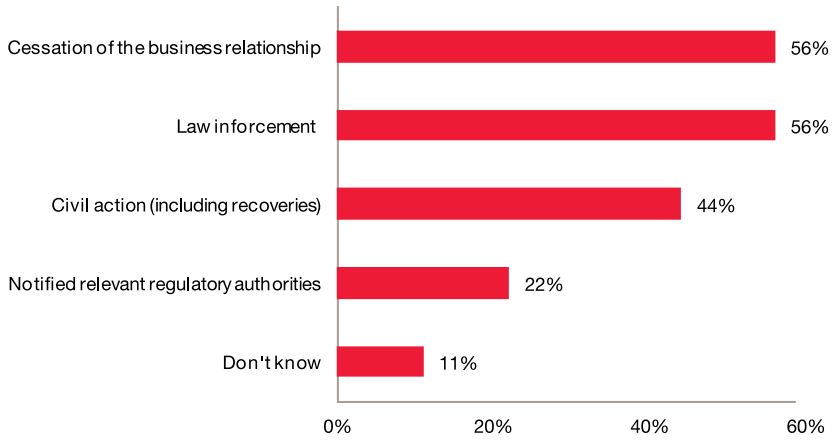
For an 'outside job', 56% of respondents terminated their relationships, 56% of respondents informed the police, 44% opted for civil action, and 22% informed the relevant regulatory authorities.

Figure 18:
Action taken against employees



% respondents who reported that an employee was the main perpetrator of fraud. Respondents were able to select multiple responses.

Figure 19:
Action taken against outsiders



% respondents who reported that an outsider was the main perpetrator of fraud. Respondents were able to select multiple responses.

One of the key fraud prevention techniques is to know who you are doing business with. Therefore, know-your-customer (KYC), vendor due diligence, agent due diligence are recognised as critical elements of risk reduction programmes. Besides, transparent programmes such as 'know your business associates' act as effective preventive tools. Also, recent anti-bribery regulatory actions have highlighted the risk that third parties pose to organisations. Third party reviews should be carefully conducted and customised to suit various businesses.

Companies should conduct a robust risk assessment and thorough background check of the existing and potential third parties to better understand their risk profile. It is also important to review the contractual terms that govern retention of third parties and organisations should ensure that they are vested with the right to review the books and records of third parties on a periodic basis.

These steps would ensure that the company's compliance policies are reflected in the business practices of associated third parties and that there is no threat of additional risk.

Despite increased levels of transparency, in a bid to prevent collateral damage many organisations do not report incidents of 'internal job.' However, when the perpetrator is an outsider organisations pursue the case with regulators in order to demonstrate good corporate governance and to reclaim as much of the loss as possible. To combat fraud, 'consistent action' against internal as well as external perpetrators is important.

Fraud detection methods

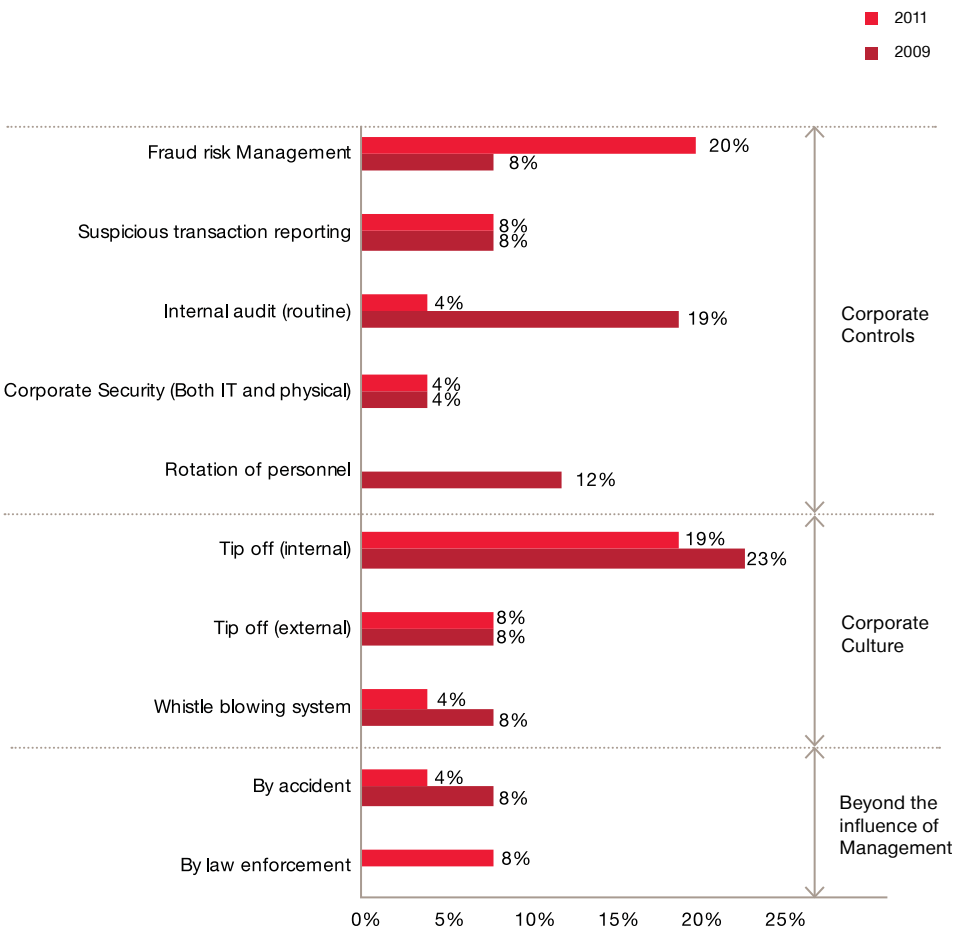
It refers to methods employed by organisations to detect economic crime. Such methods include the following:

- *Corporate culture such as internal tip-off, external tip-off and whistleblowing;*
- *Corporate controls such as internal audit, fraud risk management, electronic and automated suspicious transaction reporting, corporate security and change of personnel or duties; and*
- *Other actions outside the control of the organisation including law enforcement, investigative media, etc.*

Economic crimes committed by employees are frequently uncovered through internal tip-offs or in the internal audit process. External perpetrators are often detected from external tip-offs, effective risk management systems and good corporate security.

It is interesting to note that the effectiveness of internal audit to detect frauds has considerably declined over the years. This may be due to budgetary constraints wherein internal audit is being asked to do more work and/or with less staff and increased demands placed on internal auditors in a changing business environment.

Figure 20:
Fraud detection methods



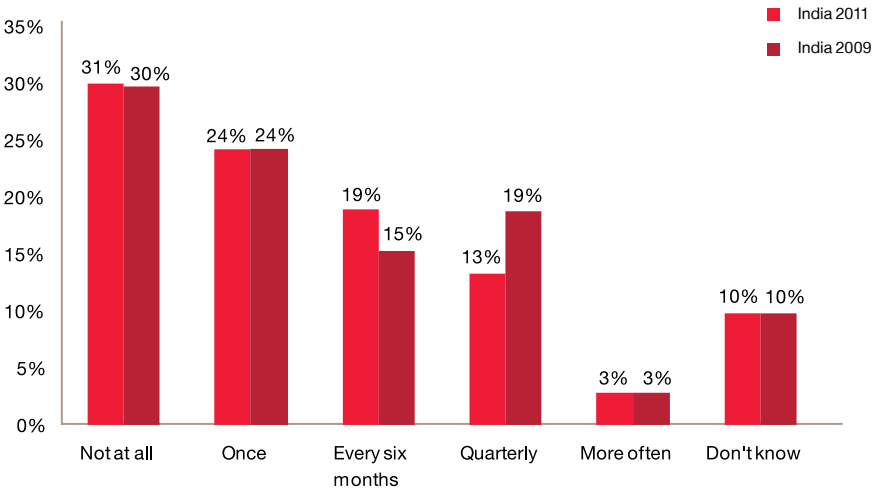
% respondents who experienced economic crime in the last 12 months.

Fraud Risk Assessment

A comprehensive fraud risk assessment should:

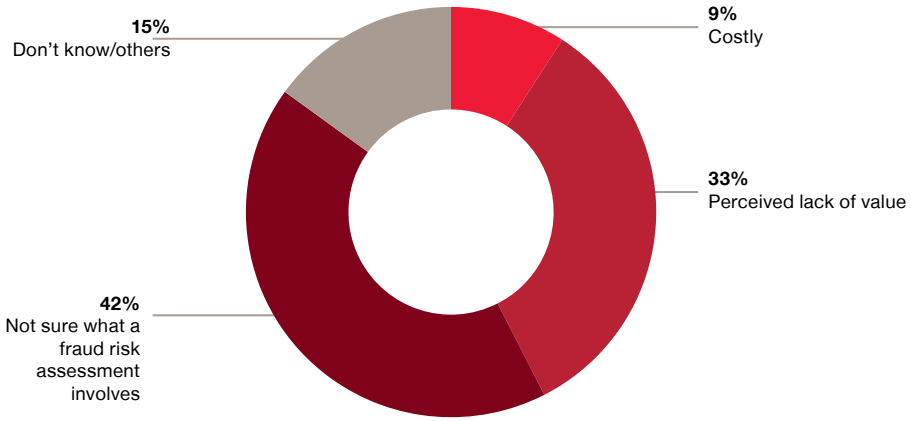
- *Identify the potential inherent fraud risks;*
- *Assess the likelihood and significance of occurrence of the identified fraud risks;*
- *Evaluate which people and departments are most likely to commit fraud and identify the methods they are likely to use;*
- *Identify and map existing preventive and detective controls to the relevant fraud risks;*
- *Evaluate whether the identified controls are operating effectively and efficiently;*
- *Identify and evaluate residual fraud risks resulting from ineffective or non-existent controls; and*
- *Respond to residual fraud risks.*

Figure 21:
Frequency of performing a Fraud Risk Assessment



% respondents who experienced economic crime in the last 12 months.

Figure 22:
Reasons for not conducting a Fraud Risk Assessment



Fraud Risk Assessment

The best way to fight fraud is to know how to assess and identify the risks. The fewer fraud risk assessments, the organisations carry out, the less fraud they are likely to detect.

According to our survey, 31% of the Indian organisations have not performed a fraud risk assessment at all. In order to protect the organisation against fraud risks and send warning signals, the assessment must be performed more often. The number of organisations that perform fraud risk assessment more often has remained stagnant since 2009.

Nearly one-third of the respondents do not perform a Fraud Risk Assessment due to a perceived lack of value. This is a matter of great concern as the survey respondents are primarily large organisations with capabilities and resources and are also most susceptible to fraud. The data reveals the need for key decision makers to be adequately informed about fraud risk assessment. This can help organisations minimise risk of fraud.

Fraud in the future
An illusion of safety

Respondents to our survey over the years have estimated their exposure to various kinds of fraud in the coming 12 months to be far less than what they actually experienced in the future. With the benefit of hindsight, it is clear that their perceptions are often misplaced.

Only 12% of our respondents to the 2009 survey perceived asset misappropriation to be a likely threat in the next 12 months. However, asset misappropriation was the most commonly experienced fraud in 2011. Moreover, only 29% of the respondents perceive it to be a likely threat in the coming 12 months.

The fight against fraud is a constant struggle. Despite the increase in the number of frauds being detected and the effectiveness of risk management systems being deployed, there are always individuals or groups of individuals who have an incentive and the ability to rationalise committing fraud and/or who are able to spot an opportunity to circumvent or override controls. Organisations must not drop their guard, but must constantly develop controls and build on the loyalty of their employees to ensure that, even if it is impossible to eradicate fraud, they do not provide an environment in which it can flourish.

Figure 23:
Fraud in the future

	Asset Misappropriation	Bribery and Corruption	Accounting Fraud
Perception 2009 (over next 12 months)	12%	10%	23%
Reality 2011 (% Reported economic crime)	68%	36%	20%
Perception 2011 (over next 12 months)	29%	28%	17%

% respondents who experienced economic crime in the past 12 months and % respondents' perception over the next 12 months. Respondents were able to choose multiple responses.

Conclusion

In a dynamic economic environment, organisations need to be vigilant and proactive when fighting economic crime. Traditional frauds like asset misappropriation, bribery and corruption and accounting fraud remain the top four that our respondents fell victim to in the last 12 months.

Interestingly, asset misappropriation as a category has registered a steady increase since 2005. The sharp rise in organisations that have experienced asset misappropriation indicates that the controls designed to detect and prevent it have not proven to be uniformly effective. Further, it indicates that controls to check such crimes are more reactive than proactive or preventive in nature.

Organisations also had to contend with 'new age' frauds - cyber crime in particular. Frequent revolution in the technology space is throwing open new ways of doing business. 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. Heightened globalisation has changed work environments. Against this backdrop, fraudsters are finding innovative ways to carry out crimes.

Are you ready for the challenge?

Organisations need to be aware of these changes and adapt their response mechanisms and detection methods accordingly. 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 crime. Advances in technology are fast-paced, as are fraudsters; however organisations are often behind the curve in combating fraud.

It is critical 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" along with effective preventive controls and stern action against perpetrators are critical in the fight against economic crime.

Methodology and acknowledgements

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, cyber crime.*

About the survey

The 2011 Global Economic Crime Survey was completed by 106 Indian respondents.

We used the following research techniques:

1. Survey of executives in the organisation. The findings in this survey come from executives' reports of their experience 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 cyber crime . This survey takes a detailed look at the growing threat of cyber crime, and how vulnerable organisations are to it. This focus enables us to understand what cyber crime really means for organisations.
3. Analysis of trends over time. Since we started doing these surveys in India from 2003, 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 at hand, we can see current themes, chart developments and find trends.

Figure 24:
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	126	14
New Zealand	93	85
Papua New Guinea	1	0
Phillippines	0	1
Singapore	18	51
South Korea	0	1
Taiwan	2	0
Thailand	79	25
Vietnam	19	0
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
Zamibia	1	0
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
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	60	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
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***

Figure 25:
Participating industry groups – India

% respondents	2011	2009
Aerospace and defence	1%	0
Automotive	5%	5%
Chemicals	2%	3%
Communications	2%	3%
Energy, utilities and mining	7%	6%
Engineering and construction	9%	10%
Entertainment and media	5%	3%
Financial services	20%	18%
Hospitality and leisure	3%	3%
Insurance	4%	0
Manufacturing	10%	17%
Pharmaceuticals and life sciences	13%	3%
Professional services	5%	4%
Retail and consumer	4%	8%
Technology	8%	9%
Transportation and logistics	3%	6%
Other industries	0	2%

Figure 26:
Organisation types participating – India

% respondents	2011	2009
Private	55%	23%
Listed on a stock exchange	44%	50%
Government/state-owned enterprises	1%	6%
Others including cooperative/ non-profit organisations	0	7%

Figure 27:
Size of participating organisations – India

% respondents	2011	2009
Up to 200 employees	21%	26%
201 to 1,000 employees	27%	31%
More than 1,000 employees	20%	22%
Don't know	1%	0

Figure 28:
Function (main responsibility) of participants in the organisation– India

% respondents	2011	2009
Executive management	17%	22%
Finance	32%	55%
Audit	9%	6%
Risk management	8%	4%
Compliance	6%	1%
Security	0	2%
Legal	6%	1%
Information technology	1%	1%
Advisory/consultancy	9%	1%
Operations and production	4%	2%
Marketing and sales	1%	2%
Human resources	0	1%
Tax	7%	2%

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.

Cyber crime

Also known as computer crime, this is committed using the computer and internet. Typical instances of cyber crime 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.

Cyber crime incident response

This would typically include in- house technical capabilities to prevent, detect and investigate cyber crime, 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:

- The fraud risks to which operations are exposed;
- An assessment of the most threatening risks (i.e. evaluate risks for significance and likelihood of occurrence);
- Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
- Assessment of the general anti-fraud programmes and controls in an organisation; and
- 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 it 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.

Acknowledgements

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

Vidya Rajarao, Leader, Forensic Services

Kunal R. Gupta, Associate Director, Forensic Services

Darshan Patel, Associate Director, Forensic Services

Anujeet Kudva, Senior Manager, Forensic Services

Particular thanks in compiling this report are also due to the following individuals at PricewaterhouseCoopers Private Limited:

Aarti Bansal Lamba, Abrity Basu, Ankita Chawla, Divya Rishi, Joyceline D'souza, Mohit Desai, Nidhi Jain and Riddhi Vora

Contacts

Forensic Services

Vidya Rajarao
Phone: +91 (80) 4079 7002
Email: vidya.rajarao@in.pwc.com

Darshan Patel
Phone: +91 22 6689 1670
Email: darshan.patel@in.pwc.com

Kunal R. Gupta
Phone: +91 (0) 124 330 6036
Email: kunal.r.gupta@in.pwc.com

Anujeet Kudva
Phone: +91 22 6689 1635
Email: anujeet.kudva@in.pwc.com

Forensic Technology Services

Vinay Nayak
Phone: +91 22 6689 1626
Email: vinay.nayak@in.pwc.com

IT Security Risk

Sivarama Krishnan
Phone: +91 (0) 124 462 0511
Email: sivarama.krishnan@in.pwc.com

Siddharth Viswanath
Phone: +91 (0) 124 462 0520
Email: siddarth.viswanath@in.pwc.com

Anirban Sengupta
Phone: +91 (0) 124 462 0126
Email: anirban.sengupta@in.pwc.com

Nikhil Donde
Phone: +91 22 6669 1383
Email: nikhil.donde@in.pwc.com

About PwC forensic services

The forensics services Practice of PricewaterhouseCoopers Pvt Ltd (PwC) provides a national and global network of analysts, actuaries, accountants, fraud examiners and others who are leaders in their respective fields. We offer a wide variety of skills to address the issues affecting parties involved in disputes. Our aim is to work in partnership with clients to implement fraud control methodologies, assist when incidents occur and help with strategies and practices to avoid fraud.

We work discreetly and use a range of skills to assist our clients. We use experienced investigators, forensic accountants, computer forensic specialists and background researchers. The team integrates proven evidence gathering skills along with control methodologies to produce effective results for our clients. We offer a complete computer forensic service through our team of trained specialists.

To provide value for our client, our forensic service collaborates with PwC Internal Audit Services. We combine an in-depth and most advanced knowledge of business risks, internal controls and audit, along with subject matter specialists who provide a perspective on industry specific risks and business practices.

About PwC

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

In India, PwC (www.pwc.com/India) offers a comprehensive portfolio of Advisory and Tax & Regulatory services; each, in turn, presents a basket of finely defined deliverables. Network firms of PwC in India also provide services in Assurance as per the relevant rules and regulations in India.

Providing organisations with the advice they need, wherever they may be located, our highly qualified, experienced professionals, who have sound knowledge of the Indian business environment, listen to different points of view to help organisations solve their business issues and identify and maximise the opportunities they seek. Our industry specialisation allows us to help co-create solutions with our clients for their sector of interest.

We are located in these cities: Ahmedabad, Bangalore, Bhubaneshwar, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune.

pwc.com/india

NJ 253 December 2011 GECS.indd
Designed by: PwC Brand and Communications, India